Jak bezpiecznie przetwarzać dane pacjentów

Chroń dane pacjenta swego **jak siebie samego**

Fot. iStockphoto.com

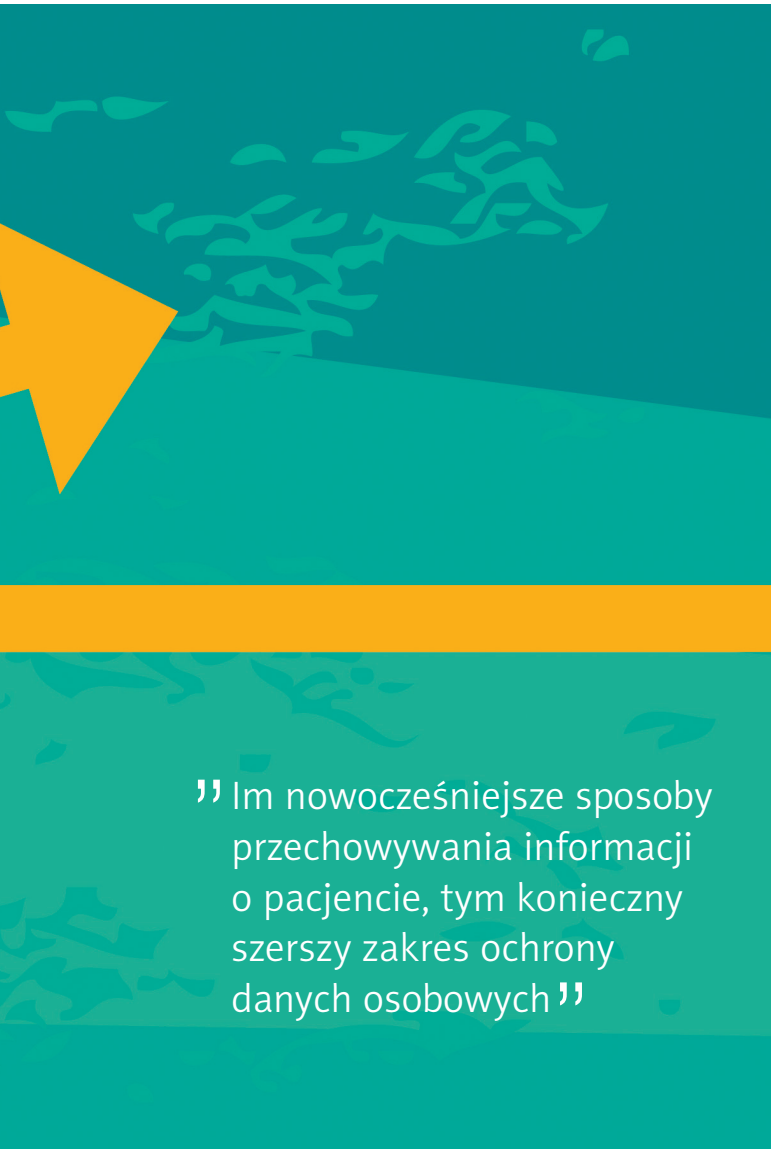
Dla prowadzenia podmiotu leczniczego, czy to w ramach gabinetu lekarskiego, przychodni, czy szpitala, niezbędne jest przetwarzanie danych osobowych pacjentów. Jak to zrobić, żeby nie narazić się na konsekwencje prawne?

Od początku. Pojęcie danych osobowych jest szerokie i obejmuje „wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej". W kontekście działalności medycznej danymi osobowymi będą zatem wszelkie informacje o pacjencie zawarte w dokumentacji medycznej umożliwiające jego identyfikację. Dane te to m.in. imię i nazwisko, PESEL i płeć, ale w kontekście pacjenta – przede wszystkim dane wrażliwe, dotyczące stanu zdrowia i świadczeń medycznych, których mu udzielono. Jak wskazuje sama nazwa, dane te wymagają specjalnego traktowania, w tym odpowiedniej ochrony, co w konsekwencji powoduje nałożenie na podmiot leczniczy szczególnych obowiązków.

Wspomniany obowiązek ochrony zgromadzonych danych osobowych pacjentów wynika z faktu, iż podmioty lecznicze przetwarzają je w ramach prowadzonej przez siebie działalności. Tymczasem definicja przetwarzania jest bardzo szeroka, obejmuje bowiem każdą operację na danych, m.in. zbieranie, utrwalanie, przechowywanie, udostępnianie, modyfikację, usuwanie. Bez wątpienia każdy podmiot świadczący usługi medyczne dokonuje tych czynności, co w świetle przepisów ustawy o ochronie danych osobowych czyni go administratorem danych.

