

**Dr Artur Romaszewski**  
*Uniwersytet Jagielloński - Collegium Medicum*  
*Wydział Nauk o Zdrowiu*  
*Zakład Medycznych Systemów Informacyjnych*

**Dr hab. med. Wojciech Trąbka**  
*Uniwersytet Jagielloński - Collegium Medicum*  
*Wydział Nauk o Zdrowiu*  
*Zakład Medycznych Systemów Informacyjnych*

## **PROCEDURY PRZETWARZANIA DANYCH MEDYCZNYCH W ASPEKTCIE WYKORZYSTANIA CHMURY OBLICZENIOWEJ**

W artykule zostaną przedstawione procedury związane z zasilaniem systemu informacji w ochronie zdrowia w dane i informacje ze świadczonych usług medycznych, funkcjonowaniem baz danych, elektronicznej dokumentacji medycznej oraz rejestrów medycznych.

### **Zasilanie systemu w dane i informacje w określonym przez prawo zakresie**

Prawo reguluje zakres danych przechowywanych przez podmioty świadczące usługi medyczne w ramach prowadzonej przez nie działalności (leczenie i diagnostyka) – dotyczy to zarówno baz danych, rejestrów, jak i elektronicznej dokumentacji medycznej oraz dokumentu elektronicznego SIM. Określono także obowiązki podmiotów świadczących usługi medyczne w zakresie udostępniania posiadanych danych i informacji o stanie zdrowia pacjentów. Chodzi tu zarówno o wskazanie przez przepisy wszystkich podmiotów uprawnionych do przetwarzania danych i informacji o stanie zdrowia zawartych w dokumentacji medycznej, jak też o zobowiązanie w zasadzie wszystkich podmiotów świadczących usługi medyczne i aptek do stałego raportowania do systemu o zrealizowanych świadczeniach (w wyniku realizacji usługi medycznej lub recepty).

Możemy wyróżnić dwa odrębne od siebie systemy przetwarzające dane i informacje o stanie zdrowia:

**1. System informacji w ochronie zdrowia** – jest zasilany nieodpłatnie na zasadzie obowiązku przekazywania danych przez wszystkie podmioty świadczące w Polsce usługi zdrowotne (z wyjątkiem podmiotów świadczących usługi na rzecz osób pozbawionych wolności). W ramach tego systemu funkcjonuje System Informacji Medycznej (SIM), tj. system teleinformatyczny

służący przetwarzaniu danych dotyczących udzielonych, udzielanych i planowanych świadczeń opieki zdrowotnej, udostępnianych przez systemy teleinformatyczne świadczeniodawców i apteki. Podmioty te przetwarzają elektroniczne dokumenty SIM w zakresie danych określonych w ustawie. Przekazanie do SIM przez usługodawców komunikatów dotyczących wydanych i zrealizowanych skierowań, recept i zleceń mających formę dokumentu elektronicznego umożliwiającego pacjentowi uzyskanie świadczenia opieki zdrowotnej określonego rodzaju dokonywane jest na bieżąco, co najmniej raz dziennie.

Przesyłanie elektronicznych dokumentów SIM polega na:

- opracowaniu treści komunikatu zawierającego elektroniczne dokumenty SIM przez podmiot zobowiązany do przekazywania informacji do SIM;
  - podpisaniu komunikatu, przy użyciu bezpiecznego podpisu elektronicznego lub podpisu potwierdzonego profilem zaufanym ePUAP;
  - wysłaniu komunikatu, przez podmiot zobowiązany do przekazywania informacji do SIM;
  - odebraniu komunikatu, weryfikacji prawidłowości i wysłaniu potwierdzenia jego otrzymania lub wykazu stwierdzonych w nim błędów lub braków do podmiotów zobowiązanych do SIM<sup>1</sup>.
2. **System informacyjny RUM-NFZ** – obowiązek wszystkich podmiotów mających umowy z NFZ (świadczeniodawcy<sup>2</sup>, apteki<sup>3</sup>). Świadczeniodawcy i apteki przekazują podmiotom zobowiązanych do finansowania świadczeń ze środków publicznych dane w formie elektronicznej. Dane w zakresie wskazanym w przepisach przekazywane są w formacie elektronicznych komunikatów opracowywanych przez każdy podmiot zobowiązany do finansowania świadczeń ze środków publicznych zgodnie z wzorami dokumentów będących opisem komunikatów. Dane przekazywane są na koniec okresu

---

<sup>1</sup> Rozporządzenie Ministra Zdrowia z dnia 28 marca 2013 r. w sprawie wymagań dla Systemu Informacji Medycznej Dz.U. 2013 poz. 463

<sup>2</sup> Rozporządzenie Ministra Zdrowia z dnia 20 czerwca 2008 r. w sprawie zakresu niezbędnych informacji gromadzonych przez świadczeniodawców, szczegółowego sposobu rejestrowania tych informacji oraz ich przekazywania podmiotom zobowiązanych do finansowania świadczeń ze środków publicznych Dz.U. 2008 nr 123 poz. 801

