Ochrona osobowych danych medycznych

dr nauk prawnych
Jakub Rzymowski

mgr prawa
Mateusz Kamiński

P R A W O

Protection of personal medical data

S U M M A R Y

In the following article are presented the basis of protection of personal medical data. The majority of the information concerning people who are being examined or cured is considered to be the personal data. It is necessary to emphasize that the subjects which conduct a medical activities bear the responsibility for protection of personal data. Disregarding of these duties can in the extreme cases be threatened by criminal liability.

W artykule zaprezentowano podstawy ochrony osobowych danych medycznych. Większość informacji dotyczących osób badanych lub leczonych ma charakter danych osobowych. Należy podkreślić, że na podmiotach wykonujących działalność leczniczą spoczywają wszystkie obowiązki związane z ochroną danych osobowych. Lekceważenie tych obowiązków może, w skrajnym wypadku, grozić odpowiedzialnością karną.

Rzymowski J.: Ochrona osobowych danych medycznych. Alergia, 2012, 1: 21-23

zymowski J.: Ochrona osobowych danych medycznych. Alergia, 2012, 1: 21-23

Dlaczego chronimy dane

Dla zrozumienia systemu ochrony danych osobowych należy postawić pytanie o powód ochrony takich danych, zwłaszcza dotyczących stanu zdrowia. Prawo do ochrony danych dotyczących stanu zdrowia jest częścią prawa do ochrony danych osobowych mającego swoje źródło w Konstytucji [1]. Kiedy kartoteka zawierająca dane dotyczące stanu zdrowia konkretnych osób znajdzie się na śmietniku i ktoś nieuprawniony zapozna się z tymi danymi, to niewątpliwie nastąpi naruszenie prawa do prywatności osób, których dane dotyczą. Realne zagrożenia tkwią jednak, gdzie indziej. Dane dotyczące stanu zdrowia chroni się, by chronić osoby, których dane owe dotyczą, przed dyskryminacją. Ma to poważne znaczenie w stosunkach zatrudnienia. Przy dzisiejszym poziomie rozwoju medycyny, wnioskować często możemy o przyszłym stanie zdrowia osoby, której aktualny stan zdrowia szczegółowo znamy. Pracodawca, mający pełne informacje o stanie zdrowia pracownika, mógłby po prostu nie przyjąć do pracy osoby, która nie jest absolutnie zdrowa. Podobne problemy osoba taka miałaby w stosunkach ubezpieczeniowych, bowiem ubezpieczyciele najchętniej ubezpieczaliby jedynie osoby absolutnie zdrowe.

Pojęcia podstawowe

Pierwszym pojęciem znaczącym dla poruszanej materii jest pojęcie danych osobowych.

Danymi osobowymi są „wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej” [2]. „Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne [3].

Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań” [4]. Prawo nie precyzuje jakie koszta czas lub działania są nadmierne, a jakie nie. Zagadnienie to trzeba zawsze oceniać badając, czy konkretny, mający przeprowadzić identyfikację podmiot jest w stanie to zrobić w oparciu o dane będące przedmiotem rozważań. Jeżeli zatem lekarz w oparciu o pewne dane jest w stanie zidentyfikować osobę, której one dotyczą, to dane te dla tego lekarza są danymi osobowymi, jeżeli natomiast w oparciu o te same ktoś inny, nie jest w stanie zidentyfikować osoby, której dane dotyczą, to dla niego dane te danymi osobowymi nie są. Jak więc widać granice definicji ustawowej danych osobowych zakreślone są nieostro, co czasem, w sytuacji krytycznej może ochronić przed odpowiedzialnością, o czym warto pamiętać, choć nie należy na to liczyć.

W Polsce obowiązuje zakaz przetwarzania danych wrażliwych, czyli między innymi danych medycznych, rozumianych jako dane „o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym” [5].

Dane takie wolno jednak, w realiach medycznych, przetwarzać w oparciu o dopuszczenia wynikające z art. 27.2.7. ustawy o ochronie danych osobowych. Z tego artykułu wynika, że dane wrażliwe wolno jednak przetwarzać, o ile: „przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych”.

Dla jasności, by uniknąć mylenia opisanych wyżej danych z danymi medycznymi, które danymi osobowymi nie są, to np. statystyczne dane medyczne, jestem zwolennikiem używania określenia osobowe dane medyczne dla nazwania danych które są jednocześnie i danymi medycznymi i danymi osobowymi.

Kolejne ważne pojęcie, to pojecie przetwarzania danych osobowych.

