Ochrona danych osobowych w gabinecie lekarskim

W związku z wieloma pytaniami dotyczącymi opracowania polityki bezpieczeństwa w gabinetach lekarskich przedstawiamy wyciąg z opinii prawnej sporządzonej przez prawnika WIL, adwokat Urszulę Nowaczyk.

Zgodnie z ustawą z 15 kwietnia 2011 r. o działalności leczniczej (Dz.U. 2013, poz. 217 t.j.), działalność lecznicza polega na udzielaniu świadczeń zdrowotnych (art. 3 ust. 1). Z kolei świadczenie zdrowotne to działania, które służą zachowaniu, ratowaniu, przywracaniu lub poprawie zdrowia oraz inne działania medyczne wynikające z procesu leczenia lub przepisów odrębnych regulujących zasady ich wykonywania (art. 2 ust. 1 pkt 10). Stosownie zaś do art. 4 ust. 1 tej ustawy podmiotami leczniczymi są:

- przedsiębiorcy w rozumieniu przepisów ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej we wszelkich formach przewidzianych dla wykonywania działalności gospodarczej, jeżeli ustawa nie stanowi inaczej,
- samodzielne publiczne zakłady opieki zdrowotnej,
- jednostki budżetowe, w tym państwowe jednostki budżetowe tworzone i nadzorowane przez ministra obrony narodowej, ministra właściwego do spraw wewnętrznych, ministra sprawiedliwości lub szefa Agencji Bezpieczeństwa Wewnętrznego, posiadające w strukturze organizacyjnej ambulatorium, ambulatorium z izbą chorych lub lekarza podstawowej opieki zdrowotnej,
- instytuty badawcze, o których mowa w art. 3 ustawy z 30 kwietnia 2010 r. o instytutach badawczych,
- fundacje i stowarzyszenia, których celem statutowym jest wykonywanie zadań w zakresie ochrony zdrowia i których statut dopuszcza prowadzenie działalności leczniczej,
- kościoły, kościelne osoby prawne lub związki wyznaniowe

– w zakresie, w jakim wykonują działalność leczniczą.

W związku z działalnością leczniczą przetwarzane są dane osobowe oraz tworzone zbiory danych osobowych pacjentów. Na podstawie art. 40 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2002 Nr 101 poz. 926 j.t.), administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków, o których mowa w jej art. 43 ust.1. Zgodnie zaś z art. 43 ust. 1 pkt 5, z obowiązku rejestracji zbioru danych zwolnieni są administratorzy danych dotyczących osób korzystających z ich usług medycznych.

Zatem nie podlega obowiązkowi zgłoszenia do rejestracji zbiór danych pacjentów, którym udzielane są świadczenia zdrowotne przez podmioty wymienione w ustawie o działalności leczniczej. Zgodnie z art. 43 ust. 1 pkt 5 ustawy o ochronie danych osobowych, zbiór danych osób korzystających z usług medycznych świadczonych przez konkretnego administratora danych jest wyłączony spod obowiązku zgłaszania do GIODO. Należy jednak pamiętać, że wyłączenie z obowiązku zgłaszania zbioru danych do rejestracji nie oznacza wyłączenia spod obowiązku odpowiedniego zabezpieczenia danych oraz ujęcia takiego zbioru w wewnętrznej dokumentacji przetwarzania danych osobowych.

Odnosząc się do obowiązku sporządzania polityki bezpieczeństwa, należy także zauważyć, że ustawa o systemie informacji w ochronie zdrowia w art. 2 pkt 1 posługuje się definicją „administratora danych" zaczerpniętą wprost z ustawy o ochronie danych osobowych.

Danymi osobowymi są także dane zatrudnianych pracowników – i choć nie trzeba „zbioru danych osobowych pracowników" zgłaszać do GIODO (z uwagi na wyłączenie zawarte w art. 43 ust. 1 pkt 4 ustawy o ochronie danych osobowych), to taki zbiór danych również należy przetwarzać zgodnie z ustawowym trybem, a więc odpowiednio zabezpieczyć oraz ująć w polityce bezpieczeństwa.

Do najważniejszych dokumentów, jakie musi posiadać i prowadzić każdy administrator danych osobowych, należy zaliczyć:

- politykę bezpieczeństwa,
- instrukcję zarządzania systemem informatycznym (służącym do przetwarzania danych osobowych),
- ewidencję osób upoważnionych do przetwarzania danych.

Jeżeli chodzi o politykę bezpieczeństwa, powinna ona zawierać, z godnie z § 4 rozporządzenia do art. 39a ustawy (bezpośrednio w tekście dokumentu, lub jako odesłanie do oddzielnego załącznika), takie elementy, jak:

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 do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Politykę bezpieczeństwa należy przygotować na podstawie przepisów zawartych w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz rozporządzeniu do art. 39a tej ustawy Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Jeśli zaś chodzi o sankcje karne przewidziane w ustawie o ochronie danych osobowych, należy wskazać, iż istnieje także ryzyko odpowiedzialności finansowej na podstawie decyzji administracyjnej wydanej przez GIODO – w przypadku gdy administrator danych nie wykona decyzji wzywającej do usunięcia uchybień przy procesie przetwarzania danych osobowych, GIODO jest uprawniony do nałożenia grzywny przymuszającej do wykonania decyzji w trybie przepisów ustawy o postępowaniu egzekucyjnym w administracji. Wysokość grzywien nie może przekroczyć 10 000 zł za każde uchybienie (ale łącznie nie więcej niż 50 000 zł) w przypadku osoby fizycznej oraz 50 000 zł za każde uchybienie (ale łącznie nie więcej niż 200 000 zł) w przypadku osoby prawnej.

Ochrona danych osobowych w gabinecie lekarskim

W związku z licznymi pytaniami oraz aktywnością wielu komercyjnych firm zapraszamy członków Wielkopolskiej Izby Lekarskiej na spotkanie informacyjne dotyczące tematyki ochrony i przetwarzania danych osobowych w gabinetach lekarskich i dentystycznych.
Spotkanie odbędzie się 10 grudnia 2013 r. o godz. 18.00 w siedzibie Wielkopolskiej Izby Lekarskiej w Poznaniu przy al. Niepodległości 37.

Program spotkania:

1. **Dane osobowe i ich przetwarzanie w gabinecie lekarskim i dentystycznym.**
2. **Zbiory danych osobowych w gabinetach lekarskich.**
3. **Czym są polityka bezpieczeństwa dla gabinetu lekarskiego i instrukcja zarządzania systemem informatycznym? Jak je opracować?**
4. **Jak przestrzegać przepisów o ochronie danych osobowych w gabinetach lekarskich.**

Spotkanie poprowadzi administrator bezpieczeństwa informacji Wielkopolskiej Izby Lekarskiej.
Spotkanie jest bezpłatne i potrwa ok. 90 minut.
Zapisy: admin@wil.org.pl lub 783 993 939