DANE MEDYCZNE POD KONTROLĄ

PRZEPISY DOTYCZĄCE DANYCH MEDYCZNYCH BĘDĄ SIĘ W NAJBLIŻSZYCH LATACH ZMIENIAĆ. O ICH SPECYFIKĘ I PODMIOTY UPRAWNIONE DO ICH PRZETWARZANIA PYTAMY DR. WOJCIECHA RAFAŁA WIEWIÓROWSKIEGO.

A KRZYSZTOF NYCZAJ

Dziennikarz, publicysta, ekspert Izby Gospodarczej Medycyna Polska, prowadzi blog poświęcony problemom informatyzacji ochrony zdrowia www.nyczaj.blog.onet.pl.

DR WOJCIECH RAFAŁ WIEWIÓROWSKI

Generalny Inspektor Ochrony Danych Osobowych

KRZYSZTOF NYCZAJ: **Jakie najważniejsze problemy, zdaniem GIODO, wiążą się z przetwarzaniem danych medycznych?**

DR WOJCIECH RAFAŁ WIEWIÓROWSKI: Część problemów, jakie występują w sektorze ochrony zdrowia, jest podobna do tych, z jakimi mamy do czynienia w innych obszarach. Jednym z powszechniejszych jest zwykłe bałaganiarstwo, które powoduje, że dane medyczne są dostępne dla osób przypadkowych. Często zdarza się też, że dane przetwarza się w niezabezpieczonych systemach teleinformatycznych, co stwarza ryzyko ich wycieku. Natomiast do problemów charakterystycznych dla sektora medycznego należą kłopoty z określeniem, którzy pracownicy zaangażowani w działania ochrony zdrowia do jakich danych powinni mieć dostęp. Jest to spowodowane m.in. tym, że w tym przypadku mamy do czynienia ze zbiegiem przepisów dotyczących ochrony danych osobowych z przepisami dotyczącymi tajemnicy lekarskiej. Nie wszystkie informacje podlegające tajemnicy lekarskiej powinny być dostępne dla całego personelu w danej placówce opieki zdrowotnej. O ile zapewnienie dostępu do takich danych np. pielęgniarkom czy położnym, które bezpośrednio uczestniczą w leczeniu pacjenta, jest dość oczywiste, o tyle umożliwienie dostępu do nich osobom z administracji, ochrony czy personelowi sprzątającemu powinno wyglądać inaczej. Klasycznym, wręcz anegdotycznym przykładem, jak nie powinno się stosować przepisów o ochronie danych osobowych w instytucji medycznej, jest przypadek jednej z kontrolowanych przez nas placówek opieki zdrowotnej, w której całemu personelowi sprzątającemu nadano, tak na wszelki wypadek, upoważnienia do przetwarzania danych osobowych, argumentując to tym, że podczas sprzątania pomieszczeń lekarskich osoby te mogą się natknąć na dokumentację medyczną. Tymczasem każde upoważnienie do przetwarzania danych osobowych musi być związane z zakresem obowiązków pracownika.

Muszę jednak podkreślić, że z założenia jako Generalny Inspektor Ochrony Danych Osobowych zajmuję się kwestią klasycznej ochrony danych osobowych i na niektóre wymagania patrzę z punktu widzenia prawa administracyjnego. Tymczasem na zagadnienie to trzeba spojrzeć również z uwzględnieniem tajemnicy lekarskiej. O ile bowiem ustawa o ochronie danych osobowych generalnie zezwala na przetwarzanie danych, o tyle tajemnica lekarska co do zasady tego zabrania.

Trzeba również pamiętać, że w przypadku danych medycznych pewnym problemem jest kwestia powierzenia przetwarzania danych poza teren jednostki oraz przekazywanie ich różnego rodzaju firmom outsourcingowym, co jest w szcze-

gólny sposób uregulowane w przepisach odnoszących się do sektora ochrony zdrowia.

