Dane osobowe muszą być bezpieczne

Czy coś może dorównać bezgranicznemu zdziwieniu Molierowskiego mieszczanina, który w kwiecie wieku został porażony informacją, że od urodzenia posługuje się prozą? Może – osłupienie prowadzącego gabinet stomatologiczny, gdy dowie się, że wraz z uruchomieniem praktyki staje się administratorem danych osobowych oraz administratorem bezpieczeństwa informacji

Bywają tytuły wiążące się z licznymi honorami. Tytuły administratorów wiążą się z licznymi, tyle że obowiązkami. Kto i jak obowiązki te wypełnia – sprawdzają brygady Generalnego Inspektora Ochrony Danych Osobowych (GIODO), które mogą wtargnąć także do gabinetu dentysty. Na szczęście nie są to żadne brygady, gdyż centrala GIODO dysponuje zaledwie grupą kilkunastu inspektorów (inspekcja na razie nie ma nawet oddziałów terenowych). O wtargnięciu także nie może być mowy, bowiem o zamiarze przeprowadzenia kontroli podmiot kontrolowany powinien być uprzedzony co najmniej tydzień wcześniej.

Jaki jest zatem powód dbania o utrzymywanie w sterylnym porządku nie tylko narzędzi pracy, ale także baz informacyjnych z danymi osobowymi? Jest jeden. Nie ma granic w wysokości roszczeń, których w powództwie cywilnym dochodzić może pacjent, i to niezależnie, czy został faktycznie poszkodowany, czy tylko poszkodowanym się czuje.

Pilnuj procedur

Podstawową zasadą, chroniącą przed zarzutem braku należytej staranności przy organizowaniu, prowadzeniu i przechowywaniu elektronicznych baz z danymi pacjentów (ale także pracowników), jest stworzenie procedur dotyczących wszystkich tych czynności. Może to być chociażby kilkanaście zdań spisanych na pojedynczej kartce papieru. Na niej właściciel gabinetu stomatologicznego powinien wyjawić, krok po kroku, w jaki sposób utrudnia nieupoważnionym osobom przejęcie danych z pacjentami. Wytyczne do tworzenia procedur znajdują się na stronie internetowej GIODO.

Przed kradzieżą można się ustrzec, np. korzystając z usług biura ochrony, instalując system antywłamaniowy, montując kraty

Ilys. Michael Brown/Dreamstime.com

i zamki patentowe lub umieszczając nośnik z tak zwaną informacją wrażliwą w kasecie pancernej. Ważne, aby z procedury wynikało, że dostęp do danych osobowych w każdej chwili jest należycie chroniony przed nieuprawnionymi ludźmi. – Dostęp do dokumentacji mogą mieć wyłącznie osoby mające pisemne upoważnienie do przetwarzania danych osobowych. Upoważnienie podpisane przez dyrektora placówki lub osobę przez niego umocowaną musi odpowiadać na pytania: kto, w jakim zakresie i do jakiego zbioru ma dostęp. Pomieszczenia, w których przechowuje się dokumentację, powinny być zamykane, a dostęp do kluczy uregulowany wewnętrzną procedurą. Hasła strzegące dostępu do danych medycznych powinny składać się co najmniej z ośmiu znaków zawierających duże i małe litery, cyfry lub znaki specjalne. Hasła takie trzeba zmieniać co 30 dni – informuje Filip Turyk, właściciel firmy IDCON Ochrona danych osobowych.

Nieroztropnością jest pozostawianie włączonego komputera sam na sam z osobami postronnymi. Takie postępowanie może skończyć się kłopotami.

Czuwaj, wróg czyha

Ostatnio w środowisku firm chroniących dane osobowe komentuje się przypadek zaistniały w poważnej instytucji funkcjonującej w ochronie zdrowia. Były, zasłużony pracownik tej instytucji odwiedził kolegów i koleżanki. Ochrona potraktowała go jak czynnego pracownika. Zaufali mu także współpracownicy z działu, pozostawiając na chwilę samotnie w pokoju. To wystarczyło, żeby odwiedzający przegrał na pendrive'a bazę z danymi osobowymi. Mógł to uczynić, bo komputer był włączony, a loginy gościa nie zostały zablokowane, pomimo że od kilku miesięcy nie był już pracownikiem firmy. Najczęściej jednak bywa tak, że dane wykrada konkurencja występująca także pod płaszczykiem pacjenta.

