Poradnik eksperta
Menedżera Zdrowia:
Bezpieczeństwo danych medycznych

graf. Thomas Roepke/zefa/Corbis

Informacje cenne jak złoto

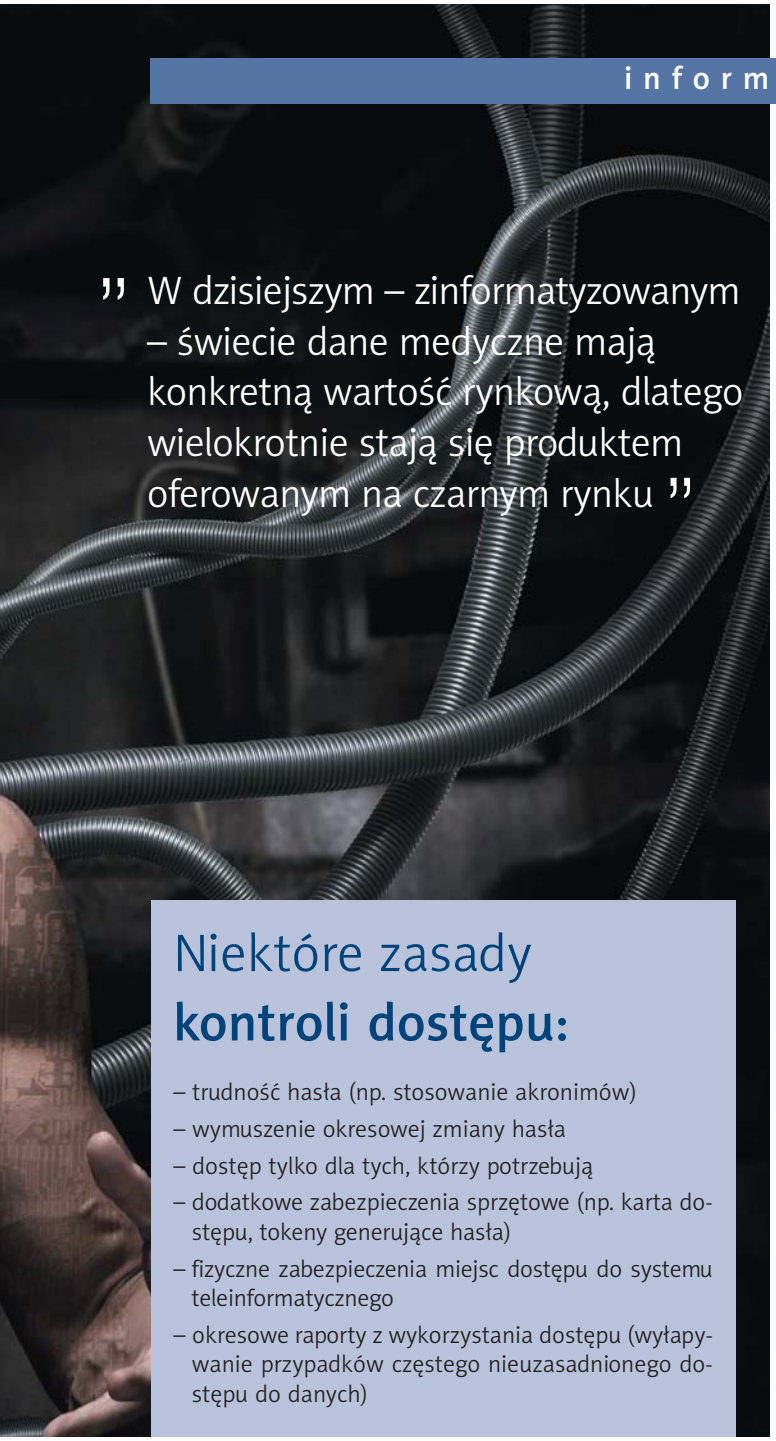
Mirosław Maj

Niedawny przypadek kradzieży laptopa jednemu z lekarzy Centrum Zdrowia Dziecka uświadomił, jak poważne mogą być skutki nieodpowiedniej ochrony danych. Bowiem w dzisiejszej zinformatyzowanej rzeczywistości dane medyczne (dalej DM), to nie tylko informacje na temat przebiegu choroby pacjentów. Są to wszelkiego rodzaju informacje na temat stanu zdrowia danej osoby w przeszłości, a również te, które mogą ułatwić ocenę jego zdrowia w przyszłości (np. wyniki badań DNA). Mają one niezwykłe znaczenie w ochronie prywatności danej osoby. Są również niezbędne w trakcie leczenia.