<sup>3</sup> Art. 45 Ustawa z dnia 12 maja 2011 r. o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych Dz.U. 2011 nr 122 poz. 696 Obwieszczenie Ministra Zdrowia z dnia 23 lipca 2013 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Ministra Zdrowia w sprawie informacji gromadzonych przez apteki oraz informacji przekazywanych Narodowemu Funduszowi Zdrowia Dz.U. 2014 poz. 122

sprawozdawczego, którym jest miesiąc kalendarzowy, nie później, niż w terminie dziesięciu dni od jego zakończenia. Dane mogą być przekazywane także w trakcie okresu sprawozdawczego. Na uzasadniony wniosek świadczeniodawcy podmiot zobowiązany do finansowania świadczeń ze środków publicznych może zwolnić świadczeniodawcę na czas określony z obowiązku gromadzenia i przekazywania danych w formie elektronicznej.

## **Prowadzenie baz danych**

Baza danych oznacza zbiór danych lub jakichkolwiek innych materiałów i elementów zgromadzonych według określonej systematyki lub metody, indywidualnie dostępnych w jakikolwiek sposób - w tym środkami elektronicznymi - wymagający istotnego, co do jakości lub ilości, nakładu inwestycyjnego w celu sporządzenia, weryfikacji lub prezentacji jego zawartości<sup>4</sup>.

Do prowadzenia baz danych zostały zobowiązane wszystkie podmioty funkcjonujące w ramach systemu informacji w ochronie zdrowia. System ten obejmuje zatem bazy danych tworzone przez podmioty obowiązane do ich prowadzenia zawierające dane o:

- udzielonych, udzielanych i planowanych świadczeniach opieki zdrowotnej;
- usługodawcach i pracownikach medycznych;
- usługobiorcach.

Podmioty prowadzące bazy danych są uprawnione do przetwarzania zgromadzonych danych w zakresie niezbędnym do realizacji wykonywanych przez nie zadań. Są obowiązane do przekazywania i udostępniania zgromadzonych danych na zasadach określonych w przepisach prawnych. Do ich obowiązków należy również sprawdzanie kompletności, poprawności i zgodności ze stanem faktycznym gromadzonych i udostępnianych danych.

Przekazywanie i aktualizacja danych do systemu informacji są dokonywane w postaci elektronicznej.

Podmioty zobligowane do prowadzenia baz danych w ochronie zdrowia będą musiały rozwiązać kilka problemów, w tym ewentualne prowadzenie ich w chmurze obliczeniowej. Przede wszystkim należy zapewnić bezpieczeństwo i poufność zgromadzonych danych, ale

---

<sup>4</sup> Art2 pkt.1 Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych. Dz.U. 2001 nr 128 poz. 1402

również w zakresie uregulowanym prawem określić zasady korzystania z baz zarówno swoich, jak i z baz innych podmiotów.

Podmioty prowadzące bazy danych w zakresie ochrony zdrowia są obowiązane do stworzenia warunków organizacyjnych i technicznych zapewniających ochronę przetwarzanych danych, w szczególności zabezpieczenia danych przed nieuprawnionym dostępem, nielegalnym ujawnieniem lub pozyskaniem, a także ich modyfikacją, uszkodzeniem, zniszczeniem lub utratą.

Bazy prowadzone w zakresie ochrony zdrowia podlegają kontroli. W przypadku, gdy czynności podejmowane w trakcie kontroli są związane z dostępem do jednostkowych danych medycznych<sup>5</sup> lub dokumentacji medycznej, mogą być realizowane wyłącznie przez osobę wykonującą zawód medyczny, właściwy ze względu na rodzaj i zakres kontrolowanych danych lub zakres udostępnianej dokumentacji medycznej.

Kontrolerzy mają obowiązek zachowania w tajemnicy informacji związanych z pacjentem, w tym jednostkowych danych medycznych, a uzyskanych w związku z wykonywanymi czynnościami kontrolnymi. Ich wykorzystanie na potrzeby czynności kontrolnych może nastąpić wyłącznie w sposób uniemożliwiający identyfikację pacjenta. Ministrowi właściwemu do spraw zdrowia w stosunku do podmiotów prowadzących bazy danych w zakresie ochrony zdrowia przysługuje prawo:

- kontroli realizacji sektorowych projektów informatycznych i systemów teleinformatycznych działających w ramach systemu informacji, w celu zapewnienia spójnego ich działania oraz prawidłowości i kompletności przekazywanych do systemu danych<sup>6</sup>
- kontroli pod względem legalności, celowości i rzetelności prowadzenia baz danych w zakresie ochrony zdrowia oraz przekazywania danych w nich zawartych do systemu informacji;
- wydawania zaleceń pokontrolnych mających na celu usunięcie stwierdzonych nieprawidłowości.

