Przetwarzanie danych medycznych poza placówką opieki zdrowotnej

Tajne bajty na zewnątrz

Jedną z najważniejszych zmian w nowym rozporządzeniu dotyczącym dokumentacji medycznej jest liberalizacja zasad przetwarzania elektronicznych danych medycznych (EDM) poza siedzibą świadczeniodawcy. Otwiera to drogę do *outsourcingu* usług informatycznych. Kiedy będzie on opłacalny i jak się do niego zabrać?

fot. iStockphoto

Zapisy rozporządzenia z 2006 r. w tej kwestii były dość restrykcyjne i większość ekspertów nie miała wątpliwości, że sformułowanie *dokumentacja wewnętrzna jest przechowywana w zakładzie, w którym została sporządzona*, oznaczało, iż dokumentacja medyczna nie może być archiwizowana poza zakładem rozumianym w sensie strukturalnym, tj. jako zbiór jego jednostek i komórek organizacyjnych. W wypadku elektronicznej dokumentacji medycznej, której samodzielne wdrożenie i utrzymanie jest dość kosztowne, takie uwarunkowania były poważnym ograniczeniem, zwłaszcza dla mniejszych placówek. Nowe rozporządzenie zliberalizowało te przepisy, m.in. poprzez zamianę słów „w" na „przez" oraz „zakład" na „podmiot". Obecnie zapis brzmi: *dokumentacja wewnętrzna jest przechowywana przez podmiot, który ją sporządził* (§ 72 rozporządzenia), co niekoniecznie musi oznaczać tożsamość miejsca położenia podmiotu oraz miejsca lokalizacji składowania dokumentacji medycznej.

Zasady dostępu

Liberalizacja zasad przetwarzania danych medycznych poza miejscem świadczenia usług zdrowotnych nie oznacza jednak liberalizacji zasad dostępu do danych. Te nadal są bardzo restrykcyjne. Świadczeniodawca, który zdecyduje się na powierzenie przetwarzania osobowych danych medycznych firmie zewnętrznej, musi więc mieć świadomość, że na podstawie obowiązujących przepisów, tj. ustawy o ochronie danych osobowych, ustawy o zawodzie lekarza i lekarza dentysty oraz ustawy o prawach pacjenta i rzeczniku praw pacjenta, pracownicy firmy zewnętrznej, jako administratorzy danych, nie mogą mieć dostępu do danych medycznych.

Szczególne zasady

Wprowadza to szczególne uwarunkowania w zakresie zastosowania *outsourcingu*. Zgodnie z art. 27 ust. 2 ustawy o ochronie danych osobowych przetwarzanie osobowych danych medycznych jest możliwe w dwóch sytuacjach:

- w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem,
- w celu zarządzania udzielaniem usług medycznych, jeśli są pełne gwarancje ochrony danych osobowych.

W kontekście rozstrzygnięcia dotyczącego możliwości powierzenia przetwarzania osobowych danych medycznych podmiotowi zewnętrznemu specjalizującemu się w przetwarzaniu danych najistotniejsze jest wyjaśnienie, czy administrowanie taką bazą można zaklasyfikować jako „zarządzanie usługami medycznymi". Według R.W. Griffina, zarządzanie to „zestaw działań (planowanie, organizowanie, motywowanie, kontrola) skierowanych na zasoby organizacji (ludzkie, finansowe, rzeczowe, informacyjne) wykorzystywanych z zamiarem osiągnięcia celów organizacji". Zdaniem B. Glińskiego, „zarządzanie to

fot. Images.com/Corbis

> „Liberalizacja zasad przetwarzania danych medycznych poza miejscem świadczenia usług zdrowotnych nie oznacza liberalizacji zasad dostępu do danych"

działalność kierownicza polegająca na ustalaniu celów i powodowaniu ich realizacji w organizacjach podległych zarządzającemu, na podstawie własności środków produkcji lub dyspozycji nimi". Pszczołowski uważa zaś, że „zarządzanie to działanie polegające na dysponowaniu zasobami". Również w wyjaśnieniach słownikowych zarządzanie jest kojarzone przede wszystkim z kierowaniem i podejmowaniem decyzji. Na podstawie powyższych wyjaśnień należy stwierdzić, że osoby pełniące kierownicze funkcje w zakładzie opieki zdrowotnej mogą przetwarzać dane medyczne ze względu na cel, którym jest zarządzanie usługami medycznymi, natomiast o wiele trudniej jest znaleźć podstawy prawne umożliwiające przetwarzanie osobowych danych medycznych pacjentów przez personel administracyjny placówki ochrony zdrowia, tj. statystyków, pracowników rejestracji, administratorów IT, a jeszcze trudniej uzasadnić umożliwienie przetwarzania tych danych osobom, które formalnie nie są nawet pracownikami placówki opieki zdrowotnej.