Outsourcing danych medycznych zapewne rozpowszechni się po 1 sierpnia 2014 roku, kiedy wejdą w życie przepisy dotyczące elektronicznej dokumentacji medycznej. W jakim zakresie firma wyspecjalizowana w profesjonalnym przetwarzaniu danych lub naprawie sprzętu medycznego może mieć dostęp do danych medycznych?

Nie ma jednej prawidłowej odpowiedzi na to pytanie, bowiem wszystko zależy od tego, czym zajmuje się firma, której np. zlecamy naprawę sprzętu – czy serwisuje wyłącznie sprzęt, czy oprogramowanie, które służy do przetwarzania danych. Jeśli np. naprawa ma polegać na usunięciu problemu związanego z wadliwie działającym wiatraczkiem w komputerze, to nie oznacza, że pracownicy firmy wykonującej tę pracę powinni mieć dostęp do twardego dysku i zapisanych na nim danych osobowych. Wtedy trzeba albo zaszyfrować dane, albo usunąć twardy dysk na czas naprawy sprzętu w serwisie. Podobnie należy postępować przy naprawie jakiegoś mało znaczącego podzespołu w aparaturze medycznej. Jednak czasem zapewnienie serwisantom dostępu do wszystkich danych zapisanych na dysku naprawianego urządzenia jest konieczne – jeżeli bowiem zlecana przez placówkę ochrony zdrowia praca ma polegać na naprawie błędów w bazie, to nie można jej dokonać bez umożliwienia firmie uzyskania dostępu do danych. Podobnie może być w przypadku serwisu niektórych skomplikowanych urządzeń medycznych zawierających dane medyczne, np. tomografu komputerowego. Sytuacje, w których dane medyczne udostępnia się firmom zewnętrznym, należy traktować jako absolutne wyjątki dopuszczalne tylko wtedy, kiedy jest to jedyne możliwe rozwiązanie problemu, przed którym stanęła placówka opieki zdrowotnej. W takich przypadkach jednak administrator danych musi zawrzeć tzw. umowę powierzenia przetwarzania danych osobowych. Może to być osobna umowa, ale wystarczające jest, aby odpowiednie regulacje w tym zakresie zawrzeć w umowie outsourcingowej lub w umowie na konkretne usługi. Najistotniejsze jest to, by miała formę pisemną, określała zakres i cel przetwarzania danych i zapewniała administratorowi danych kontrolę nad tym, w jaki sposób dane są przetwarzane.

Dlatego też tak ważna jest świadomość, jakie dane medyczne przechowywane są w urządzeniach medycznych i oprogramowaniu…

Dokładnie tak. Musimy zdawać sobie również sprawę z tego, że laptop, a niekiedy nawet smartfon lub iPad to urządzenia, na których również mogą znajdować się dane medyczne i dokonywanie różnego rodzaju synchronizacji tych urządzeń z innymi urządzeniami może spowodować przeniknięcie danych medycznych do urządzenia, nad którym nie mamy kontroli. Często jako przykład podaję synchronizację iPada z komputerem pokładowym w samochodzie. Przecież w ten sposób część danych, które znajdowały się na iPadzie lekarza, znajdzie się w komputerze samochodowym, do którego dostęp będzie miał np. serwisant.

W nawiązaniu do wcześniejszego pytania. Możemy oczekiwać znacznego poszerzenia oferty firm specjalizujących się w przetwarzaniu danych medycznych w chmurze. Na co szczególnie powinny zwrócić uwagę podmioty lecznicze, aby decydując się na takie rozwiązanie, nie naruszyć prawa ochrony danych osobowych oraz tajemnicy lekarskiej?