Nie jest żadną przesadą, że bardzo często mówiąc o ochronie danych medycznych, mówimy o ochronie zdrowia i życia pacjentów. Dlatego są one chronione wieloma przepisami, począwszy od ustawy zasadniczej (art. 51 Konstytucji RP), skończywszy na rozporządzeniach do ustaw (np. *Rozporządzenie ministra spraw wewnętrznych i administracji z 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*).

Zmiana świadomości

Wydaje się, że nie wszyscy zdają sobie z tego sprawę. Trzeba zdecydowanie zwiększyć tę świadomość. Dane medyczne to jedne z najistotniejszych *danych osobowych*.



„W dzisiejszym – zinformatyzowanym – świecie dane medyczne mają konkretną wartość rynkową, dlatego wielokrotnie stają się produktem oferowanym na czarnym rynku”

Niektóre zasady **kontroli dostępu:**

– trudność hasła (np. stosowanie akronimów)
– wymuszenie okresowej zmiany hasła
– dostęp tylko dla tych, którzy potrzebują
– dodatkowe zabezpieczenia sprzętowe (np. karta dostępu, tokeny generujące hasła)
– fizyczne zabezpieczenia miejsc dostępu do systemu teleinformatycznego
– okresowe raporty z wykorzystania dostępu (wyłapywanie przypadków częstego nieuzasadnionego dostępu do danych)

fot. Scott Stulberg/Corbis

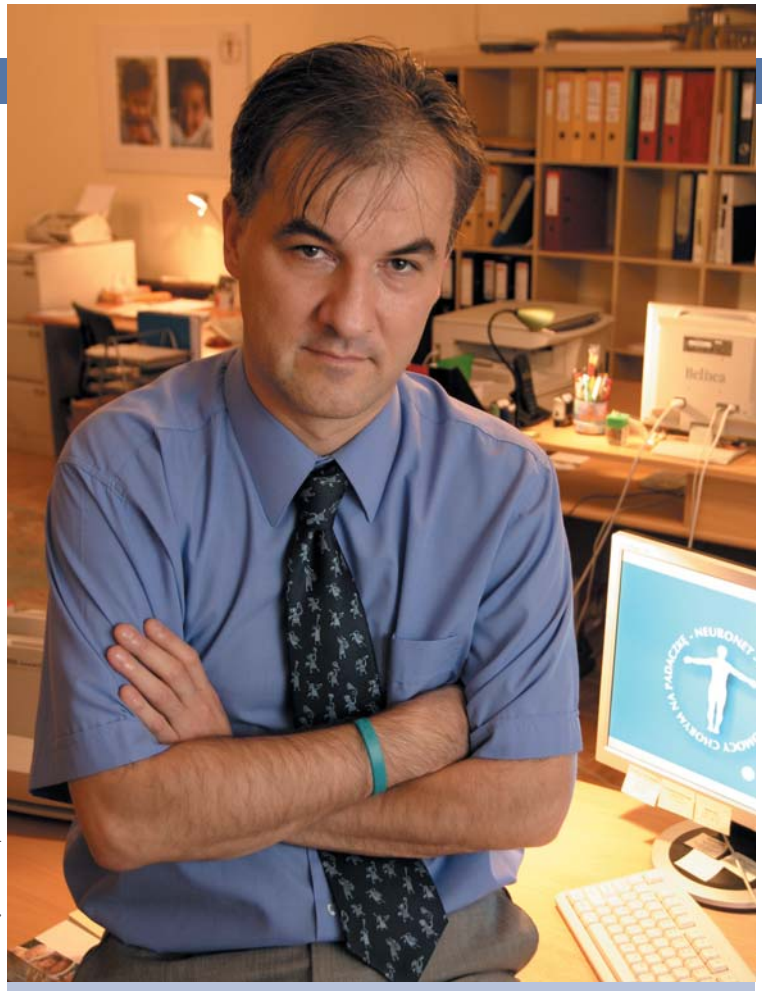
„Pokusa wykorzystania danych pacjentów w celu zwiększenia dochodów (np. przez firmy farmaceutyczne lub ubezpieczeniowe) sprawia, że jest na nie duży popyt”

