Przetwarzanie danych osobowych w szpitalu – co nakazują, a czego zabraniają przepisy

Dane wrażliwe

Michał Sztąberek

Chciałbym się skupić na trzech zasadniczych sprawach. Pierwszą z nich jest ustalenie, jakie dane osobowe szpital na pewno może przetwarzać. Druga dotyczy kwestii zbierania dodatkowych danych. Trzeci zaś temat to wskazanie, jakich informacji szpital na pewno nie będzie mógł przetwarzać.

fot.123RF.com

Szpital jako zakład opieki zdrowotnej stanie się administratorem danych w rozumieniu ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (UODO). Oznacza to, że do działalności tego typu placówek zastosowanie będą miały zapisy tej ustawy, ale także przepisy szczególne, zwłaszcza gdy przepisy tych odrębnych ustaw przewidują dalej idącą ochronę, niż wynika to z UODO. Przepisy szczególne będą również niezwykle istotne w kontekście zbierania danych osobowych przez szpitale.

Dane zbierane przez szpital

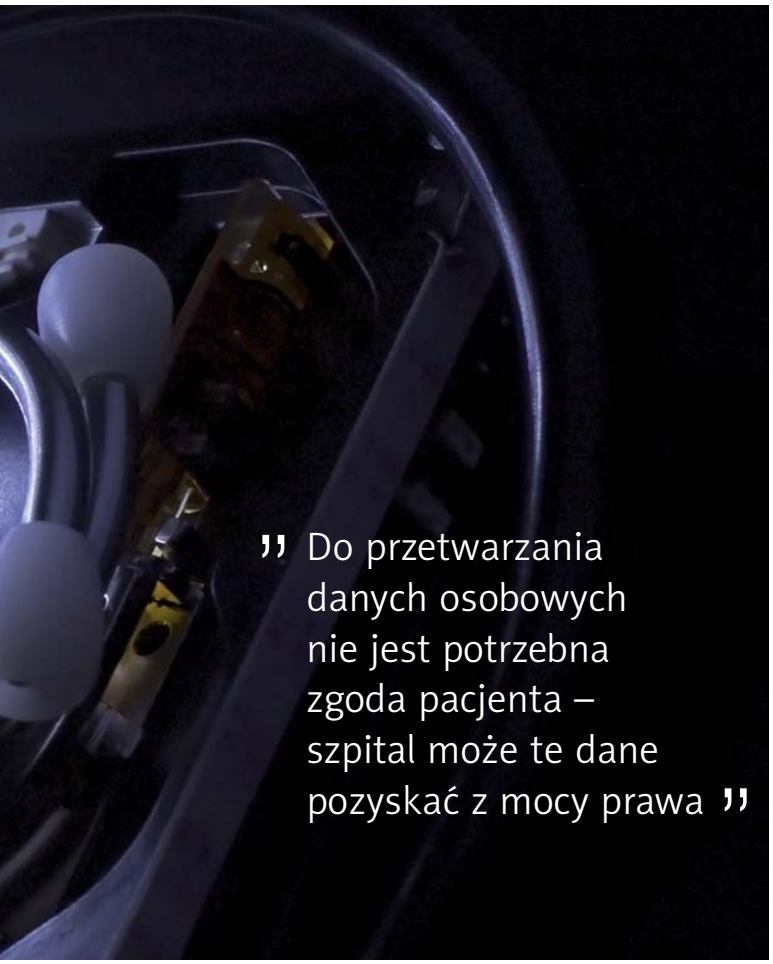
Jak zostało wskazane we wstępie, szpital musi przestrzegać takich samych reguł dotyczących przetwarzania danych osobowych jak każdy inny administrator danych. Oznacza to, że zastosowanie będą miały oba przepisy UODO, które regulują kwestię m.in. pozyskiwania danych osobowych, tj. art. 23 ust. 1 (który odnosi się do danych zwykłych, np. imię, nazwisko, numer PESEL, adres zamieszkania) oraz art. 27 ust. 2 (odnoszący się do danych wrażliwych, w tym zwłaszcza informacji o stanie zdrowia). Przyjrzyjmy się zatem bliżej tym przepisom.

Jeśli chodzi o art. 23 ust. 1 UODO, to przede wszystkim powinniśmy sięgnąć po przesłankę, zgodnie z którą przetwarzanie danych jest dopuszczalne, gdy jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Gdzie szukać tych przepisów? Przede wszystkim w ustawodawstwie „branżowym", czyli ustawie

z 31 sierpnia 1991 r. o zakładach opieki zdrowotnej, a także wydanym na podstawie art. 18 ust. 8 tej ustawy rozporządzeniu Ministra Zdrowia z 21 grudnia 2006 r. w sprawie rodzajów i zakresu dokumentacji medycznej w zakładach opieki zdrowotnej oraz sposobu jej przetwarzania.