Placówki opieki zdrowotnej, rozważając korzystanie z cloud computingu, muszą ocenić wpływ przetwarzania danych w tym modelu na bezpieczeństwo nie tylko danych osobowych, ale i danych medycznych, i z tej perspektywy ocenić jego przydatność. Decydując się na jego zastosowanie, muszą pamiętać o przestrzeganiu nie tylko zasad wynikających z ustawy o ochronie danych osobowych i przepisów wykonawczych do niej, ale także z uregulowań dotyczących sektora ochrony zdrowia, w tym tajemnic prawnie chronionych. Zatem placówka medyczna zamierzająca przekazać dane do przetwarzania w chmurze musi brać pod uwagę ich rodzaj i wymagany poziom zabezpieczeń. Z punktu widzenia ochrony danych osobowych musi być odpowiednia gwarancja zabezpieczenia danych przed wyciekiem czy dostępem osób nieupoważnionych. Trzeba również zdawać sobie sprawę z faktu, że podpisanie źle skonstruowanej umowy dotyczącej cloud computingu może narazić nas na przywiązanie do jednego dostawcy rozwiązań chmurowych. Dodatkowo, warto także wskazać na pewną nierównowagę, jeżeli chodzi o poziom wiedzy tym zakresie. Inny bowiem mają podmioty z sektora ochrony zdrowia, które nie specjalizują się w takich rozwiązaniach, a innym dysponują firmy, które trudnią się zawodowo usługami informatycznymi.

Wracając zaś do kwestii tajemnic prawnie chronionych, to istotnym problemem jest to, że jakikolwiek transfer za granicę danych, które są nimi objęte, jest niekiedy niemożliwy – tak jest np. w przypadku informacji niejawnej dotyczącej bezpieczeństwa państwa, a i taka informacja może znajdować się w zasobach jednostki ochrony zdrowia. Przy czym chodzi tu nie tylko o kraje spoza terytorium UE, ale o wszystkie państwa UE. Z drugiej strony istnieje zasób informacyjny, który bez większych problemów może być przetwarzany i udostępniany w modelu usług chmurowych; jest on obecnie na tyle wygodny i popularny, że trzeba przyzwyczaić się do myśli, że w ciągu najbliższych miesięcy i lat zaistnieje jako istotne narzędzie przetwarzania danych.

Thinkstock/FPM

A jak w świetle przepisów o ochronie danych osobowych wygląda kwestia wzajemnego udostępniania danych medycznych przez personel medyczny?

Co do zasady, jedynym podmiotem uprawnionym do przetwarzania danych medycznych pacjenta jest jego lekarz. Nawet ich przekazanie przez jednego lekarza drugiemu lekarzowi może nastąpić tylko w sytuacji, kiedy jest to konieczne dla zachowania ciągłości leczenia. To jest m.in. problem, który pojawia się przy tworzeniu tzw. systemu informacji medycznej. Jednym z podstawowych złożeń tego systemu jest to, by dostęp do danych medycznych pacjenta mógł uzyskać lekarz w każdym miejscu w Polsce. Ale nie oznacza to wcale, że w każdym miejscu w Polsce każdy lekarz powinien mieć dostęp do każdych danych każdego pacjenta. Informacje dotyczące konkretnego pacjenta powinien móc uzyskać ten lekarz, który go leczy lub uczestniczy w świadczeniu usług medycznych dla niego.

Z takich doświadczeń międzynarodowych dotyczących ochrony danych medycznych powinniśmy korzystać?

Przede wszystkim warto zwrócić uwagę na to, że w niektórych krajach, które powszechnie uznawane są za łagodniej podchodzące do ochrony danych osobowych, jak np. Stany Zjednoczone, ochrona danych medycznych jest co najmniej taka sama, o ile nie większa niż w Europie. Zachęcam lekarzy, ale również prawników, aby analizowali, w jaki sposób kodeksy etyczne obowiązujące w innych państwach reagują na pojawianie się nowych technologii informacyjnych. Jednym z takich zagadnień jest możliwość korzystania z usług cloud computingu. To dla nas temat stosunkowo nowy, ale już w pewnym stopniu rozpoznany przez placówki zdrowotne z drugiej strony oceanu. W przypadku ochrony danych medycznych tak naprawdę nie ma poważniejszych różnic w podejściu między krajami Europy, Stanów Zjednoczonych, Kanady czy Australii. Dlatego wiele rozwiązań, zwłaszcza z zakresu organizacyjnego, jest możliwych do wykorzystania w Polsce.