Zgodnie z prawem ochrona danych pacjentów to świętość

Zarówno pojęcie danych osobowych, jak i ich przetwarzania są bardzo szerokie. Konsekwencją takiego uregulowania prawnego jest również rozlegle rozumia-



na ochrona danych, która implikuje konieczność stosowania odpowiednich środków przez podmiot przetwarzający dane osobowe.

Kompleksowa analiza wspomnianych wyżej pojęć prowadzi do wniosku, iż administratorem danych będzie zarówno lekarz w gabinecie lekarskim, jak i spółka prowadząca działalność leczniczą. To właśnie na administratorze ciąży ustawowy obowiązek zastosowania odpowiednich środków (technicznych i organizacyjnych) zapewniających odpowiednią ochronę przetwarzanych danych osobowych, rozumianą jako dostosowaną do zagrożeń oraz kategorii danych podlegających ochronie. Innymi słowy, należy zabezpieczyć dane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, przetwarzanie ich w sposób naruszający ustawę oraz ich zmianę, uszkodzenie i zniszczenie.

Jak wskazuje praktyka, im nowocześniejsze sposoby przechowywania informacji o pacjencie, np. elektroniczna baza pacjentów, tym konieczny jest szerszy zakres ochrony danych osobowych – bardziej rozbudowany niż w przypadku gabinetu lekarskiego, w którym lekarz prowadzi dokumentację w formie papierowej i nie zatrudnia personelu medycznego.

Jak chronić dane pacjentów?

Podmiot świadczący usługi medyczne jako administrator danych jest zobligowany do prowadzenia dokumentacji opisującej sposób ich przetwarzania oraz do podjęcia środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych informacji o pacjentach. Przepisy prawa dają również możliwość wyznaczenia administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony w danym podmiocie, co pozwala na delegację obowiązków. W przypadku niepowołania administratora bezpieczeństwa podmiot świadczący usługi medyczne jest zobowiązany sam wykonywać jego zadania, polegające na sprawdzaniu zgodności przetwarzania danych osobowych z przepisami ustawy, nadzorowaniu opracowywania i aktualizacji dokumentacji i przestrzeganiu zasad w niej określonych oraz zapoznaniu z nimi osób upoważnionych do ich przetwarzania w zgodzie z przepisami.

Kompleksowa analiza przepisów związanych z ochroną danych pacjentów przez podmiot świadczący usługi medyczne wskazuje, iż powinien on jako administrator:

- sporządzić i wprowadzić do stosowania Politykę bezpieczeństwa informacji oraz w przypadku dokumentacji prowadzonej w formie elektronicznej Instrukcję zarządzania systemem informatycznym,
- prowadzić Ewidencję osób upoważnionych do przetwarzania danych, czyli personelu, który przetwarza dane osobowe pacjentów, oraz wprowadzić imienne upoważnienia uprawniające do dostępu do danych osobowych z określeniem zakresu tego dostępu,
- informować pacjentów o nazwie praktyki, jej adresie, celu zbierania danych osobowych, prawie dostępu do treści i zmiany swoich danych, a zatem niezbędne jest szkolenie personelu w tym zakresie.

Podstawowe dokumenty związane z ochroną danych

Polityka bezpieczeństwa informacji jest dokumentem podstawowym w zakresie ochrony danych osobowych pacjentów. Dokument ten jest zbiorem spójnych, precyzyjnych reguł i procedur, według których dany podmiot leczniczy organizuje, zarządza oraz udostępnia dane osobowe. Określa ona, które dane i w jaki sposób mają być chronione. Polityka powinna zawierać w szczególności wykaz pomieszczeń, w których przetwarzane są dane osobowe, wskazywać zbiory danych wraz z informacją o sposobie ich przetwarzania, opis struktury danych dokumentacji medycznej, który określa, jakie pola informacyjne wypełnia pacjent, sposób przepływu danych pomiędzy poszczególnymi sys-

temami, środki techniczne i organizacyjne niezbędne do zapewnienia odpowiedniej ochrony przetwarzanych danych.

E-dokumentacja

W przypadku, gdy dokumentacja medyczna prowadzona jest w formie elektronicznej, niezbędne jest przygotowanie także Instrukcji zarządzania systemem, w której należy wskazać: zasady nadawania uprawnień do przetwarzania danych osobowych, sposób kontroli dostępu osób uprawnionych do kontroli, procedurę rozpoczęcia, zawieszenia i zakończenia pracy programu komputerowego, który służy do przetwarzania danych osobowych, procedurę wykonywania kopii zapasowych danych oraz sposób zabezpieczenia programu przed ingerencją osób trzecich lub złośliwego oprogramowania.