Dane identyfikujące

Rozporządzenie, o którym mowa wyżej, reguluje m.in. kwestie danych zbieranych w ramach księgi



głównej przyjęć i wypisów, księgi oczekujących na przyjęcie do szpitala, księgi raportów pielęgniarskich, a także w ramach indywidualnej dokumentacji medycznej (wewnętrznej i zewnętrznej).

W tym kontekście najważniejsze wydaje się pojęcie danych identyfikujących, które pojawia się w wypadku każdej z wymienionych ksiąg, ale również w opisie indywidualnej dokumentacji (tam też wymieniono, jakie informacje składają się na dane identyfikujące). Przyjrzyjmy się zatem, jakie dane osobowe szpital na pewno może zbierać. Zgodnie z § 6 ust. 1 pkt 3 rozporządzenia na dane identyfikujące pacjenta składają się: imię (imiona) i nazwisko, data urodzenia, płeć, adres zameldowania, zamieszkania lub pobytu, numer PESEL (jeżeli został nadany), a w wypadku noworodka numer PESEL matki, gdyby natomiast nie było tego numeru – seria i numer dokumentu stwierdzającego tożsamość.

Warto w tym miejscu podkreślić, że do przetwarzania wyżej wymienionych informacji (będących niewątpliwie danymi osobowymi) nie jest potrzebna zgoda pacjenta, gdyż szpital może te dane pozyskać z mocy prawa (czyli wspomnianego wyżej przepisu).

Informacje o stanie zdrowia

W odniesieniu do danych wrażliwych, które obejmują informacje o stanie zdrowia (ale też np. o nałogach, które mogą mieć istotne znaczenie z punktu widzenia leczenia pacjenta), zastosowanie mają przepisy art. 27 ust. 2 UODO. Szybki przegląd wymienionych w nim przesłanek jednoznacznie wskazuje, że najlepszą będzie ta, która dopuszcza przetwarzanie danych, jeżeli jest ono prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, ale także zarządzania udzielaniem usług medycznych (działy administracyjne szpitali). Ponadto wymagana jest gwarancja ochrony danych osobowych przez ich administratora (jest o tym mowa m.in. we wspomnianym rozporządzeniu, gdzie zapisano, jak przechowywana ma być dokumentacja medyczna przetwarzana w formie tradycyjnej oraz elektronicznej).

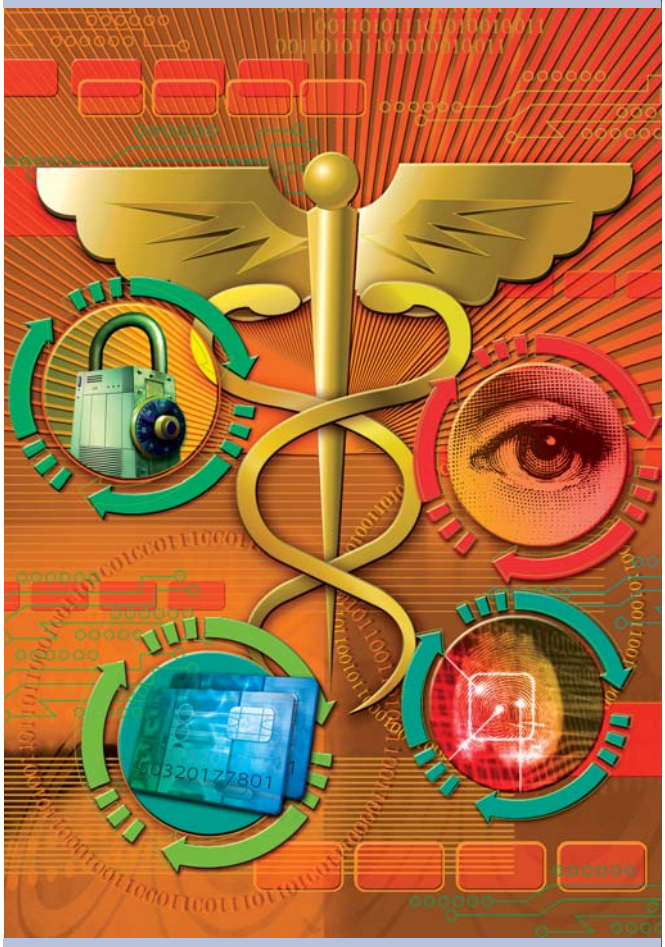
Szpitale idealnie wpisują się w powyższą definicję. Właśnie na podstawie tej przesłanki ich pracownicy (lekarze, pielęgniarki, kadra administracyjna) mogą przetwarzać dane osobowe, w szczególności informacje o stanie zdrowia (np. diagnoza choroby, jej przebieg, wcześniejsze schorzenia). Również w tym wypadku należy zaznaczyć, że do przetwarzania informacji o stanie zdrowia nie jest potrzebna pisemna (ani żadna inna) zgoda pacjenta bądź jego przedstawiciela ustawowego.