Przetwarzaniem danych osobowych są jakiekolwiek operacje dokonywane na tych danych [6].

Podmiotem istotnym dla ochrony danych osobowych w każdym konkretnym przypadku przetwarzania tych danych jest administrator danych [7].

W realiach medycznych administratorem danych jest zwykle podmiot leczniczy, czyli na przykład: samodzielny publiczny zakład opieki zdrowotnej, spółka prowadząca przychodnie lub szpitale.

Podkreślenia wymaga fakt, że administratorami danych są wymienione podmioty, nie zaś kierujące nimi osoby fizyczne [8]. Osoba fizyczna może być administratorem danych, kiedy przetwarza dane osobowe niejako dla siebie, czy też we własnym imieniu.

Dobrym przykładem osoby fizycznej będącej administratorem danych jest lekarz prowadzący indywidualną praktykę medyczną.

Sam decyduje on o celu ich przetwarzania, jakim jest leczenie osób, których dane dotyczą. Lekarz wybiera także sposoby przetwarzania tych danych (np. w kartotekach, za pomocą systemu informatycznego). Nieco komplikuje się sytuacja, gdy lekarze prowadzą grupową praktykę lekarską. Można ją prowadzić w formie spółki cywilnej, spółki jawnej albo spółki partnerskiej [9]. W nauce prawa przyjmuje się, że administratorami danych osobowych są wspólnicy spółki cywilnej, a nie sama spółka cywilna [10]. Nie ma ona osobowości prawnej, gdyż nie może nabywać praw, zaciągać zobowiązań, ani pozywać lub pozywaną. Jest jedynie zespołem wspólników dążących do osiągnięcia wspólnego celu gospodarczego. W przypadku grupowej praktyki medycznej jest nim zarobkowanie poprzez świadczenie usług medycznych.

Każdy z lekarzy - wspólników, a nie sama spółka cywilna jest jednak, w świetle ustawy o swobodzie działalności gospodarczej, odrębnym przedsiębiorcą [11].

W konsekwencji uważa się, że to on decyduje o celach i środkach przetwarzania danych osobowych, a co za tym idzie każdy z lekarzy prowadzących grupową praktykę medyczną w formie spółki cywilnej jest administratorem danych osobowych.

Inaczej jest w przypadku spółki partnerskiej, która jest osobową spółką handlową. Posiada ona status przedsiębiorcy. Funkcjonuje w obrocie prawnym jako podmiot mogący nabywać prawa, zaciągać zobowiązania, pozywać i być pozywaną. Dlatego też należy uznać, że to spółka partnerska, a nie jej wspólnicy, jest administratorem danych osobowych. Podobnie rzecz się przedstawia ze spółką jawną [12].

Kolejnym ważnym podmiotem jest administrator bezpieczeństwa informacji.

Administrator danych wyznacza administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony, chyba, że sam wykonuje te czynności [13].

W realiach indywidualnej praktyki lekarskiej niekonieczne jest zatem wyznaczanie administratora bezpieczeństwa informacji, gdyż lekarz prowadzący taką praktykę może sam nadzorować przestrzeganie zasad ochrony. Inaczej jest w podmiocie leczniczym. Tam administratorem danych jest jednostka organizacyjna, a nie jeden człowiek, zatem osoba zarządzająca takim podmiotem powinna wyznaczyć administratora bezpieczeństwa informacji nadzorującego przestrzeganie zasad ochrony [14].

Upoważnienia do przetwarzania danych osobowych i ich ewidencja

Kluczowym dla ochrony osobowych danych medycznych zagadnieniem jest fakt iż „do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych” [15].

Można spierać się, czy upoważnienie to powinno zawierać szczegółowe wyliczenie czynności, do wykonywania których dana osoba jest upoważniona, czy też powinno mieć ono charakter ogólny, z odwołaniem się do zakresu czynności służbowych. Sporządzenie szczegółowego upoważnienia jest właściwsze z punktu widzenia bezpieczeństwa danych, należy jednak zawsze, przenosząc pracownika na inne stanowisko pracy, sprawdzać zakres wydanego mu uprzednio upoważnienia i ewentualnie zakres ten dostosowywać do nowej sytuacji. Nadanie pracownikowi upoważnienia o charakterze ogólnym, w którym upoważnia się go do przetwarzania danych osobowych w zakresie koniecznym do wykonywania czynności służbowych opisanych w zakresie obowiązków tego pracownika jest wygodne dla administratora danych. Może to jednak mieć zły wpływ na

bezpieczeństwo danych, ponieważ pracownik, któremu takowe upoważnienie nadano, może być fałszywie przeświadczony o tym, że jest upoważniony do dokonywania wszelkich czynności mających związek z danymi osobowymi.