---

<sup>5</sup> Art. pkt 7 jednostkowe dane medyczne – dane osobowe oraz inne dane osób fizycznych dotyczące uprawnień do udzielonych, udzielanych i planowanych świadczeń opieki zdrowotnej, stanu zdrowia, a także inne dane przetwarzane w związku z planowanymi, udzielanymi i udzielonymi świadczeniami opieki zdrowotnej oraz profilaktyką zdrowotną i realizacją programów zdrowotnych;

<sup>6</sup> na zasadach określonych w przepisach art. 25–35 Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz.U. 2005 nr 64 poz. 565

Bazy danych podlegają ochronie uregulowanej w ustawie o ochronie baz danych<sup>7</sup>. Jest to tzw. ochrona *sui generis* niezależnie od ochrony przysługującej niektórym bazom na mocy ustawy o prawie autorskim i prawach pokrewnych<sup>8</sup>. Ustawa chroni przede wszystkim ekonomiczne interesy podmiotu, który poniósł nakłady na stworzenie i funkcjonowanie bazy.

W przypadku nieuprawnionego ujawnienia lub przekazywanie danych z bazy mamy do czynienia z czynem nieuczciwej konkurencji<sup>9</sup> polegającym na naruszeniu tajemnicy przedsiębiorstwa, o ile przedsiębiorca poczynił działania w celu zachowania w poufności danych.

Ministrowie Zdrowia oraz Minister odpowiedzialny za procesy informatyzacji mają za zadanie opracować i udostępnić nieodpłatnie model oprogramowania służący do prowadzenia elektronicznych baz danych, w tym rejestrów medycznych umożliwiającą zakładanie, aktualizowanie zbiorów danych, budowę baz danych w zakresie ochrony zdrowia i ich integrowanie w ramach systemu informacji z uwzględnieniem zasady neutralności technologicznej<sup>10</sup>.

## Rejestry

Rodzajem bazy danych odrębnie zdefiniowanym w ustawie są rejestry medyczne<sup>11</sup>. Są to przede wszystkim zbiory ewidencyjne, listy, spisy i inne uporządkowane zbiory danych, w tym danych osobowych. Powołanie do życia rejestru medycznego oraz jego likwidacja jest możliwa w drodze rozporządzenia. Rejestry medyczne prowadzone są przez podmioty wskazane przepisami prawnymi. Dane do rejestrów są przekazywane przez:

- świadczeniodawców oraz apteki;
- podmioty prowadzące rejestry publiczne i rejestry medyczne.

Przepisy dotyczące rejestrów zobowiązują podmioty świadczące usługi zdrowotne do wypełniania odpowiednich formularzy elektronicznych (niekiedy również papierowych) i przekazywania ich do podmiotów prowadzących rejestry.

---

<sup>7</sup> Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych. Dz.U. 2001 nr 128 poz. 1402

<sup>8</sup> Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych. Dz.U. 1994 nr 24 poz. 83

<sup>9</sup> Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji. Dz.U. 1993 nr 47 poz. 211

<sup>10</sup> wyrażonej w przepisach Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Dz.U. 2005 nr 64 poz. 565

<sup>11</sup> rejestr medyczny – tworzony zgodnie z prawem rejestr, ewidencja, lista, spis albo inny uporządkowany zbiór danych osobowych lub jednostkowych danych medycznych art. 2 pkt. 12 Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia. Dz.U. 2011 nr 113 poz. 657

Przepisy wielu ustaw i rozporządzeń szczegółowo regulują zasady przekazywania danych i informacji do i z rejestrów prowadzonych w ochronie zdrowia.

Dane z rejestrów są udostępniane nieodpłatnie przez usługodawców oraz przez podmioty prowadzące rejestry medyczne do systemu informacji w ochronie zdrowia. Część z rejestrów jest (będzie) prowadzona w chmurze obliczeniowej. Dane zawarte w rejestrach medycznych mogą być udostępniane do celów statystycznych i naukowo-badawczych jedynie w formie uniemożliwiającej ich powiązanie z konkretną osobą fizyczną.

Zakres danych przetwarzanych w rejestrach jest określony w przepisach. Dane inne, niż wskazane w ustawie dające się powiązać z konkretną osobą fizyczną mogą być przetwarzane w rejestrach medycznych wyłącznie wtedy, gdy źródłem danych w nich zawartych jest dokument obejmujący dane osobowe niedające się oddzielić przy ich przekazywaniu lub gdy identyfikacja jest niezbędna do realizacji zadań i celów rejestru.

Warunkiem legalności przetwarzania danych w rejestrze jest obowiązek informacyjny w stosunku do osoby, której dane dotyczą. Podmiot prowadzący rejestr jest obowiązany w terminie 30 dni od dnia rozpoczęcia przetwarzania danych osobowych poinformować każdą osobę, której dane dotyczą i są przetwarzane w rejestrze o:

- adresie swojej siedziby i pełnej nazwie;
- celu, zakresie i sposobie przetwarzania dotyczących jej danych;
- prawie dostępu do treści swoich danych oraz ich poprawiania;
- kategoriach odbiorców, którym dane z rejestru są udostępniane;
- dobrowolności albo obowiązku podania danych, które są przetwarzane
- w rejestrze, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

W przypadku wniesienia przez osobę, której przetwarzane dane dotyczą, sprzeciwu, administrator danych zawartych w rejestrze medycznym jest obowiązany do usunięcia z tego rejestru wszelkich danych umożliwiających identyfikację osoby, chyba że ich przetwarzanie jest niezbędne w celu uniknięcia zagrożenia dla życia i zdrowia ludzi.