fot. iStockphoto

> „Powierzanie przetwarzania osobowych danych medycznych wyspecjalizowanym firmom nadal jest problematyczne, chociaż już nie zakazane"

Ochrona danych

Druga przesłanka umożliwiająca przetwarzanie osobowych danych medycznych to zapewnienie pełnych gwarancji ochrony danych osobowych. W związku z tym, że w ustawie o ochronie danych osobowych nie określono precyzyjnego kryterium oceny poziomu gwarancji ochrony danych medycznych, należałoby się odwołać do przepisów unijnych stanowiących punkt odniesienia dla polskiej ustawy o ochronie danych osobowych. Zgodnie z art. 8 ust. 3 Dyrektywy 95/46 WE osobowe dane medyczne powinny być przetwarzane „wyłącznie przez osoby zobowiązane do zachowania tajemnicy".

Na podstawie powszechnie obowiązujących przepisów poza przedstawicielami zawodów medycznych trudno jest znaleźć inną grupę zawodową, która byłaby zobowiązana do tajemnicy w stopniu równorzędnym. W wypadku personelu administracyjnego placówki ochrony zdrowia (statystycy, informatycy, pracownicy rejestracji) można tę kwestię próbować rozwiązać poprzez odpowiednie zapisy w umowie o pracę, w których osoby niewykonujące zawodu medycznego byłyby zobowiązane do zachowania tajemnicy, podobnie jak pracownicy medyczni. W takim wypadku przesłanka „stworzenia pełnych gwarancji ochrony" wydaje się spełniona, gdyż placówka, zatrudniając taką osobę na umowę o pracę, sprawuje nad nią kontrolę.

Firma zewnętrzna

W wypadku powierzenia przetwarzania medycznych danych osobowych firmie zewnętrznej pojawiają się bardzo duże wątpliwości. Bezpośrednia kontrola podmiotu zlecającego nad pracownikami firmy zewnętrznej nie jest możliwa w ramach tradycyjnego stosunku służbowego. Trudno więc w takiej sytuacji mówić o „stworzeniu peł-

nych gwarancji". Byłoby to możliwe, gdyby placówki ochrony zdrowia podlegały rygorom rejestracji zbiorów danych osobowych w GIODO, a co za tym idzie – gdyby wchodziły w reżim procedur kontrolnych ze strony tego urzędu. Wtedy firmy przetwarzające medyczne dane osobowe na podstawie umowy powierzenia podlegałyby również procedurom kontrolnym GIODO. Ustawa o ochronie danych osobowych zwolniła jednak placówki ochrony zdrowia z obowiązku rejestracji zbiorów danych osobowych.

Należy więc stwierdzić, że powierzenie przetwarzania osobowych danych medycznych specjalistycznym firmom, chociaż już nie zakazane, nadal jest problematyczne. Teoretycznie można sobie wyobrazić sytuację, kiedy każdorazowo pacjent wyrażałby zgodę na przetwarzanie danych w firmie zewnętrznej. Byłoby to jednak bardzo trudne praktycznie, gdyż nie można zagwarantować, czy uda się uzyskać takie zgody za każdym razem, a brak zgody choćby w jednym wypadku przekreśla sens wdrażania rozwiązania. Innym pomysłem, który wydaje się najbardziej odpowiedni, jest przyjęcie założenia, że w firmie zewnętrznej archiwizowane będą tylko dane zaszyfrowane przez pracowników medycznych, przy wykorzystaniu infrastruktury PKI (*Public Key Infrastructure*).

