VIA MEDICA

Ginekologia i Perinatologia Praktyczna 2017
tom 2, nr 1, strony 22–23

ISSN 2451–0122

GIODO skontroluje poziom ochrony danych osobowych w podmiotach leczniczych

The inspection of the quality of personal data protection in healthcare entities

Zakres kontroli

Generalny Inspektor Ochrony Danych Osobowych (GIODO) przedstawił ostatnio plan kontroli sektorowych na 2017 rok. Celem ich przeprowadzenia jest sprawdzenie, czy dana kategoria podmiotów przestrzega, w ramach swojej działalności, właściwych standardów ochrony danych osobowych oraz czy stosuje przewidziane prawem procedury ich przetwarzania. Zgodnie z przedstawionym planem w tym roku kontrolą zostaną objęte podmioty działające w sektorze ochrony zdrowia. Mając na uwadze specyfikę działalności tych placówek, chcielibyśmy w niniejszym artykule pokrótce wskazać na najistotniejsze kwestie praktyczne, na które właściciele podmiotów leczniczych powinni zwrócić uwagę przed ewentualną wizytą inspektora.

Planem kontroli zostały objęte zarówno publiczne, jak i prywatne przychodnie i poradnie lekarskie, które zostaną sprawdzone pod kątem wywiązywania się z ustawowych obowiązków przestrzegania przepisów o ochronie danych osobowych. Zgodnie z zapowiedziami GIODO przedmiotem kontroli zostanie objęty przede wszystkim sposób rejestracji pacjentów w przychodni lub poradni lekarskiej. Jest to uzasadniane koniecznością sprawdzenia, czy ww. podmioty zapewniają warunki właściwe dla poszanowania prywatności oraz czy zapewniają odpowiedni stopień poufności na etapie podawania danych osobowych.

Warto zwrócić uwagę, że to właśnie liczne skargi pacjentów stały się przyczyną tak sprecyzowanej kontroli. Pacjenci dostrzegają istotny problem, jakim jest konieczność podawania przy rejestracji danych często w obecności postronnych osób trzecich. Podmioty działające w sektorze ochrony zdrowia każdego dnia zbierają i utrwalają nie tylko standardowe dane osobowe pacjentów, takie jak imię, nazwisko czy data urodzenia, ale również informacje o stanie zdrowia, historii chorób, przyjmowanych lekach czy przebytych zabiegach. Jest to o tyle istotne, że dane związane ze stanem zdrowia należą do kategorii danych sensytywnych, a co za tym idzie podlegają ostrzejszemu reżimowi prawnemu i dodatkowym obostrzeniom, czego celem jest zapewnienie odpowiednio wysokiej ochrony dla tej kategorii informacji o pacjencie.

Podmiot leczniczy, który zostanie poddany kontroli GIODO, może się spodziewać, że inspektorzy sprawdzą między innymi następujące kwestie:

- przebieg rejestracji pacjentów, w tym zastosowane środki techniczne oraz organizacyjne mające umożliwić podawanie danych osobowych w sposób zapewniający zachowanie poufności:
  - na przykład może zostać zweryfikowane, czy podczas podawania danych osobowych pacjent jest narażony na to, że usłyszą je osoby trzecie oraz czy przy ich wprowadzaniu do systemu przez obsługę nie będą one widoczne na monitorach dla osób trzecich, lub czy na stanowisku, przy którym rejestrują się pacjenci, nie znajdują się dokumenty zawierające dane osobowe innych pacjentów;
- wdrożenie oraz stosowanie środków technicznych niezbędnych do zapewnienia bezpieczeństwa przetwarzania danych osobowych pacjentów, a w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
- fakt posiadania przez pracowników oddelegowanych do zadań związanych z przetwarzaniem danych osobowych (np. pracownicy rejestracji) stosownych upoważnień nadanych im przez administratora danych oraz prowadzenie ewidencji tych osób, a w tym:
  - czy zostały zawarte odpowiednie umowy z pracownikami IT oraz pracownikami rejestracji,
  - czy upoważnienia dla pracowników do przetwarzania danych osobowych zostały udzielone w odpowiedniej formie,

Adres do korespondencji: adw. Oskar Luty, Kancelaria DFL LEGAL, tel. 22 616 41 41, 505 422 382, e-mail: oskar.luty@dfl-legal.pl

  - czy w przypadku lekarzy będących na kontrakcie zastosowano prawidłowe rozdzielenie funkcji dotyczącej przetwarzania danych osobowych;
- znajomość przepisów o ochronie danych osobowych przez osoby upoważnione do ich przetwarzania.