Dane zawarte w rejestrach medycznych mogą być udostępniane do celów statystycznych i naukowo-badawczych jedynie w formie uniemożliwiającej ich powiązanie z konkretną osobą fizyczną.

Minister właściwy do spraw zdrowia prowadzi w Biuletynie Informacji Publicznej wykaz rejestrów medycznych. Wykaz jest aktualizowany niezwłocznie po utworzeniu albo likwidacji rejestru.

Administratorem danych gromadzonych w rejestrach medycznych jest minister właściwy do spraw zdrowia.

Została uregulowana procedura udostępniania informacji znajdujących się w rejestrach. Podmiot prowadzący rejestr publiczny<sup>12</sup> wydając informacje z tego rejestru w drodze wymiany obowiązany jest zapewnić rozliczalność takiej operacji.

Podmiot prowadzący rejestr informuje w sposób powszechnie dostępny, w tym w Biuletynie Informacji Publicznej, o warunkach, sposobie, zakresie i terminie udostępniania danych zgromadzonych w rejestrze oraz o formacie, w którym dane są udostępniane. W przypadku, gdy przepisy, na których podstawie jest prowadzony rejestr, nie określają terminu udostępnienia danych, dane udostępnia się nie później niż w terminie 14 dni od dnia doręczenia wniosku o ich udostępnienie. Dane zgromadzone w rejestrze udostępnia kierownik jednostki organizacyjnej, w której jest prowadzony rejestr lub osoba przez niego upoważniona.

Podmiot, któremu udostępniono dane zgromadzone w rejestrze, zabezpiecza otrzymane dane przed dostępem osób nieupoważnionych lub nieuprawnioną zmianą ich zawartości oraz przed ich wykorzystaniem niezgodnym z celem, dla którego zostały uzyskane. Podmiot ten odpowiada za bezpieczeństwo i integralność uzyskanych danych. Informacje o warunkach zabezpieczeń technicznych i organizacyjnych niezbędnych do uzyskania dostępu do danych zgromadzonych w rejestrze kierownik podmiotu prowadzącego rejestr przedstawia w sposób powszechnie dostępny, w tym w Biuletynie Informacji Publicznej<sup>13</sup>.

Wymiana danych dokonywana pomiędzy rejestrami publicznymi obejmuje jedynie informacje niezbędne do prawidłowego funkcjonowania tych rejestrów. Wymiana danych odbywa się przez bezpośrednie odwołanie się do danych referencyjnych przez rejestr inicjujący

---

<sup>12</sup> rejestr publiczny - rejestr, ewidencję, wykaz, listę, spis albo inną formę ewidencji, służące do realizacji zadań publicznych, prowadzone przez podmiot publiczny na podstawie odrębnych przepisów ustawowych; Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Dz.U. 2005 nr 64 poz. 565

<sup>13</sup> Rozporządzenie Rady Ministrów z dnia 27 września 2005 r. w sprawie sposobu, zakresu i trybu udostępniania danych zgromadzonych w rejestrze publicznym Dz.U. 2005 nr 205 poz. 1692

wymianę. Wymiana danych w innym trybie, w tym przez kopiowanie danych przez rejestr inicjujący wymianę, jest dopuszczalna tylko w uzasadnionych przypadkach.

## **Wybór miejsca przechowywania danych o stanie zdrowia**

Podjęcie decyzji o miejscu przechowywania danych i informacji o stanie zdrowia to jedna z najistotniejszych decyzji, którą należy podjąć wprowadzając elektroniczną dokumentację medyczną.

Jeżeli chodzi o przepisy dotyczące możliwości przetwarzania danych zgromadzonych w dokumentacji medycznej przetwarzanej w chmurach obliczeniowych to takie nie istnieją.

W przypadku danych zawartych w dokumentacji (również tej w postaci elektronicznej) decyzja o miejscu i sposobie przechowywania danych podejmowana jest przez kierownika podmiotu leczniczego. Dokumentacja wewnętrzna jest przechowywana przez podmiot, który ją sporządził.

Miejsce przechowywania bieżącej dokumentacji wewnętrznej określa podmiot, a w placówce medycznej – kierownicy poszczególnych komórek organizacyjnych tego zakładu w porozumieniu z kierownikiem zakładu<sup>14</sup>. Nie ma wymogu, by elektroniczna dokumentacja medyczna była przetwarzana w miejscu funkcjonowania podmiotu. Bardziej precyzyjnie problem został uregulowany przez Ministra Spraw Wewnętrznych.<sup>15</sup> Określono wprowadzić miejsce przechowywania dokumentacji wewnętrznej - w zakładzie, w którym została sporządzona, ale jednocześnie dopuszczono archiwizację dokumentacji przez inny podmiot, pod warunkiem zabezpieczenia jej przed zniszczeniem, uszkodzeniem lub utratą i dostępem osób nieupoważnionych.