> „W rejestrze usługodawców oraz pracowników medycznych oprócz podstawowych danych identyfikacyjnych ewidencjonowane będą certyfikaty klucza publicznego"

Miejsce przechowywania

Zlecając przetwarzanie i archiwizację elektronicznej dokumentacji medycznej wyspecjalizowanej firmie, należy zwrócić uwagę na konieczność jednoznacznej identyfikacji miejsca przetwarzania danych. Świadczeniodawca powinien wiedzieć, na którym serwerze będą archiwizowane jego dane medyczne. W zasadzie powinien to być tzw. serwer dedykowany, oznaczający odrębny komputer (maszynę fizyczną) skonfigurowany dla konkretnego świadczeniodawcy. Najlepiej byłoby, gdyby taki serwer był formalnie własnością świadczeniodawcy, a *outsourcing* polegał tylko na powierzeniu firmie zewnętrznej zarządzania nim w specjalistycznym ośrodku przetwarzania danych (*data center*). Rozwiałoby to ostatecznie wszelkie wątpliwości prawne związane z udostępnianiem danych medycznych podmiotom nieuprawnionym.

Alternatywnym rozwiązaniem mogłaby być dzierżawa albo konkretnego serwera (tzw. serwer dedykowany), albo części jego przestrzeni dyskowej (tzw. wirtualny serwer dedykowany). Wirtualizacja serwera dedykowanego polega na logicznym podziale maszyny fizycznej (komputera) na kilka mniejszych serwerów wirtualnych, które zachowują funkcjonalność serwerów dedykowanych. Dla potrzeb świadczeniodawcy przydzielona zostaje gwarantowana część zasobów maszyny fizycznej. Takie rozwiązanie również nie powinno wzbudzać wątpliwości prawnych, wszak świadczeniodawca zachowuje określone prawo do miejsca, gdzie przetwarzane są dane medyczne jego pacjentów. Można to porównać do sytuacji, kiedy placówka ochrony zdrowia wykonuje świadczenia zdrowotne w użyczonym pomieszczeniu lub budynku. Korzystanie z wirtualnych serwerów dedykowanych może być szczególnie korzystne dla małych placówek ochrony zdrowia, np. indywidualnych praktyk lekarskich, pielęgniarek i położnych.

Standardy bezpieczeństwa

Niezależnie od tego, czy elektroniczna dokumentacja zdrowotna jest gromadzona w systemie informatycznym w siedzibie świadczeniodawcy, czy w siedzibie specjalizującego się w *outsourcingu* podmiotu, system ten powinien spełniać wymagania opisane w normie PN-EN ISO 10781. Norma ta dotyczy modelu funkcjonalnego systemu elektronicznej dokumentacji zdrowotnej (*electronic health record system* – EHR-S) i zawiera listę referencyjną funkcji tych systemów. Zgodnie z intencją normy, opisy funkcji są tworzone z perspektywy użytkownika i są niezależne od technologii oraz strategii implementacji. W związku z powyższym, wybierając system informatyczny do gromadzenia dokumentacji medycznej oraz podmiot świadczący usługi *outsourcingu*, należy wziąć pod uwagę obligatoryjne funkcje infrastruktury informacyjnej z zakresu bezpieczeństwa dla systemu EHR opisane w normie.

Autoryzacja dokumentacji

Chociaż nowe rozporządzenie dotyczące dokumentacji medycznej, które obowiązuje od 1 stycznia 2011 r., zniosło obowiązek stosowania podpisu elektronicznego podczas tworzenia elektronicznej dokumentacji medycznej,

fot. Pete Saloutos/CORBIS

> „Najlepszym rozwiązaniem wydaje się przyjęcie założenia, że w firmie zewnętrznej archiwizowane będą tylko dane zaszyfrowane przez pracowników medycznych"

to jego zastosowanie i tak będzie konieczne, gdyż w przeciwnym razie placówka opieki zdrowotnej nie będzie w stanie włączyć się w procesy wymiany dokumentacji medycznej za pośrednictwem Elektronicznej Platformy Gromadzenia, Analizy i Udostępnienia Zasobów Cyfrowych o Zdarzeniach Medycznych, którą ustanawia ustawa z 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (wykorzystanie przez usługodawców platformy jako narzędzia umożliwiającego przekazywanie dokumentacji medycznej, skierowań, recept i zleceń będzie możliwe od 1 sierpnia 2014 r.).

