Prawo w pigułce

PAWELCZYK KOZIK | KANCELARIA RADCÓW PRAWNYCH

Krzysztof Kozik
radca prawny
e-mail: k.kozik@pawelczyk-kozik.pl

Wiktor Dymecki
ekspert ds. podatków
e-mail: b.pawelczyk@pawelczyk-kozik.pl

Ochrona informacji o pacjencie

Ochrona informacji dotyczących pacjenta i udzielanych mu świadczeń zdrowotnych stanowi bardzo istotny wymóg. Coraz większą wagę przywiązują do jego przestrzegania nie tylko sami pacjenci, lecz także organy państwowe, w tym Generalny Inspektor Ochrony Danych Osobowych. Kontrole ze strony tego urzędu, dotąd raczej sporadyczne, zdarzają się coraz częściej, a – co więcej – część uprawnień kontrolnych w tym względzie posiada także Państwowa Inspekcja Pracy. Dlatego uznaliśmy za celowe, aby przypomnieć – z konieczności jedynie w zarysie – wymogi prawne, które dotyczą tej bardzo ważnej problematyki.

Prawo pacjenta do informacji o swoim stanie zdrowia

Jednym z podstawowych praw pacjenta, uregulowanym w ustawie o prawach pacjenta i Rzeczniku Praw Pacjenta, jest prawo do informacji o swoim stanie zdrowia. Przysługuje ono nie tylko pacjentom pełnoletnim, lecz także małoletnim, którzy ukończyli 16 lat (oraz ich przedstawicielom ustawowym). Osoby te mają prawo do uzyskania od lekarza przystępnej informacji o stanie zdrowia pacjenta, rozpoznaniu, proponowanych oraz możliwych metodach diagnostycznych i leczniczych, dających się przewidzieć następstwach ich zastosowania albo zaniechania, wynikach leczenia oraz rokowaniu. Trzeba tu przypomnieć, że inne osoby będą miały prawo do uzyskania takiej informacji tylko i wyłącznie wówczas, gdy pacjent ich do tego upoważni. Zatem sam fakt bycia członkiem rodziny nie upoważnia automatycznie do uzyskiwania takich informacji. Zgodnie z rozporządzeniem Ministra Zdrowia w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania, obligatoryjnie w dokumentacji indywidualnej wewnętrznej zamieszcza się lub dołącza do niej oświadczenie pacjenta o upoważnieniu osoby bliskiej do uzyskiwania informacji o jego stanie zdrowia i udzielonych świadczeniach zdrowotnych, ze wskazaniem imienia i nazwiska osoby upoważnionej oraz danych umożliwiających kontakt z tą osobą, albo oświadczenie o braku takiego upoważnienia. Zatem odebranie takiego oświadczenia jest koniecznością, a udzielenie informacji o stanie zdrowia pacjenta osobie nieupoważnionej stanowi bardzo poważne naruszenie praw pacjenta i może rodzić odpowiedzialność prawną.

Prawo pacjenta do zachowania tajemnicy lekarskiej

Z powyższym prawem do informacji o stanie zdrowia ściśle wiąże się prawo pacjenta do zachowania w tajemnicy przez osoby wykonujące zawód medyczny, w tym udzielające mu świadczeń zdrowotnych, informacji z nim związanych, a uzyskanych w związku z wykonywaniem zawodu medycznego. Tajemnicą lekarską objęte są więc nie tylko informacje dotyczące zdrowia pacjenta, ale wszelkie uzyskane od pacjenta – np. związane z sytuacją rodzinną czy finansową. Zwolnienie z tajemnicy lekarskiej może nastąpić tylko w sytuacjach określonych przepisami prawa, m.in. gdy pacjent lub jego przedstawiciel ustawowy wyraża zgodę na ujawnienie tajemnicy, gdy zachowanie tajemnicy może stanowić niebezpieczeństwo dla życia lub zdrowia pacjenta lub innych osób czy gdy zachodzi potrzeba przekazania niezbędnych informacji o pacjencie związanych z udzielaniem świadczeń zdrowotnych innym osobom wykonującym zawód medyczny, uczestniczącym w udzielaniu tych świadczeń. Osoby wykonujące zawód medyczny są związane tajemnicą również po śmierci pacjenta.

Polityka bezpieczeństwa informacji

Informacje dotyczące stanu zdrowia pacjentów stanowią tzw. dane wrażliwe, wobec których znajdują zastosowanie przepisy ustawy o ochronie danych osobowych i rozporządzenia wydane na jej podstawie. Każdy podmiot wykonujący działalność leczniczą pełni zatem z tego tytułu funkcję administratora danych, co z kolei rodzi szereg obowiązków. Administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były:

1) przetwarzane zgodnie z prawem,
2) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Wymaga szczególnego podkreślenia, że administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych od-

powiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Ponadto administrator danych zobowiązany jest prowadzić w formie pisemnej dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa powyżej. Na taką dokumentację składa się polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Pełen wykaz informacji objętych powyższymi dokumentami został uregulowany w rozporządzeniach. Poniżej wskazujemy jedynie wybrane spośród nich. Polityka bezpieczeństwa musi zawierać m.in.:

1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
4) sposób przepływu danych pomiędzy poszczególnymi systemami;
5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Z kolei instrukcja zarządzania systemem informatycznym musi obejmować w szczególności:

1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
5) sposób, miejsce i okres przechowywania:
   a) elektronicznych nośników informacji zawierających dane osobowe,
   b) kopii zapasowych,
6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania;
7) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Stworzenie powyższych dokumentów jest obowiązkowe dla każdego podmiotu wykonującego działalność leczniczą. Ponadto podmioty te – jako administratorzy danych – mogą, ale nie muszą powołać administratora bezpieczeństwa informacji oraz administratora systemów informatycznych. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby mające upoważnienie nadane przez administratora danych. Administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

Powyższe wymogi muszą zostać przełożone na organizację i funkcjonowanie każdego podmiotu wykonującego działalność leczniczą.