Warunkiem przetwarzania elektronicznej dokumentacji medycznej jest:

- prowadzenie jej w systemie teleinformatycznym zapewniającym:

---

<sup>14</sup> § 74. Rozporządzenie Ministra Zdrowia z dnia 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania. Dz.U. 2010 nr 252 poz. 1697

<sup>15</sup> § 58. 1. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 18 maja 2011 r. w sprawie rodzaju i zakresu oraz sposobu przetwarzania dokumentacji medycznej w zakładach opieki zdrowotnej utworzonych przez ministra właściwego do spraw wewnętrznych. Dz.U. 2011 nr 125 poz. 712



- 1) zabezpieczenie dokumentacji przed uszkodzeniem lub utratą;
  - 2) zachowanie integralności i wiarygodności dokumentacji;
  - 3) stały dostęp do dokumentacji dla osób uprawnionych oraz zabezpieczenie przed dostępem osób nieuprawnionych;
  - 4) identyfikację osoby udzielającej świadczeń zdrowotnych i rejestrowanych przez nią zmian,
  - 5) udostępnienie, w tym przez eksport w postaci elektronicznej dokumentacji albo części dokumentacji będącej formą dokumentacji określonej w rozporządzeniu, w formacie XML i PDF;
  - 6) eksport całości danych w formacie XML, w sposób zapewniający możliwość odtworzenia tej dokumentacji w innym systemie teleinformatycznym;
  - 7) wydrukowanie dokumentacji w formach określonych w rozporządzeniu.
- odpowiednie zabezpieczenie. Przepisy precyzują warunki, które należy spełniać w sposób ciągły, aby dokumentację w postaci elektronicznej można uważać za zabezpieczoną. Należy zapewnić:
    - 1) jej dostępność wyłącznie dla osób uprawnionych;
    - 2) jej ochronę przed przypadkowym lub nieuprawnionym zniszczeniem;oraz zastosować metody i środki ochrony dokumentacji, których skuteczność w czasie ich zastosowania jest powszechnie uznawana.

Działania niezbędne w celu zabezpieczenia elektronicznej dokumentacji medycznej to przede wszystkim:

- systematyczne dokonywanie analizy zagrożeń;
- opracowanie i stosowanie procedur zabezpieczania dokumentacji i systemów ich przetwarzania, w tym procedur dostępu oraz przechowywania;
- zastosowanie środków bezpieczeństwa adekwatnych do zagrożeń;
- bieżące kontrolowanie funkcjonowania wszystkich organizacyjnych i techniczno-informatycznych sposobów zabezpieczenia, a także okresowe dokonywanie oceny skuteczności tych sposobów;

- przygotowanie i realizacja planów przechowywania dokumentacji w długim czasie, w tym jej przenoszenia na nowe informatyczne nośniki danych i do nowych formatów danych, jeżeli tego wymaga zapewnienie ciągłości dostępu do dokumentacji.

Jednocześnie w przepisach dotyczących dokumentacji medycznej w postaci elektronicznej znajduje się odesłanie do przepisów zapewniających ochronę informacji prawnie chronionych w niej zawartych. Przepisy te przede wszystkim dotyczą: praw pacjenta, tajemnic zawodowych oraz ochrony danych osobowych.

Decydując się na miejsce przetwarzania, w tym przechowywania danych o stanie zdrowia, należy uwzględnić wiele problemów. Najwięcej uwagi przy analizach możliwości wykorzystania modelu chmury obliczeniowej do przetwarzania danych o stanie zdrowia poświęca się regulacjom dotyczącym ochrony danych osobowych. Problematyka jest skomplikowana, a w niedługim czasie można spodziewać się wejścia w życie nowych regulacji, które dodatkowo wymuszą szereg działań, w zasadzie we wszystkich podmiotach świadczących usługi z zakresu ochrony zdrowia. Jest to wynikiem planowanego wejścia w życie rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych. Rozporządzenie to akt, który obowiązywałby bezpośrednio w krajach członkowskich bez potrzeby wydawania aktów prawnych wdrażających je do porządku krajowego. Dzięki jego wprowadzeniu nastąpiłaby pełna harmonizacja prawa materialnego w ramach Unii Europejskiej i swobodnego przepływu danych<sup>16</sup>.

Do problemów informatyzacji sektora ochrony zdrowia oraz wykorzystania chmury obliczeniowej do przetwarzania danych o stanie zdrowia odniósł się Generalny Inspektor Ochrony Danych Osobowych : - *„Oczywiste jest, że duża grupa podmiotów zajmujących się działalnością leczniczą nie jest przygotowana do prowadzenia w postaci elektronicznej wszystkich czynności takich, jak przechowywanie, przetwarzanie i archiwizowanie danych medycznych. Im mniejszy jest podmiot leczniczy, który będzie dane przetwarzał, tym więcej problemów dotyczących jego samodzielnego działania będzie się pojawiać. To oznacza, że eksploduje nam rynek usług outsourcingu dla tych podmiotów. Co więcej, spodziewam się, że bardzo duża część podmiotów medycznych będzie chciała realizować je w modelu chmury obliczeniowej – czyli przekazywać dane do podmiotów, które dostarczą im infrastrukturę razem*

---

<sup>16</sup> Informacje ogólne – strona internetowa Generalnego Inspektora Ochrony Danych Osobowych <http://www.giODO.gov.pl/1520143/j/pl/> data dostępu 30.10.2014