Na koniec tej części chciałbym nadmienić, że zgodnie z przywołanym wcześniej rozporządzeniem, można pozyskiwać dane od przedstawiciela ustawowego pacjenta, opiekuna lub innej osoby wskazanej przez pacjenta, umożliwiające pracownikom szpitala kontakt z nimi (imię i nazwisko oraz dane kontaktowe). Te same dane szpital może przetwarzać w odniesieniu do osób, które pacjent wskaże jako upoważnione do otrzymywania informacji o jego stanie zdrowia i udzielonych świadczeniach zdrowotnych.

Dane opcjonalne

Łatwo sobie wyobrazić sytuację, w której szpital będzie potrzebował innych informacji stanowiących dane osobowe niż te, na które zezwalają mu przepisy prawa. Tak może się zdarzyć, gdy placówka np. ma możliwość wykonywania pewnych zabiegów komer-

> Zbieranie dodatkowych danych przez szpital zawsze musi się odbywać zgodnie z dwoma zasadami – legalności oraz adekwatności



fot. Images.com/Corbis

> Jeśli szpital będzie w stanie powołać się na odpowiednią przesłankę i spełnić inne zobowiązania wskazane w UODO, nie ma powodów do obaw, że nagle okaże się, że przetwarzanie danych odbywa się nielegalnie

cyjnie. Wówczas może chcieć zbierać dane do celów marketingowych.

Zbieranie dodatkowych danych przez szpital zawsze musi się odbywać według dwóch zasad – legalności i adekwatności (oraz przy założeniu, że spełnione są inne wymogi wskazane w UODO, np. obowiązki informacyjne). Ta pierwsza oznacza oparcie przetwarzania danych na jednej z przesłanek wskazanych we wspomnianych już przeze mnie przepisach, tj. art. 23 ust. 1 (dane zwykłe) albo art. 27 ust. 2 (dane wrażliwe) UODO. Jeśli mówimy o celu marketingowym, do którego zrealizowania szpital będzie wykorzystywał np. dane kontaktowe pacjentów, to – w zależności od tego, jak ten cel ma być osiągnięty (czy marketing będzie polegał np. na wysłaniu ofert listownie czy w formie e-maili) – zasadne wydaje się skorzystanie ze zgody na przetwarzanie danych osobowych (art. 23 ust. 1 pkt. 1 UODO; zwłaszcza jeśli marketing będzie miał postać wysyłki mailowej) albo można będzie powołać się na usprawiedliwiony cel administratora danych (tu: marketing bezpośredni własnych produktów i usług – art. 23 ust. 1 pkt. 5 UODO).

Druga z zasad nakazuje natomiast administratorowi zbieranie tylko tych danych osobowych, które są niezbędne do osiągnięcia zakładanego celu. Nie można zatem gromadzić wszystkich informacji, w tym zwłaszcza takich, które być może przydadzą się w przyszłości. Warto w tym miejscu nadmienić, że kwestia adekwatności – podobnie jak legalności pozyskania danych osobowych – zawsze bywa skrupulatnie sprawdzana przez GIODO, czy to w trakcie weryfikacji wniosku rejestracyjnego zbioru danych, czy podczas kontroli bezpośredniej.

Czego nie wolno

Trudno jest stworzyć precyzyjny katalog informacji stanowiących dane osobowe, których szpital nie powinien przetwarzać. Jak wspomniano powyżej, istnieje wiele przesłanek umożliwiających gromadzenie zarówno danych zwykłych, jak i wrażliwych. Jeśli szpital będzie w stanie powołać się na którąś z nich, a także wypełnić inne zobowiązania wskazane w UODO (np. zasada adekwatności), raczej nie ma powodów do obaw, że nagle okaże się, że przetwarzanie danych odbywa się niezgodnie z przepisami. Każda taka sytuacja wymaga oczywiście szczegółowej analizy i musi być traktowana indywidualnie, by móc stwierdzić, że podejmowane czynności są wykonywane w duchu UODO.

Konkludując, chciałbym podkreślić, że szpitale, jak każdy administrator danych, muszą działać zgodnie z wymogami UODO, przy czym – jako że działalność tych placówek regulowana jest wieloma przepisami szczególnymi – zawsze trzeba mieć na uwadze wskazane w nich wyjątki lub modyfikacje podstawowych reguł.

Autor jest prawnikiem i audytorem, partnerem zarządzającym w iSecure Sp. z o.o., firmie specjalizującej się w doradztwie w zakresie ochrony danych osobowych.