Paradoks polega na tym, że dziś wiele osób protestuje przeciwko wywieszaniu spisu lokatorów na klatkach schodowych, jak słusznie zauważa Michał Jackowski (Michał Jackowski, *Ochrona danych medycznych*), jednocześnie w ogóle nie interesując się tym, co się dzieje z receptą po przekazaniu jej w aptece do realizacji, która dość szczegółowo może mówić o tym, na co jest chory. Jak więc chronić DM? Poniżej przedstawione zostaną podstawowe zasady ochrony danych w systemach informatycznych, ze szczególnym uwzględnieniem DM, tam gdzie jest to możliwe i wskazane.

Prawo dostępu

Z pewnością jedną z najważniejszych kwestii w ochronie DM jest ochrona dostępu do nich. Największe zagrożenie związane z przetwarzaniem DM jest takie, że trafią one w niepowołane ręce. Wynika to zazwyczaj ze zbyt szerokiego dostępu do nich. W dzisiejszym świecie DM mają konkretną wartość rynkową, dlatego wielokrotnie stają się produktem oferowanym na czarnym rynku. Pokusa wykorzystania danych w celu zwiększenia dochodów (np. przez firmy farmaceutyczne lub ubezpieczeniowe) sprawia, że na takie dane jest duży popyt. Zresztą nieuprawniony dostęp do danych nie musi wynikać z zaplanowanego działania naruszającego prawo. Wyciek istotnych informacji z systemu informatycznego może być wynikiem niedbałego przetwarzania tych informacji i nienależytego zabezpieczenia.

Jak sobie z tym radzić? Wskazane powyżej problemy są najczęściej wynikiem zbyt szerokiego dostępu do DM. Tymczasem dostęp taki powinien wynikać ze stosowania zasady, którą w języku angielskim określa



fot. Piotr Gęsicki/Fotorzepa

Cyber**katastrofa**

– *Katastrofa! Życie i zdrowie dzieci jest zagrożone!* – mówi dr Piotr Zwoliński. Neurochirurg z Centrum Zdrowia Dziecka jest załamany. W drugiej połowie września ukradziono mu laptop, w którym zapisane są historie chorób dzieci czekających na operacje. Piotr Zwoliński od 15 lat zajmuje się leczeniem padaczki u dzieci i młodzieży. W laptopie miał dane kilkuset swoich pacjentów. Historie chorób, informacje o lekach i ich podawaniu, terminy wizyt i dane pacjentów przygotowywanych do operacji, wyniki ich badań i zdjęcia diagnostyczne. Jak twierdzą eksperci, odtworzenie tylko części danych to pół roku przekopywania się przez papierową dokumentację, bo w laptopie były m.in. lista operacyjna, kolejka do zabiegów i bezcenne dane dotyczące zdrowia pacjentów.

się jako *need to know*, czyli dostęp tylko dla tych, którzy rzeczywiście tego potrzebują.

Jak ustalić kto i do jakich danych potrzebuje dostępu? Na to pytanie oczywiście nie odpowie informatyk, tylko lekarz. Informatyk może podpowiedzieć, że aby w praktyce zastosować metodę kontroli dostępu, można posłużyć się stworzeniem kilku lub kilkunastu profili dla poszczególnych grup pracowników służby zdrowia (lub innych, którym dane są udostępniane). Można stworzyć profil dla pielęgniarki, która będzie miała dostęp tylko do tych danych, które są jej konieczne przy wykonywaniu pracy. Dostęp ten będzie się różnił od zakresu dostępu lekarza specjalisty opiekującego się danym pacjentem. Jeszcze inny dostęp będzie miał pracownik administracyjny szpitala, który najprawdopodobniej do wykonywania pracy w ogóle nie potrzebuje szczegółowych informacji na temat choroby pacjenta.