Czy GIODO przewiduje jakieś zmiany w prawie, czy też wyjdzie z jakąś inną inicjatywą legislacyjną wzmacniającą ochronę danych medycznych?

Jeśli chodzi o ochronę danych medycznych, to rozwiązania, które istnieją w Polsce, są w zasadzie wystarczające na obecny moment. Trzeba jednak pamiętać, że wprowadzenie systemu informacji medycznej, elektronicznych rejestrów czy rozwiązań informatycznych umożliwiających sprawdzenie, czy pacjent ma prawo do bezpłatnego leczenia, to są wyzwania, które cały czas stoją przed nami i powinniśmy bardzo ostrożnie na nie patrzeć. Czasem bowiem dobrymi chęciami piekło jest wybrukowane. Niewątpliwie umożliwienie, by za pośrednictwem internetu pacjent mógł mieć dostęp do swoich danych medycznych i informacji o wykonanych na jego rzecz usługach, to bardzo interesująca koncepcja, ale w związku z tym pojawia się wiele pytań i wątpliwości. Na przykład, w jaki sposób uwierzytelniać się w takim systemie? W jaki sposób instytucja udostępniająca dane medyczne będzie sprawdzać, czy ten, który o nie pyta, to pacjent, a nie np. jego ubezpieczyciel, bank czy komornik albo ktokolwiek inny, kto byłby zainteresowany takimi informacjami? Czy osoby nie będą zmuszane do sporządzania wyciągów z dokumentacji medycznej, niby dla siebie, ale w rzeczywistości po to, aby następnie przekazywać je ubezpieczycielowi, np. przed zawarciem umowy. Co prawda, już dzisiaj możemy wystąpić do NFZ, aby uzyskać dane o świadczeniach, które zostały dla nas wykonane. Zmieni się jednak medium, za pośrednictwem którego będzie można tego dokonywać. To spowoduje znaczne skrócenie czasu oczekiwania na taką informację, gdyż będzie ona dostępna w kilka sekund.

Jeśli chodzi generalnie o przepisy dotyczące ochrony danych osobowych, to musimy pamiętać, że w najbliższym czasie dojdzie do bardzo dużych zmian w tym zakresie. Komisja Europejska w styczniu 2012 roku zaproponowała zmianę całości ram prawnych dotyczących ochrony danych osobowych w krajach unijnych, która – w dużym uproszczeniu – polegać będzie na wyeliminowaniu 27 ustaw krajowych i zastąpieniu ich jednym rozporządzeniem europejskim dotyczącym ochrony danych osobowych. W jego projekcie kwestie dotyczące zarówno danych o stanie zdrowia, danych biometrycznych czy genetycznych, jak i danych dotyczących zarządzania ochroną zdrowia, zostały opracowane w szczególny sposób. Jak sądzę, możemy się spodziewać poważnej dyskusji na ten temat.

Ponadto pamiętać należy, że cały czas trwają dyskusje na temat ratyfikacji konwencji bioetycznej oraz de facto wprowadzenia jej w Polsce choćby poprzez uregulowanie badań genetycznych czy biobankowania. Zapowiadają się również zmiany w przepisach dotyczących badań klinicznych, bowiem w lipcu 2012 r. Komisja Europejska zaproponowała nowy projekt rozporządzenia w tym zakresie. To wszystko oznacza, że przez najbliższe kilka lat przepisy dotyczące szeroko rozumianych danych medycznych będą wciąż się zmieniać. Jest istotne, aby w procesie tym uczestniczyły nie tylko jednostki z sektora ochrony zdrowia, ale również instytucje, które zajmują się ochroną praw człowieka czy praw pacjenta, a także podmioty, które reprezentują szeroko rozumiany biznes medyczny.

Na czym generalnie polegają zmiany zaproponowane przez Komisję Europejską?