Ufaj, ale nie całkowicie

Obowiązki, którym lekarz nie zawsze potrafi sprostać, najbezpieczniej jest zatem scedować na firmę zewnętrzną. Korzystanie z usług profesjonalistów nie zwalnia jednak właściciela gabinetu dentystycznego z odpowiedzialności za dane osobowe. Warto zatem uzyskać od sprzedającego system informatyczny pisemne oświadczenie, że zastosowane w nim rozwiązania zapewniają tzw. wysoki poziom bezpieczeństwa danych wymagany przez ustawę o ochronie danych osobowych – radzi Filip Turyk.

Kto mniema, że panuje nad zawiłościami systemów informatycznych, musi wiedzieć, że nawet adres IP może być zakwalifikowany jako tzw. dane osobowe, o ile w prosty sposób tą drogą można zidentyfikować stojącą za nim osobę fizyczną. Trzeba wiedzieć też i to, że niedopuszczalne jest przetwarzanie danych osobowych np. w arkuszach Excela. – Zestawienia takie mogą służyć tylko wykonaniu wydruku. Później muszą być usuwane, o ile nie zostały zanonimizowane (pozbawione danych osobowych) – wyjaśnia Filip Turyk.

Jeżeli do bazy danych ma dostęp kilka osób, każda z nich powinna znać tylko swoje hasło, umożliwiające logowanie się w systemie. Dzięki temu w dowolnej chwili można ustalić, kto i w jakich okolicznościach mógł przeglądać i przetwarzać dane osobowe pracowników lub pacjentów.

Martw się na zapas

Nie wystarczy zakupić system, który zapewnia kontrolowany dostęp do informacji osobowych. Równie ważna jest kwestia posiadania kopii zapasowych tych danych. Kto wie, że nośnik z zapisanymi informacjami powinien być umieszczony w innym pomieszczeniu niż to, w którym przechowuje się rejestr podstawowy? Pracownicy GIODO wspominają nawet o zasadności zamykania takich danych w skrytce bankowej. Nie sposób sądzić, że takie rozwiązanie zastosują małe gabinety dentystyczne. Ale ich właściciele także powinni pomyśleć chociażby o zamykanej kasetce przytwierdzonej do podłoża.

Bądź gotowy na wydatki albo…

Kontrolę poziomu bezpieczeństwa systemu informatycznego można zlecić wyspecjalizowanej firmie, ale to kosztuje. Za profesjonalny audyt płaci się od kilku do nawet kilkudziesięciu tysięcy złotych. Cena zależy głównie od stopnia złożoności systemu.

Jest jeden sposób, który może uchronić przed uciążliwościami administrowania informacjami tzw. wrażliwymi. Wystarczy wszystko zapisywać w głowie: imię, nazwisko pacjenta, numer jego telefonu, stan jego uzębienia, wyniki badań diagnostycznych, opis przebiegu procesu leczenia. Prawo uzna wówczas, że dane te są w miarę bezpieczne, o ile oczywiście lekarz nie uczestniczy w seansach hipnotycznych. ■

Mirosław Stańczyk

źródło: GIODO

Dr Wojciech Rafał Wiewiórowski, generalny inspektor ochrony danych osobowych

Przy przetwarzaniu danych osobowych na potrzeby usług medycznych trzeba przestrzegać wszystkich zasad zawartych zarówno w przepisach, na podstawie których działają placówki ochrony zdrowia, jak i w ustawie o ochronie danych osobowych. W przypadku wątpliwości właściciel zbioru informacji, na przykład o pacjentach, powinien wykazać, że wszystkie gromadzone dane niezbędne są do prawidłowej realizacji określonej usługi. Nie należy stosować procedur, które – być może – są wygodne dla właściciela, ale które pozwalają na swobodny dostęp chociażby do nazwisk osób leczących się. Stosownym przykładem jest wywieszanie listy pacjentów na drzwiach gabinetu lekarskiego. Nie jest prawdą, że takich rozwiązań już się nie stosuje. Mamy dokładne rozeznanie sytuacji, bo napływają do nas skargi także w tej kwestii.