Zlekceważenie obowiązku nadania upoważnień grozi administratorowi danych popełnieniem przestępstw: umożliwienia dostępu do danych osobie nieupoważnionej i udostępnienia danych osobowych osobie nieupoważnionej, zaś osobie która dane przetwarza grozi to popełnieniem przestępstwa przetwarzania danych osobowych, lub wrażliwych danych osobowych bez uprawnienia [16].

Na administratorze danych spoczywa również obowiązek prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych [17].

Prowadzić ją można zarówno w postaci zapisu na papierze, jak i w postaci zapisu w pamięci komputera. Może to być nawet baza danych, w której zapisane są uprawnienia poszczególnych użytkowników systemu informatycznego, w którym przetwarzane są dane. Ze względów bezpieczeństwa lepiej jednak ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzić w formie zapisu na papierze. Co więcej prowadzenie ewidencji w formie papierowej może pomóc ustrzec się przed pewnym błędem. Otóż administratorzy prowadzący ewidencje upoważnień w formie zapisu w pamięci komputera opisującego prawa dostępu do poszczególnych zbiorów danych zgromadzonych w tymże komputerze, zapominają o umieszczeniu w tej ewidencji również upoważnień dotyczących dostępu do danych przetwarzanych poza systemem informatycznym – na przykład podczas zbierania wywiadu przez lekarza. Ustawodawca nie sprecyzował też formy upoważnień.

Upoważnienie do przetwarzania danych osobowych jest aktem woli administratora tychże danych, na mocy którego to aktu, konkretna osoba fizyczna otrzymuje uprawnienie do przetwarzania danych osobowych.

Poza imieniem i nazwiskiem osoby upoważnionej upoważnienie zawiera zakres upoważnienia do przetwarzania danych osobowych. Upoważnienie nadane zostaje w konkretnej dacie, może ono z czasem ustać. Jeżeli dane przetwarzane są w systemie informatycznym, to częścią upoważnienia powinien być identyfikator. Dla celów dowodowych dobrze jest upoważnienia utrwalać na piśmie, lub chociaż w pamięci komputera. Jeśli się zrezygnuje z tej praktyki, to może się tak zdarzyć, że wszystkie wymienione powyżej elementy upoważnienia utrwalone zostaną jedynie w ewidencji upoważnień.

Pozostałe obowiązki dokumentacyjne

Obowiązki wynikające z opisywanej ustawy mogą się wydawać dziwne, zwłaszcza lekarzom, których zadaniem jest przede wszystkim leczenie pacjentów. Warto jednak by wypełnienia przedziwnych czasem wymagań ustawy nie traktować jak pustych obrzędów przed ołtarzem współczesnej Temidy, należy obowiązki te postrzegać jako narzędzia z pomocą których można lepiej chronić prawa i interesy pacjentów.

Podkreślenia wymaga, że niezależnie od prawnej formy działania czy wielkości, na każdym podmiocie przetwarzającym dane osobowe spoczywa obowiązek posiadania dokumentacji przetwarzania danych osobowych, czyli instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych i polityki bezpieczeństwa [18]. Polityka bezpieczeństwa i instrukcja, zawierające wyłącznie elementy wymienione w przepisach byłyby zgodne z prawem, ale z punktu widzenia bezpieczeństwa ułomne, powinny bowiem mieć one charakter szczegółowy [19]. Ponadto tworzenie tych

dokumentów warto wykorzystać jako okazję do analizy przetwarzania danych osobowych w jednostce.

Osoby zmarłe i nienarodzone

Ustawa o ochronie danych osobowych nie dotyczy osób zmarłych, chyba że z danych osoby zmarłej wynikają informacje dotyczące osób żyjących.

W istocie informacje te mimo, że niejako przypisane osobie zmarłej dotyczą w istocie osoby żyjącej, czyli osoby fizycznej. W ustawie nie unormowano zagadnienia danych dotyczących osób poczętych, ale jeszcze nieurodzonych.

Uważa się, że dane dotyczące osoby poczętej stają się danymi osobowym pod warunkiem, że urodzi się ona żywa i wtedy chronione są od momentu poczęcia.