Jeśli chodzi o ochronę danych medycznych, to najbardziej charakterystyczne jest odróżnienie od siebie dwóch rodzajów danych, a mianowicie danych o stanie zdrowia od danych związanych z ochroną zdrowia. To drugie pojęcie jest

znacznie szersze i obejmuje dane, które nie dotyczą wprost danych medycznych pacjenta, lecz odnoszą się do udzielonych mu świadczeń. Dane o stanie zdrowia, czyli np. dokumentacja medyczna, będą poddane bardziej restrykcyjnym zasadom ochrony, niż dane związane z ochroną zdrowia.
Bardzo istotną zmianą proponowaną przez Komisję Europejską jest wprowadzenie szczególnych obostrzeń dotyczących przeprowadzania oceny wpływu przetwarzania danych biometrycznych i danych genetycznych na prywatność. Ta sprawa jest dość istotna, gdyż coraz częściej dane o stanie zdrowia zaczynają zawierać dane, które mają charakter danych biometrycznych lub danych genetycznych.

Doszły do nas informacje o problemach związanych z rejestrem onkologicznym. Czy to prawda, że GIODO nie chciał zgodzić się na funkcjonowanie tego rejestru w obecnym kształcie?

GIODO od lat nie godzi się z sytuacją, gdy jedyną podstawą prawną do istnienia tego – niezbędnego przecież rejestru – jest załącznik do rozporządzenia wykonawczego do ustawy o statystyce publicznej. Żądamy wprowadzenia samodzielnej podstawy prawnej dla rejestru onkologicznego. Prawdą jest, że nie zaakceptowaliśmy rozszerzenia programu badań statystycznych zaproponowanego przez GUS na rok 2013 i prawdą jest, że prezes Rady Ministrów, po zasięgnięciu opinii Rady Legislacyjnej, potwierdził wszystkie zastrzeżenia, które GIODO zgłaszał do tego projektu. Prawdą jest również, że poinformowaliśmy premiera i prezesa GUS, że jesteśmy w stanie zaakceptować Program Badań Statystycznych na rok 2013 w kształcie, jaki obowiązywał w 2012 roku, pod warunkiem, że w 2013 dojdzie do zmiany ustawy o statystyce publicznej i że w tym samym roku pojawią się prawidłowe podstawy prawne do prowadzenia m.in. rejestru onkologicznego. Prawdą jest również, że nie zgodziliśmy się na treść projektu rozporządzenia dotyczącego Krajowego Rejestru Nowotworów opracowanego przez ministra zdrowia, uznając, że ono w żaden sposób nie oddaje zasad zbierania danych osobowych, które w Polsce powinny obowiązywać. Nie może być tak, że jedno rozporządzenie odsyła do innego rozporządzenia – w tym przypadku do Programu Badań Statystycznych Statystyki Publicznej. To nie minister zdrowia korzysta z danych GUS, lecz odwrotnie – to GUS korzysta z pewnych danych, które zebrał minister zdrowia. Nie mieszajmy pojęć. Administratorem danych gromadzonych w rejestrze onkologicznym jest minister zdrowia.
Podkreślam, że jesteśmy absolutnymi zwolennikami istnienia rejestru onkologicznego. Co więcej, uważamy, że wprowadzenie poprawnych podstaw prawnych jego funkcjonowania podniosłoby jakość gromadzonych w nim danych, m.in. ułatwiłoby to gromadzenie danych o tzw. przeżywalności pacjentów. Dzisiaj, aby przygotować te informacje, trzeba pytać placówki opieki zdrowotnej, czy pacjent jeszcze żyje, a przecież takie informacje można byłoby otrzymywać automatycznie z rejestru PESEL. Działanie jest stosunkowo proste do wykonania, pod warunkiem, że istnieje możliwość automatycznego porównania takiego rejestru np. z bazą PESEL. Jeśli w jednej bazie mamy informacje, że w określonym roku konkretny pacjent o określonym numerze PESEL zachorował na raka i zostały mu udzielone określone świadczenia medyczne i możemy zestawić je z danymi zawartymi w bazie PESEL, to łatwo dla celów sprawozdawczych ustalić przeżywalność, czy w kolejnych latach pacjent wciąż żyje. Jednak każde z tych działań, aby było legalne, musi odbywać