Należy także pamiętać, że nie można swobodnie udostępniać informacji o przebiegu leczenia najbliższej rodzinie pacjenta. Lekarz powinien albo mieć na to zgodę osoby, której dokumentacja dotyczy, albo członek najbliższej rodziny musi dysponować stosownym upoważnieniem. Informacje o lekarzach pracujących w klinikach nie muszą być już tak skrywane. Właściciel gabinetu może upubliczniać dane personelu wraz z telefonami służbowymi, także komórkowymi, o ile uzna, że takie rozwiązanie usprawni pracę. Oczywiście uzupełnianie danych podstawowych o inne treści dotyczące życia osobistego lekarzy jest niedopuszczalne. Można je zbierać, przetwarzać i upubliczniać tylko po uzyskaniu wyraźnej zgody.

Dokumentacja medyczna prowadzona przez uprawniony podmiot zgodnie z obowiązującymi przepisami nie podlega obowiązkowi rejestrowania w GIODO. Na dysponentów takich zbiorów nałożone są jednak inne obowiązki, których należyte wypełnienie nie jest możliwe bez poznania większości aktów prawnych dotyczących ochrony danych osobowych. Lekarze powinni pamiętać, że prócz ustawy o ochronie danych osobowych – teks jednolity podaje Dz. U. Nr 101 z 2002 roku, poz. 926 – obowiązuje ich co najmniej kilka ważnych regulacji sektorowych, m.in. ustawy: z 30 sierpnia 1991 roku o zakładach opieki zdrowotnej, z 6 listopada 2008 roku o prawach pacjenta i rzeczniku praw pacjenta, z 5 grudnia 1996 roku o zawodach lekarza i lekarza dentysty. Ważne są także zapisy rozporządzenia ministra zdrowia w sprawie rodzajów i zakresu dokumentacji medycznej w zakładach opieki zdrowotnej oraz sposobu jej przetwarzania, a także rozporządzenie MSWiA w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Gra muzyka, a dentysta płaci jak za zboże (epilog)

Konieczność płacenia za publiczne odtwarzanie utworów chronionych prawem autorskim nie wynika z prawa powielaczowego, a takie przypuszczenia zgłaszała część naszych czytelników po zapoznaniu się z artykułem zamieszczonym w 14. numerze „Medical Tribune Stomatologia" – „Gra muzyka, a dentysta płaci jak za zboże". O konieczności płacenia przesądza m.in. ustawa o prawie autorskim i prawach pokrewnych z 4 lutego 1994 roku, tj. Dz. U. Nr 80 z 2000 roku poz. 904.

Teoretycznie słuchanie w pracy radia lub oglądanie telewizji nie musi wiązać się z koniecznością uiszczania opłat, ale tylko wtedy gdy słuchamy lub oglądamy wyłącznie programy informacyjne. Wówczas jednak trzeba być przygotowanym na taką argumentację inspektorów: pomiędzy audycjami nadawane są zazwyczaj reklamy, często ilustrowane materiałem muzycznym, a ten już podlega ochronie pod względem praw autorskich.

Kary za odtwarzanie utworów bez uiszczania należnego wykonawcom wynagrodzenia także są nakładane w majestacie prawa. Mówi o tym m.in. rozdział 14. ustawy o prawie autorskim i prawach pokrewnych. Z odpowiedzialnością karną muszą się liczyć ci, którzy uniemożliwiają lub utrudniają kontrolę korzystania z artystycznych wykonań (art. 119). Reperkusje to grzywna, a nawet kara ograniczenia albo pozbawienia wolności (do roku). ■

Mirosław Stańczyk