*z oprogramowaniem znajdującym się w chmurach. Upraszczając, lekarz nie będzie miał u siebie na komputerze oprogramowania, które służy mu do zbierania, przetwarzania, archiwizowania danych medycznych. To oprogramowanie wraz z infrastrukturą, gdzie dane będą przechowywane, będzie znajdowało się poza jego gabinetem. Nie będzie się ono znajdowało u konkretnego outsourcingera, który będzie przechowywał dane na konkretnym komputerze. Oprogramowanie będzie znajdowało się w chmurze obliczeniowej. Biorąc pod uwagę wszystkie kwestie związane z bezpieczeństwem danych medycznych, musimy zdawać sobie z tego sprawę. System Informacji Medycznych w Polsce jest wdrażany. Będzie aktywniej korzystał z zasobów, a być może także z zasobów, które lekarze będą chcieli przechowywać w chmurach obliczeniowych<sup>17</sup>”.*

### **Instytucja powierzenia danych o stanie zdrowia**

Jednym z kluczowych elementów związanych z możliwością korzystania z chmury obliczeniowej jest instytucja powierzenia danych<sup>18</sup>.

Administrator danych może przetwarzać dane:

- samodzielnie;
- powierzyć ich przetwarzanie innemu podmiotowi.

W obydwu przypadkach chmury obliczeniowe mogą być wykorzystane jako miejsce przetwarzania danych. Jednak pierwszy przypadek w polskich warunkach w zasadzie odnosiłby się do chmur prywatnych lub hybrydowych, natomiast skorzystanie z większych zasobów i mocy obliczeniowych związane jest z korzystaniem z chmur zarządzanych przez podmioty zewnętrzne. Intencją ustawodawcy było rozdzielenie obowiązków administratora od podmiotu zarządzającego danymi.

Administrator danych powierza innemu podmiotowi w drodze umowy zawartej na piśmie, przetwarzanie danych.

Podmiot, któremu powierzono dane:

---

<sup>17</sup> Pełny zapis przebiegu posiedzenia Komisji Innowacyjności i Nowoczesnych Technologii (Nr 86) z dnia 11 września 2013 r. Generalny Inspektor Ochrony Danych Osobowych Wojciech Wiewiórowski, źródło internetowe <http://www.sejm.gov.pl/Sejm7.nsf/biuletyn.xsp?sknr=INT-86>, data dostępu: 30.10.2014

<sup>18</sup> Art. 31 Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Dz.U. 2002 nr 101 poz. 926

- może je przetwarzać wyłącznie w zakresie i celu przewidzianym w umowie. Jednak w przypadku chmury może dojść do sytuacji, w której o środkach przetwarzania będzie decydował podmiot dysponujący chmurą obliczeniową.
- jest zobowiązany do podjęcia działań zapewniających bezpieczeństwo przetwarzanych danych. W zakresie przestrzegania tych wymogów podmiot ponosi odpowiedzialność jak administrator danych.

Odpowiedzialność za przestrzeganie przepisów ustawy o ochronie danych osobowych spoczywa na administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową. Podmiot, któremu powierzono dane, podlega kontroli w zakresie zgodności przetwarzania danych z ustawą.

W przypadku przetwarzania danych osobowych przez podmioty mające siedzibę albo miejsce zamieszkania w państwie trzecim administrator danych jest obowiązany wyznaczyć swojego przedstawiciela w Rzeczypospolitej Polskiej.

Ostatnio pojawiły się propozycje wprowadzenia instytucji „powierzenia danych innemu podmiotowi” w założeniach do zmian ustawy o prawach pacjenta<sup>19</sup>. Proponuje się też wprowadzenie w ustawie instytucji „powierzenia przechowywania dokumentacji medycznej”.

Podobnie, jak w ustawie o ochronie danych administratorem danych pozostałby podmiot udzielający świadczeń zdrowotnych. Natomiast podmiot, któremu powierzono przechowywanie dokumentacji medycznej byłby zobowiązany zabezpieczyć zbiór danych, tzn. zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. W szczególności musi zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Ponadto byłby on zobligowany do m.in: prowadzenia dokumentacji opisującej sposób przetwarzania danych oraz środków technicznych i organizacyjnych powziętych dla jej ochrony (na którą składa się polityka bezpieczeństwa oraz instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych), wyznaczenie administratora bezpieczeństwa informacji, dopuszczenie do przetwarzania danych wyłącznie osób posiadających upoważnienie nadane przez administratora danych, prowadzenie ewidencji osób

---

<sup>19</sup> Założenia do projektu ustawy o zmianie ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta oraz niektórych innych ustaw październik 2013, źródło internetowe <http://legislacja.rcl.gov.pl/lista/1/projekt/185992>, data dostępu 30.10.2014

upoważnionych do przetwarzania danych. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane do zachowania w tajemnicy tych danych oraz sposobu ich zabezpieczenia. Podmiot, któremu powierzono przetwarzanie danych ponosiłby odpowiedzialność za działania niezgodne z prawem z umową zawartą z administratorem danych. Rozwiązanie takie wzmocniałoby gwarancje bezpieczeństwa danych przekazywanych przez administratora danych.