Jednocześnie dane dotyczące osoby poczętej, która jednak nie urodziła się żywa danymi osobowymi nie są.

Nie znaczy to jednak, że dane w ogóle wyłączone są spod zakresu ochrony przewidzianego w ustawie o ochronie danych osobowych. Dane dotyczące płodu, który nie urodził się żywy są chronione, ponieważ są danymi osobowymi matki.

Jak chronić osobowe dane medyczne pacjentów

Posiadłszy wiedzę teoretyczną chciałoby się określić dokładnie jak w realiach medycznych chronić dane osobowe pacjentów. Zarówno ustawa o ochronie danych osobowych, jak i wydane na jej podstawie akty wykonawcze nie uczą nas precyzyjnie jak to czynić. Ustawa zobowiązuje administratora danych do „zastosowania środków technicznych i organizacyjnych zapewniających ochronę danych osobowych odpowiednią do zagrożeń i kategorii danych” [20]. Jest to sformułowanie, z którego nie wynika obowiązek wdrożenia konkretnych rozwiązań. Na jego podstawie można jednak np. stwierdzić, że przy dobieraniu środków ochrony danych osobowych przetwarzanych w podmiocie wykonującym działalność leczniczą trzeba mieć na uwadze fakt, iż przetwarza się tam osobowe dane medyczne, czyli dane należące do kategorii danych wrażliwych. Już w tym miejscu kwestia zabezpieczenia osobowych danych medycznych w gabinecie lekarskim jawi się jako problem, do którego rozwiązania potrzebna jest wiedza specjalistyczna. Większość administratorów danych osobowych nie ma takiej wiedzy. Najlepiej skorzystać więc z pomocy specjalistów zajmujących się bezpieczeństwem przetwarzania danych (nie tylko w systemach informatycznych), którzy wskażą odpowiednie rozwiązania. To oni są w stanie zalecić odpowiednie, dla konkretnego podmiotu rozwiązania.

Wśród zalecanych środków ochrony znajdą się:

- **przetwarzanie danych osobowych w pomieszczeniach z drzwiami zaopatrzonymi w zamki**
- **przechowywanie dokumentów i informatycznych nośników danych zawierających dane osobowe w szafach zamykanych na klucz**
- **używanie niszczarek do likwidowania dokumentów zawierających dane osobowe**
- **prowadzenie dokumentacji przetwarzania danych osobowych**
- **przeszkolenie osób zatrudnionych do pomocy w gabinecie w zakresie przetwarzania danych osobowych.**

W przypadku przetwarzania danych za pomocą systemu informatycznego wśród zalecanych środków ochrony będą:

- **rozpoczynanie pracy w systemie informatycznym po zalogowaniu się przez użytkownika za pomocą identyfikatora i co najmniej 8-znakowego hasła**
- **rejestrowanie poszczególnych logowań**
- **ustawienie monitorów komputerów za pomocą, których przetwarzane są dane osobowe w sposób uniemożliwiający zapoznanie się z danymi osobom postronnym**
- **zabezpieczanie komputerów stale aktualizowanymi programami antywirusowymi**
- **zabezpieczanie komputerów, zarówno sprzętowo, jak i programowo przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego**
- **podłączenie komputerów do urządzenia chroniącego przed utratą danych, którą może spowodować awaria zasilania lub zakłócenia w sieci**
- **usuwanie danych z informatycznych nośników wielokrotnego zapisu dokonywane za pomocą specjalistycznego oprogramowania.**

Trzeba mieć na uwadze to, że jest to jedynie wyliczenie przykładowe, a środki ochrony powinny być w każdym przypadku dobierane z uwzględnieniem specyfiki konkretnego podmiotu wykonującego działalność leczniczą [21].

Jeśli chodzi o realizację wymogów prawnych wynikających bezpośrednio z ustawy o ochronie danych osobowych, to by pokusić się o harmonogram wdrożenia przepisów można zaproponować następującą kolejność:

- **wydanie upoważnień do przetwarzania danych osobowych**
- **zaprowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych**
- **wyznaczenie administratora bezpieczeństwa informacji (nie w indywidualnej praktyce lekarskiej)**
- **sporządzenie polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych**
- **rejestracja posiadanych zbiorów danych osobowych, jeżeli są wykorzystywane w celu marketingowym.** □

Piśmiennictwo dostępne w redakcji

Adres autora: rzym@prawokomputerowe.pl www.prawokomputerowe.pl

Pracę nadesłano. 2012.02.18
Zaakceptowano do druku. 2012.03.18