CZY NASZE DANE MEDYCZNE BĘDĄ BEZPIECZNE,

MÓWI MARCIN KĘDZIERSKI, DYREKTOR CSIOZ: Ochrona informacji w systemie informacji medycznej realizowanym przez CSIOZ oparta jest na wielopoziomowym systemie zabezpieczeń, uwzględniającym stosowanie ochrony organizacyjnej, teleinformatycznej i fizycznej. Została ona zaprojektowana z uwzględnieniem wszystkich wymagań zapewnienia bezpieczeństwa przetwarzanych informacji, a przede wszystkim przepisów ustawy o ochronie danych osobowych. Realizując wymagania zapewnienia odpowiedniego poziomu poufności i integralności danych, a także wymaganej dostępności, szeroko wykorzystywać będziemy techniki separacji i anonimizacji danych.
W dużym skrócie polegać one będą m.in. na wydzieleniu danych identyfikacyjnych i składowaniu ich w bazie danych o wyższym rygorze kontroli dostępu. Pozostałe po rozdzieleniu informacje nie będą pozwalać na prostą identyfikację osób. Funkcjonowanie takich mechanizmów będzie kluczowym elementem systemu zapewnienia bezpieczeństwa przetwarzanych danych. Całość systemu zapewnienia bezpieczeństwa informacji obejmować będzie szereg zabezpieczeń zaprojektowanych zgodnie z wymaganiami prawnymi i normatywnymi w zakresie danych medycznych, w szczególności przy uwzględnieniu wymagań normy PN-ISO/IEC 27001.

się na określonej podstawie prawnej. Musi zatem istnieć prawny przymus pozyskiwania danych o wykryciu i leczeniu raka, od którego nikt nie może się uchylić, oraz prawna możliwość zestawiania tych informacji z danymi PESEL.
Jednak do tego, żeby prowadzić tak ważny rejestr, a jest to tylko jeden z przykładów kilkudziesięciu rejestrów medycznych w Polsce, działających bez prawidłowej podstawy prawnej, niezbędne jest istnienie przepisu rangi ustawy i rozporządzenia regulującego wszystkie kwestie związane co najmniej z zakresem i sposobem przetwarzania gromadzonych w nim danych oraz określa, które osoby mogą mieć do nich dostęp. Tymczasem od lat jedyną podstawą istnienia rejestru onkologicznego w Polsce jest formularz statystyczny będący załącznikiem do rozporządzenia w sprawie programu badań statystycznych wydanego na podstawie ustawy o statystyce publicznej. Reasumując więc. Nie jest prawdą, że nie zgadzamy się na istnienie rejestru onkologicznego. Zgadzamy się, aby jeszcze przez rok obwiązywał stan, który uważamy za niezgodny z Konstytucją RP, biorąc pod uwagę, że dostaliśmy zapewnienie zarówno ze strony Głównego Urzędu Statystycznego, jak i Rządowego Centrum Legislacji, że nasze oczekiwania zostaną uwzględnione, a niezbędne zmiany będą wprowadzone i do ustawy statystycznej, i do przepisów dotyczących ochrony zdrowia.

20 grudnia 2012 roku minister zdrowia podpisał rozporządzenie w sprawie utworzenia Krajowego Rejestru Nowotworów. Czy jego treść rozwiała wątpliwości GIODO?

Niestety nie. To rozporządzenie nie uwzględnia uwag GIODO.

Na koniec pytanie, które jest najbardziej interesujące dla kierujących podmiotami leczniczymi. Jak, Pana zdaniem, najlepiej zabezpieczyć dane medyczne w podmiocie leczniczym?