" Można stworzyć profil dla pielęgniarki, która będzie miała dostęp tylko do tych danych, które są jej konieczne przy wykonywaniu pracy. Dostęp ten będzie się różnił od zakresu dostępu lekarza specjalisty opiekującego się danym pacjentem "

Sytuacje wyjątkowe

Przy ustalaniu zasad dostępu warto pamiętać o dwóch ważnych sprawach – uwzględnieniu czynnika czasu oraz sytuacjach wyjątkowych. Jeśli chodzi o okres dostępu, to zapewne informacje o stanie zdrowia pacjentów, którzy przebywali w placówce służby zdrowia wiele lat temu nie są szczególnie istotne i możemy dostęp do nich maksymalnie ograniczyć (np. poprzez wyłączenie możliwości wyświetlania danych starszych niż zaproponowany okres). Oczywiście, przypadki szczególne, pomagające w prowadzeniu podobnych terapii u innych pacjentów, mogą być nadal dostępne. W prowadzeniu leczenia mamy też do czynienia z sytuacjami wyjątkowymi, kiedy dostęp do danych może być konieczny natychmiast, a dodatkowo dostępu tego potrzebuje osoba, która na co dzień nie jest do tego uprawniona (np. zdalne telefoniczne konsultacje lekarza uczestniczącego w akcji ratunkowej). Dla takich sytuacji powinniśmy mieć również specjalną procedurę, z użycia której dokonamy rozliczenia. Na koniec rozważań na temat kontroli dostępu warto dodać, że istniejąca powszechnie w świadomości nieograniczona władza informatyka-administratora systemu przetwarzania DM, to zbyt często powtarzany mit. Jeśli chodzi o prawo dostępu do danych, trzeba wiedzieć, że dobry system przetwarzania danych ma możliwość połączenia sprawnego nim zarządzania i wyłączenia dostępu do DM dla administratora tego systemu (informatyka).

Rozliczalność dostępu

Z prawem dostępu do danych nierozerwalnie łączy się konieczność zapewnienia tzw. rozliczalności przetwarzania tych danych. W praktyce oznacza to, że system informatyczny powinien zapewniać możliwość kontroli tego, kto i kiedy wpisał DM do systemu, przeglądał je, zmieniał, wreszcie – jeśli to nastąpiło – usunął. To nie

tylko obowiązek. Takie zasady mogą być niezwykle pożyteczne. Wyobraźmy sobie sytuację, w której w *kartotece* danego pacjenta znajdujemy informację o konkretnym, nowatorskim zabiegu, który zdecydowanie poprawił jego stan zdrowia. O ileż bardziej pomocna będzie ta informacja, jeśli dodatkowo będziemy wiedzieli, kto taki zabieg wykonał (czyli w tym przypadku dokonał takiego wpisu). Konsultacja z tym lekarzem może okazać się niezwykle pomocna.

W rozporządzeniu o ochronie danych osobowych o tych wymogach możemy znaleźć następujące zapisy, mówiące o tym, co system zapewnia:

- datę pierwszego wprowadzenia danych do systemu;
- identyfikator użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych ma wyłącznie jedna osoba;
- źródła danych – w przypadku zbierania danych od innej osoby niż ta, której one dotyczą;
- informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych.

Pierwsze dwa z powyższych warunków powinny być zrealizowane automatycznie po zatwierdzeniu operacji wprowadzenia danych (to wymóg rozporządzenia). Zresztą przy tej okazji warto wspomnieć, że tego typu warunków, jakie powinien spełniać system informatyczny, w którym przetwarzane są DM, jest więcej. DM to szczególnie chronione dane osobowe, często określane jako wrażliwe, i przetwarzanie ich objęte jest dodatkowymi warunkami (patrz: ustawa o ochronie danych osobowych – art. 27). Aby odpowiedzieć na pytanie, czy zarządzany przez nas system spełnia te wymogi, warto skorzystać z prac organizacji ISACA, która kilka lat temu opracowała *SurvivalKit*, czyli zestaw wytycznych do audytu i kontroli systemów informatycznych pod kątem zgodności z ustawą o ochronie danych osobowych (www.isaca.org.pl – *Projekty – Zamknięte projekty*).