Uprawnienia GIODO w ramach kontroli

Generalny Inspektor Ochrony Danych Osobowych posiada szerokie uprawnienia kontrolne. Ma prawo wstępu na teren objęty kontrolą oraz może ponadto żądać złożenia wyjaśnień, a także wzywać i przesłuchiwać pracowników. Jest również uprawiony do wglądu do wszelkich dokumentów i danych mających bezpośredni związek z przedmiotem kontroli oraz sporządzania ich kopii, jak również przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych, czy też do zlecania sporządzania ekspertyz i opinii.

Zasadą jest, że kontrole są zapowiadane z kilkudniowym wyprzedzeniem, w pierwszej kolejności telefonicznie, a następnie na piśmie. Inspektor określa również ogólny przedmiot kontroli, dokładny jej termin oraz zwraca się z prośbą o przygotowanie stosownej dokumentacji. Podmiot kontrolowany ma zatem zaledwie kilka dni na „przygotowanie się" do wizyty inspektorów, co z pewnością nie jest wystarczającym czasem na wdrożenie stosownych zmian. Dlatego już na tym etapie warto zastanowić się nad poprawnością przetwarzania danych osobowych w podmiocie leczniczym i dostosowaniem systemu funkcjonowania przychodni do obowiązujących regulacji prawnych. Jest to szczególnie istotne również dlatego, że brak zawiadomienia nie może stanowić podstawy odmowy dopuszczenia inspektora do przeprowadzenia kontroli. Jedynie brak stosownego upoważnienia i legitymacji inspektora uzasadnia nieudzielenie zgody na ich wstęp.

Skutki stwierdzenia naruszeń przepisów o ochronie danych osobowych

Jeżeli kontrola uwidoczni nieprawidłowości w zakresie przetwarzania danych osobowych przez podmiot leczniczy, inspektor w pierwszej kolejności nakaże wdrożenie rozwiązań, które usuną zaobserwowane naruszenia. Podmiot kontrolowany będzie wówczas zobowiązany do naprawienia zaistniałych uchybień. Inspektor może również nakazać zastosowanie dodatkowych środków zabezpieczających albo polecić zabezpieczenie danych, a w szczególnych wypadkach nawet ich usunięcie.

W przypadku wykrycia naprawdę poważnych nieprawidłowości GIODO może skierować sprawę do prokuratury. W takich przypadkach rośnie prawdopodobieństwo nałożenia przez sąd na podmiot leczniczy sankcji karnych w postaci grzywny, kary ograniczenia wolności lub nawet kary pozbawienia wolności.

Należy podkreślić, że dostosowanie wewnętrznych procedur i zasad przetwarzania danych osobowych do obowiązujących przepisów już teraz leży w interesie podmiotów działających w sektorze ochrony zdrowia, ponieważ w maju 2018 roku zacznie obowiązywać unijne rozporządzenie ujednolicające przepisy o ochronie danych osobowych. Nowe regulacje wprowadzą o wiele bardziej dotkliwe sankcje dla podmiotów przetwarzających dane osobowe niezgodnie z wymogami, zaś cały rygor przetwarzania danych osobowych ulegnie zaostrzeniu. Przyjrzenie się wewnętrznym procedurom funkcjonowania placówki ochrony zdrowia jest więc nieuniknione — dlatego warto to zrobić już teraz i nie narażać się na nieprzyjemności związane z negatywnym wynikiem ewentualnej kontroli.

adw. Oskar Luty, Natalia Łukawska
Specjalistyczna kancelaria prawnicza DFL LEGAL
prowadząca obsługę prawną Polskiego Towarzystwa Ginekologicznego