Każda placówka opieki zdrowotnej, rozważając kwestie związane z zabezpieczeniem danych, powinna wziąć pod uwagę swoją specyfikę. Zupełnie inaczej organizacja dostępu do danych medycznych powinna wyglądać np. w ośrodku zdrowia, który de facto jest obsługiwany przez kilkunastu niezależnych od siebie lekarzy wynajmujących pomieszczenia na potrzeby prowadzenia indywidualnej praktyki lekarskiej, a zupełnie inaczej w zamkniętym szpitalu psychiatrycznym. Jeżeli chodzi o dostęp poszczególnych osób w danej placówce do danych medycznych pacjentów, to – jak wspominałem, trzeba wziąć pod uwagę to, czy wszystkie z nich zajmują się tymi samymi pacjentami. W zamkniętym szpitalu psychiatrycznym lekarze, pielęgniarki, pielęgniarze, technicy zazwyczaj zajmują się wszystkimi pacjentami. Inaczej wygląda sytuacja w dużym szpitalu otwartym, a jeszcze inaczej w ośrodku zdrowia, w którym po jednej stronie korytarza znajdują się gabinety udzielające świadczeń zdrowotnych w ramach medycyny plastycznej, a po drugiej – świadczeń związanych z procedurami in vitro.
Innym przykładem pokazującym, jak bardzo trudno jest generalizować zasady ochrony danych osobowych w placówkach opieki zdrowotnej, jest kwestia stosowania monitoringu wizyjnego. Posłużę się tutaj przykładem szpitali. Potrzeba nieustannej kontroli stanu zdrowia pacjenta uzasadnia w pełni stosowanie monitoringu na oddziałach intensywnej opieki medycznej. Te względy nie uzasadniają jednak stosowania monitoringu na wszystkich oddziałach szpitala. W przypadku jednostek służby zdrowia trzeba brać pod uwagę m.in. rodzaj placówki oraz to, kto może przebywać w określonych pomieszczeniach – wyłącznie personel, czy także pacjenci lub goście odwiedzający chorych. Takiej oceny należy dokonać de facto w stosunku do każdego z pomieszczeń, w których instalujemy monitoring, z osobna. Ważnym aspektem jest także to, kto będzie miał dostęp do przetwarzanych danych. Posługując się znowu przykładem oddziału intensywnej opieki medycznej, wątpliwości nie budzi to, że dostęp do danych z monitoringu mają lekarze, pielęgniarki z tego oddziału czy osoby zarządzające szpitalem. Nie powinni go zaś mieć np. pracownicy firmy ochroniarskiej. Odwrotnie może być natomiast w przypadku monitoringu magazynu, w którym są przechowywane lekarstwa.
Tak samo wygląda sprawa, jeśli chodzi o przetwarzanie informacji medycznej w systemach teleinformatycznych. Po pierwsze, zastosowane sposoby zabezpieczeń powinny zależeć od tego, czy te systemy podłączone są do internetu. Jeżeli są podłączone do internetu, to czy przy ich pomocy można uzyskać dostęp do jakichś dodatkowych zasobów internetowych. Jeżeli są odłączone, to kto ma do nich dostęp, w jaki sposób możemy się do nich zalogować.

Na zakończenie, już ostatnie pytanie dotyczące systemu informacji medycznej, który wdraża Ministerstwo Zdrowia przy pomocy Centrum Systemów Informacyjnych Ochrony Zdrowia, i czego wyrazem jest ustawa o systemie informacji w ochronie zdrowia. Czy i ewentualnie, jakie wątpliwości ma GIODO do tej koncepcji?

Niestety, jeszcze nie wiemy dokładnie, jak ma wyglądać działanie – tworzonego przez Centrum Systemów Informacyjnych Ochrony Zdrowia – systemu informacji medycznej. Nie znamy tej konstrukcji w całości. Między innymi z tego powodu podjęliśmy decyzję, że w 2013 roku tematem przewodnim obchodzonego 28 stycznia Europejskiego Dnia Ochrony Danych Osobowych będzie w Polsce zagadnienie ochrony danych medycznych. Planujemy zorganizowanie w tym dniu dużej konferencji pt. „Dane osobowe w ochronie zdrowia i w badaniach klinicznych". Będzie się ona składała z trzech paneli. Pierwszy poświęcony danym medycznym i tajemnicy lekarskiej. Drugi dotyczyć będzie systemów informacyjnych w ochronie zdrowia. Trzeci zaś odnosić się będzie do ochrony prywatności w badaniach klinicznych.