W celu identyfikacji podmiotów uczestniczących w przekazywaniu elektronicznej dokumentacji medycznej ustawodawca utworzył trzy nowe rejestry: usługodawców, usługobiorców oraz pracowników medycznych. Dwa pierwsze będą miały charakter wtórny, co oznacza, że będą zasilane danymi pochodzącymi z innych rejestrów i ewidencji (np. rejestry ubezpieczonych, rejestr aptek, rejestr podmiotów leczniczych, centralny wykaz świadczeniodawców) bez bezpośredniego angażowania w ten proces placówek opieki zdrowotnej. Rejestr pracowników medycznych będzie miał natomiast charakter pierwotny i zasilany będzie przez usługodawców. Ma on obejmować tylko pracowników aktualnie zatrudnionych. Wszystkie trzy rejestry będą spełniać funkcje przede wszystkim identyfikacyjne, a ich charakter będzie typowo administracyjny. W rejestrze usługodawców oraz pracowników medycznych oprócz danych identyfikacyjnych, jak numer księgi rejestrowej, imię i nazwisko, numer PESEL, numer prawa wykonywania zawodu, ewidencjonowane będą certyfikaty klucza publicznego. Zgodnie z ustawą z 18 września 2001 r. o podpisie elektronicznym (Dz.U. 01.130.1450, z późn. zm.) przez certyfikat należy rozumieć elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do osoby składającej podpis elektroniczny i umożliwiają identyfikację tej osoby. W wypadku rejestru usługodawców będą to certyfikaty przyznane placówkom opieki zdrowotnej jako podmiotom prawnym, a w wypadku rejestru pracowników medycznych – certyfikaty przyznane osobom wykonującym zawód medyczny jako osobom fizycznym. Za pomocą certyfikatów usługodawcy będą uwierzytelniać w SIM dane o udzielonych usługobiorcom świadczeniach opieki zdrowotnej oraz dane dotyczące pracowników medycznych udzielających świadczeń opieki zdrowotnej. Pracownicy medyczni będą ich natomiast używać w celu autoryzacji elektronicznej dokumentacji medycznej udostępnianej podmiotom uprawnionym oraz uzyskania dostępu do elektronicznej dokumentacji medycznej wytworzonej w innych placówkach opieki zdrowotnej.

Nieco inaczej jest w wypadku nowego rejestru pod nazwą Centralny Wykaz Usługobiorców. Chociaż będzie miał, podobnie jak pozostałe centralne rejestry wtórne, charakter głównie administracyjny (realizacja funkcji identyfikacyjnej), to ma on pełnić również funkcje weryfikacyjne. Podmioty świadczące usługi zdrowotne będą mogły się odwoływać do niego, jako wiarygodnego źródła danych, w celu weryfikacji uprawnień do świadczeń (ubezpieczenia publiczne oraz komercyjne), stopnia niepełnosprawności, uprawnień do świadczeń szczególnego rodzaju (honorowi dawcy krwi i szpiku kostnego, honorowi dawcy narządów). Obok danych identyfikacyjnych w rejestrze gromadzone mają być również dane dotyczące wykształcenia, stanu cywilnego, płci, przyczyny zgonu oraz jednostkowe dane medyczne. Zgodnie z ustawą wszystkie trzy rejestry mają zostać uruchomione 1 listopada 2012 r.

O ile kwestia stosowania certyfikatów przez osoby fizyczne została uregulowana w ustawie o podpisie elektronicznym, o tyle nieuregulowany pozostaje problem stosowania podpisu elektronicznego przez instytucje jako osoby prawne. Polskie prawo nie dopuszcza możliwości stosowania tzw. pieczątki elektronicznej. Takie m.in. rozwiązania przewidują przepisy unijne, w tym dyrektywa Parlamentu Europejskiego i Rady Europy 1999/93/WE z 13 grudnia 2009 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych oraz rządowy projekt nowej ustawy o podpisach elektronicznych, który właśnie jest procedowany przez Sejm. W tym kontekście niezwykle ważny będzie zapis art. 6 ust. 3 projektu ustawy, na podstawie którego przyjmować się będzie, że *podpis elektroniczny podpisującego niebędącego osobą fizyczną został złożony przez organ tego podpisującego, zgodnie ze sposobem reprezentacji ujawnionym we właściwym rejestrze.*

Krzysztof Nyczaj
Autor jest konsultantem w gabinecie prezesa GUS. Brał aktywny udział w pracach nad projektem ustawy o informacji w ochronie zdrowia.