Dodatkowym zagadnieniem związanym z dostępem do DM i rozliczalnością tego dostępu jest kwestia udostępniania tych danych do celów naukowo-badawczych. Jak wiadomo, mogą one być źródłem wielu informacji, bardzo pomocnych zarówno w procesie powszechnych studiów medycznych, jak również zaawansowanych badań naukowych. W takich przypadkach mamy do czynienia zazwyczaj z dwoma typami informacji, która są pożądane – ze zbiorczą informacją statystyczną oraz szczegółową informacją na temat konkretnych przypadków leczenia. W pierwszym z przypadków sprawa jest prostsza – należy przekazywać tylko informacje zbiorcze, podając dane statystyczne zgodnie z profilem zapytania. Najlepiej, jeśli system umożliwia generowanie wcześniej zdefiniowanych raportów. W drugim przypadku jest niezwykle istotne, aby dokonać pełnej anonimizacji danych. Na podstawie danych, które zostaną udostępnione osoba, która je uzyskała, nie może mieć możliwości ustalenia, kogo te dane w rzeczywistości dotyczą. Należy zwrócić uwagę, że anonimizacja danych nie może być realizowana poprzez wymieszanie przypisania DM losowym osobom w bazie danych. Fałszywa informacja, że ktoś może być chory na jakąś chorobę jest równie niebezpieczna w ochronie prywatności, jak informacja prawdziwa. Najlepszym sposobem anonimizacji jest usunięcie wszelkiego rodzaju danych.

Autor jest szefem polskiego zespołu ds. reagowania na naruszenia bezpieczeństwa w Internecie (NASK/CERT)

Artykuł jest pierwszym z cyklu omawiającego najważniejsze zasady ochrony danych medycznych przetwarzanych w systemach teleinformatycznych. Dzięki nim czytelnik będzie miał możliwość zapoznania się z podstawowymi zasadami ochrony danych medycznych przetwarzanych elektronicznie. Przedstawione zostaną zasady tworzenia i utrzymywania zasad dotyczących praw dostępu do danych medycznych, zasad rozliczalności tego dostępu, ochrony transmisji danych, odpowiedniej archiwizacji itp.

Szpiegowanie lekarzy

Ostatnia duża kradzież danych medycznych w USA zdarzyła się w marcu tego roku. Z firmy Affiliated Computer Services, obsługującej służbę zdrowia stanu Georgia, skradziono dane 2,9 mln osób. Affiliated Computer Services została zobligowana do poinformowania listownie wszystkich zainteresowanych o wypadku, stosownych środkach ostrożności oraz zapewnienia wszelkiej pomocy osobom poszkodowanym utratą danych. Samo wysłanie listów będzie kosztowało miliony. Jeszcze większe włamanie miało miejsce w styczniu 2007 r. Wtedy z amerykańskiego centrum medycznego dla weteranów wojennych w Birmingham ukradziono laptop zawierający dane lekarzy i pacjentów – 1,8 mln rekordów, których wartość wyceniono na 367 mln dol. W sumie liczba danych skradzionych w Stanach Zjednoczonych w ostatnim czasie wynosi ok. 100 mln. Specjaliści ostrzegają, że w Polsce pojawiły się wirusy, zwane trojanami, kierowane do określonych grup, np. lekarzy. Przedostają się do komputerów ofiar zazwyczaj z załącznikami do wiadomości elektronicznych. Po pierwszym uruchomieniu na dysku instaluje się program szpiegowski i włącza automatyczne wczytywanie się wraz z systemem Windows. Potem poszukuje danych osobowych pacjentów czy klientów i wysyła je do swego mocodawcy. Dysponując takimi informacjami, autor trojana może dokonywać poważnych nadużyć. Wystarczy np. znać adres i datę urodzenia określonej osoby, aby otworzyć konto w internetowym domu aukcyjnym. Co gorsza, złodziej może sprzedać grupom przestępczym pozyskane dane, które posłużą do ustalenia adresów zamożnych klientów (np. na podstawie statusu pacjenta) w celu zaplanowania napadu rabunkowego.