Dodatkowo niezwykle istotne jest wdrożenie środków technicznych w celu zabezpieczenia obszaru przetwarzania danych osobowych przed dostępem osób nieupoważnionych, przykładowo: systemów podtrzymywania, „silnego" hasła dostępu, szyfrowania danych w przypadku przesyłania ich za pośrednictwem publicznej sieci internetowej.

W zakresie bardzo szerokich obowiązków związanych z przetwarzaniem danych osobowych ustawodawca zwolnił podmioty lecznicze z obowiązku:

- uzyskiwania zgody pacjentów na przetwarzanie danych (co nie uchyla obowiązku informacyjnego wobec nich),
- rejestracji zbioru danych osobowych pacjentów korzystających z usług medycznych dla Generalnego Inspektora Ochrony Danych Osobowych (dalej: GIODO).

Jednocześnie należy podkreślić, że jeżeli zbiór danych jest w podmiocie leczniczym wykorzystywany również do innych celów niż świadczenie usług medycznych, obowiązek zgłoszeniowy istnieje.

Ochrona danych osobowych a GIODO

Generalny Inspektor Ochrony Danych Osobowych to podmiot powołany do badania zgodności przetwarzania danych osobowych z przepisami prawa. Tym samym, jeżeli w wyniku przeprowadzonej kontroli zostanie stwierdzone naruszenie przepisów, GIODO w drodze decyzji administracyjnej nakazuje w pierwszej kolejności przywrócenie stanu zgodnego z prawem, m.in. poprzez usunięcie uchybień, zastosowanie dodatkowych środków zabezpieczających lub przekazanie ich innym podmiotom. Inspektor może żądać także wszczęcia postępowania dyscyplinarnego lub innego przewidzianego prawem postępowania przeciwko osobom winnym dopuszczenia uchybień i poinformowania go w określonym terminie o wynikach i podjętych działaniach. Z kolei w przypadku stwierdzenia, że działanie lub zaniechanie administratora danych wyczerpuje znamiona przestępstwa określonego w ustawie, GIODO jest zobowiązany skierować zawiadomienie o popełnieniu przestępstwa do organu powołanego do ścigania przestępstw, dołączając dowody dokumentujące podejrzenie.

Konsekwencje prawne

Przetwarzając dane osobowe pacjentów w sposób niezgodny z obowiązującymi przepisami, można się narazić na konsekwencje prawne w postaci sankcji o charakterze zarówno administracyjnym, jak i karnym. Ustawodawca wprowadził szczególne rodzaje przestępstw polegające na:

- przetwarzaniu danych osobowych, których przetwarzanie nie jest dopuszczalne albo do których przetwarzania osoba nie jest uprawniona,
- udostępnieniu lub umożliwieniu dostępu do danych osobowych osobom nieupoważnionym,
- naruszeniu, choćby nieumyślnie, obowiązku zabezpieczenia danych przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem,
- niepoinformowaniu osoby, której dane są przetwarzane, o jej prawach wynikających m.in. z ustawy o ochronie danych osobowych.

Powyższe przestępstwa zagrożone są surowymi karami – przykładowo, w przypadku popełnienia pierwszego z nich jest to nawet pozbawienie wolności do lat trzech.

W zakresie możliwości nakładania przez GIODO kar administracyjnych należy wspomnieć, iż posiada on także uprawnienia organu egzekucyjnego. Również te kary mogą być dla podmiotu leczniczego dotkliwe, bowiem:

- za każde uchybienie kara może wynieść nawet do 10 000 zł w przypadku osoby fizycznej (lekarza), a w przypadku osoby prawnej (np. spółki z o.o.) 50 000 zł;
- łącznie za wszystkie uchybienia kara nie może przekroczyć 50 000 zł w przypadku osoby fizycznej (lekarza), a w przypadku osoby prawnej (np. spółki z o.o.) 200 000 zł.

Wachlarz sankcji, zarówno finansowych, jak i związanych z odpowiedzialnością osobistą, wskazuje, jak ważne dla podmiotu leczniczego powinno być zadbanie o prawidłową ochronę danych osobowych. Nie należy lekceważyć obowiązków nakładanych przez przepisy prawa, albowiem koszty nałożonych sankcji mogą być wyższe niż te związane z prawidłowym wdrożeniem metod ochrony danych osobowych. Warto również skorzystać z pomocy profesjonalistów przy sporządzaniu koniecznej dokumentacji, aby sprostać wymaganiom przepisów ustawodawczych oraz wykonawczych i zapewnić bezpieczeństwo własne i prowadzonej bądź zarządzanej przez siebie działalności leczniczej.

Monika Błońska
Autorka jest radcą prawnym
z Mariański Group Kancelaria Prawno-Podatkowa.