Ponadto przewiduje się możliwość prowadzenia działalności „przechowalniczej” w stosunku do dokumentacji papierowej. Podmiot udzielający świadczeń zdrowotnych mógłby zlecić przechowywanie dokumentacji medycznej prowadzonej w postaci papierowej, na podstawie umowy zawartej z podmiotem leczniczym, którego statut przewidywałby prowadzenie tego typu działalności. Podmiot udzielający świadczeń zdrowotnych obowiązany byłby uporządkować i oznaczyć przekazywaną na przechowanie dokumentację medyczną. Z uwagi na fakt, że zlecenie przechowywania dokumentacji papierowej jest związane z jej fizycznym przekazaniem, co ogranicza bezpośredni dostęp do niej, byłoby ono dopuszczalne pod warunkiem zapewnienia dostępu do dokumentacji bez zbędnej zwłoki. Pomimo zlecenia usługi przechowywania innemu podmiotowi, udzielający świadczeń zdrowotnych byłby nadal obowiązany do jej udostępniania uprawnionym podmiotom i organom. Zmiana powyższa pozwoliłaby podmiotom udzielającym świadczeń zdrowotnych skorzystać z pomieszczeń innego podmiotu, ale nie miałyby wpływu na sytuację i uprawnienia pacjenta, który tak jak obecnie występowałby o udostępnienie dokumentacji medycznej bezpośrednio do podmiotu udzielającego świadczeń zdrowotnych i powinien ją uzyskać bez zbędnej zwłoki<sup>20</sup>.

Często można spotkać się ze stanowiskiem, że co do zasady każda usługa korzystania z chmury obliczeniowej jest związana z instytucją powierzenia danych<sup>21</sup>. Nie wszyscy jednak podzielają takie stanowisko. Szczególnie jest ono dyskusyjne wówczas gdy dostawca chmury nie ma dostępu do danych, np. w przypadku ich zaszyfrowania przez odbiorcę chmury. Problem jednak jest związany z definicją pojęcia przetwarzania danych.

Zgodnie z definicją ustawową *przez przetwarzanie danych rozumie się jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie,*

---

<sup>20</sup> Założenia do projektu ustawy o zmianie ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta oraz niektórych innych ustaw październik 2013 źródło internetowe <http://legislacja.rcl.gov.pl/lista/1/projekt/185992>, data dostępu 30.10.2014

<sup>21</sup> Grupy roboczej art. 29 wyrażonym w Opinii 1/2010 z dnia 16 lutego 2010 r. w sprawie pojęć „administrator danych” i „przetwarzający”, hosting co do zasady stanowić będzie powierzenie przetwarzania danych osobowych do przetwarzającego dane.

*opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,*<sup>22</sup>

Przechowywanie danych jest w związku z tym jedną z operacji przetwarzania danych i zlecenie tej czynności dostawcy chmury będzie w istocie stanowiło powierzenie przetwarzania danych osobowych. Generalny Inspektor Danych Osobowych uważa<sup>23</sup> z kolei, że jeżeli podmiot udostępniający infrastrukturę informatyczną posiada wiedzę co do charakteru przetwarzanych danych, wówczas powinien odpowiednio dane zabezpieczyć zgodnie z przepisami o powierzeniu<sup>24</sup>. Natomiast, jeżeli podmiot udostępniający zasoby chmurowe nie posiada wiedzy co do charakteru przetwarzanych danych, to nie podlega wówczas przepisom o powierzeniu tylko przepisom o wyłączeniu odpowiedzialności usługodawcy z tytułu świadczenia usług drogą elektroniczną<sup>25</sup>. W praktyce jednak najczęściej zasłonięcie się przez dostawcę infrastruktury brakiem wiedzy o charakterze przetwarzanych danych nie będzie wiarygodne<sup>26</sup>.

Przedstawione procedury przetwarzania danych oraz istniejące w systemie opieki zdrowotnej rozwiązania muszą zostać uwzględnione przy wykorzystywaniu modelu chmury obliczeniowej do przetwarzania danych medycznych. Jak widać w szczególności w przypadku instytucji powierzania danych procedury te wymagają dostosowania i doprecyzowania w odniesieniu do danych o stanie zdrowia i możliwości ich zastosowania w modelu chmur obliczeniowych.

## **Literatura**

- [1] ABC bezpieczeństwa danych osobowych przetwarzanych przy użyciu systemów informatycznych, strona GIODO  
[https://edugiodo.giodo.gov.pl/pluginfile.php/113/mod\\_resource/content/15/INF1/INF\\_R05.html#](https://edugiodo.giodo.gov.pl/pluginfile.php/113/mod_resource/content/15/INF1/INF_R05.html#), data dostępu 30.10.2014
- [2] *Cloud Computing* w Sektorze Finansowym, Regulacje i Standardy pod redakcją Macieja Gawrońskiego, źródło internetowe,

---

<sup>22</sup> Art. 7 pkt 2 Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Dz.U. 1997 nr 133 poz. 883

<sup>23</sup> ABC bezpieczeństwa danych osobowych przetwarzanych przy użyciu systemów informatycznych strona GIODO [https://edugiodo.giodo.gov.pl/pluginfile.php/113/mod\\_resource/content/15/INF1/INF\\_R05.html#](https://edugiodo.giodo.gov.pl/pluginfile.php/113/mod_resource/content/15/INF1/INF_R05.html#)

<sup>24</sup> Art. 31 w zakresie art.36–39 zabezpieczenia danych osobowych,

<sup>25</sup> Ar 12-15 Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną. Dz.U. 2002 nr 144 poz. 1204

<sup>26</sup> *Cloud Computing* w Sektorze Finansowym, Regulacje i Standardy pod redakcją Macieja Gawrońskiego, <http://www.twobirds.com/~media/PDFs/PolandPDFs/Cloud%20Computing%20w%20Sektorze%20Finansowym%20Regulacje%20i%20Standardy%202011.pdf>, data dostępu 30.10.2014

<http://www.twobirds.com/~media/PDFs/PolandPDFs/Cloud%20Computing%20w%20Sektorze%20Finansowym%20Regulacje%20i%20Standardy%202011.pdf>, data dostępu 30.10.2014

- [3] Pełny zapis przebiegu posiedzenia Komisji Innowacyjności i Nowoczesnych Technologii (Nr 86) z dnia 11 września 2013 r. Generalny Inspektor Ochrony Danych Osobowych Wojciech Wiewiórowski, źródło internetowe <http://www.sejm.gov.pl/Sejm7.nsf/biuletyn.xsp?skrn=INT-86>, data dostępu: 30.10.2014
  - [4] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 18 maja 2011 r. w sprawie rodzaju i zakresu oraz sposobu przetwarzania dokumentacji medycznej w zakładach opieki zdrowotnej utworzonych przez ministra właściwego do spraw wewnętrznych. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 18 maja 2011 r. w sprawie rodzaju i zakresu oraz sposobu przetwarzania dokumentacji medycznej w zakładach opieki zdrowotnej utworzonych przez ministra właściwego do spraw wewnętrznych. Dz.U. 2011 nr 125 poz. 712
  - [5] Rozporządzenie Ministra Zdrowia z dnia 20 czerwca 2008 r. w sprawie zakresu
  - [6] Rozporządzenie Ministra Zdrowia z dnia 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania. Dz.U. 2010 nr 252 poz. 1697
  - [7] Rozporządzenie Ministra Zdrowia z dnia 28 marca 2013 r. w sprawie wymagań dla Systemu Informacji Medycznej, Dz.U. 2013 poz. 463
  - [8] Rozporządzenie Rady Ministrów z dnia 27 września 2005 r. w sprawie sposobu, zakresu i trybu udostępniania danych zgromadzonych w rejestrze publicznym Dz.U. 2005 nr 205 poz. 1692
- sposobu rejestrowania tych informacji oraz ich przekazywania podmiotom
- [9] Ustawa z dnia 12 maja 2011 r. o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych, Dz.U. 2011 nr 122 poz. 696; Obwieszczenie Ministra Zdrowia z dnia 23 lipca 2013 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Ministra Zdrowia w sprawie informacji gromadzonych przez apteki oraz informacji przekazywanych Narodowemu Funduszowi Zdrowia Dz.U. 2014 poz. 122
  - [10] Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji. Dz.U. 1993 nr 47 poz. 211
  - [11] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Dz.U. 2005 nr 64 poz. 565
  - [12] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną. Dz.U. 2002 nr 144 poz. 1204
  - [13] Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych. Dz.U. 2001 nr 128 poz. 1402
  - [14] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Dz.U. 2002 nr 101 poz. 926
  - [15] Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych. Dz.U. 1994 nr 24 poz. 83

- [16] Założenia do projektu ustawy o zmianie ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta oraz niektórych innych ustaw październik 2013, źródło internetowe <http://legislacja.rcl.gov.pl/lista/1/projekt/185992>, data dostępu 30.10.2014
- [17] Źródło internetowe - strona internetowa Generalnego Inspektora Ochrony Danych Osobowych <http://www.giodo.gov.pl/1520143/j/pl/> data dostępu: 30.10.2014

### ***Streszczenie***

W artykule zostały przedstawione procedury związane z zasilaniem systemu informacji w ochronie zdrowia w dane i informacje ze świadczonych usług medycznych, z funkcjonowaniem baz danych, elektronicznej dokumentacji medycznej oraz rejestrów medycznych. Omówiono procedury zasilania systemu w dane i informacje, prowadzenia baz danych i rejestrów, przechowywanie danych o stanie zdrowia oraz instytucję powierzenia danych. Przedstawione procedury przetwarzania danych oraz istniejące w systemie opieki zdrowotnej rozwiązania muszą zostać uwzględnione przy wykorzystywaniu modelu chmury obliczeniowej do przetwarzania danych medycznych. Jak widać, w szczególności w przypadku instytucji powierzenia danych, procedury te wymagają dostosowania i doprecyzowania w odniesieniu do danych o stanie zdrowia i możliwości ich zastosowania w modelu chmur obliczeniowych.