Dr Artur Romaszewski
Uniwersytet Jagielloński - Collegium Medicum
Wydział Nauk o Zdrowiu
Zakład Medycznych Systemów Informacyjnych
artur.romaszewski@uj.edu.pl

Dr hab. med. Wojciech Trąbka
Uniwersytet Jagielloński - Collegium Medicum
Wydział Nauk o Zdrowiu
Zakład Medycznych Systemów Informacyjnych
wojciech.trabka@uj.edu.pl

Mgr Mariusz Kielar
Uniwersytet Jagielloński - Collegium Medicum
Wydział Nauk o Zdrowiu
Zakład Medycznych Systemów Informacyjnych
mariusz.kielar@uj.edu.pl

Mgr Krzysztof Gajda
Uniwersytet Jagielloński - Collegium Medicum
Wydział Nauk o Zdrowiu
Zakład Medycznych Systemów Informacyjnych
krzysztof.gajda@uj.edu.pl

ELEKTRONICZNA DOKUMENTACJA MEDYCZNA - PRZETWARZANIE DANYCH O STANIE ZDROWIA POZA MIEJSCEM ŚWIADCZENIA USŁUG ZDROWOTNYCH

Wstęp

Rok 2018 to kolejny już termin wprowadzania do polskiego systemu opieki zdrowotnej elektronicznej formy dokumentacji medycznej (EDM). Niezależnie od opóźnień przetwarzanie danych medycznych w formie elektronicznej ma miejsce w coraz większej ilości podmiotów świadczących usługi zdrowotne. Wolno przechodzi do historii dokument papierowy i zastąpiony zostaje dokumentem w postaci elektronicznej. Dotyczy to również w większości podmiotów świadczących usługi zdrowotne i dokumentujących ich realizację w dokumentacji medycznej. Przepisy wprowadzające, jako standard prowadzenie elektronicznej dokumentacji medycznej były już wielokrotnie zmieniane. Niemniej jednak daje się zauważyć przechodzenie wielu podmiotów na model elektronicznej dokumentacji medycznej.

W ostatnim czasie następuje zmiana koncepcji wprowadzenia dokumentu elektronicznego jako rozwiązania kompleksowego na obowiązek stosowania trzech wystandaryzowanych dokumentów: karty informacyjnej leczenia szpitalnego, karty odmowy przyjęcia do szpitala i informacji pisemnej lekarza specjalisty dla lekarza kierującego[1]. Odrębnymi dokumentami w postaci elektronicznej będą również: recepta elektroniczna oraz zaświadczenia lekarskie o czasowej niezdolności do pracy z powodu choroby, pobytu w szpitalu albo innym zakładzie leczniczym podmiotu leczniczego wykonującym działalność leczniczą albo o konieczności osobistego sprawowania opieki nad chorym członkiem rodziny (tzw. druk L4). Usługi w postaci elektronicznej rejestrowane są przede wszystkim w bazach danych. Powstaje problem jak tak gromadzone dane odpowiednio przetwarzać, a w szczególności konserwować, archiwizować i odpowiednio zabezpieczyć.

Wprowadzenie EDM jako obowiązującej formy stawia przed świadczeniodawcami konieczność podjęcia kluczowych decyzji dotyczących wprowadzenia komputerowych systemów przetwarzania elektronicznej dokumentacji medycznej. Jednym z niech jest powierzenia danych medycznych podmiotom firmom zajmującym się profesjonalnie przetwarzaniem danych.

Outsourcing jako możliwe rozwiązanie

Generalnie osoby zarządzające podmiotami świadczącymi usługi zdrowotne mają dwa wyjścia:

- decydują się na przetwarzanie danych na terenie swojej firmy (podmiotu leczniczego) i w związku z tym godzą się na wykonywanie wielu czynności wynikających w przepisów prawa,
- przekazują dane na podstawie odpowiednich umów do podmiotów profesjonalnie zajmujących się przetwarzaniem danych w innej lokalizacji niż firma medyczna i cedują jednocześnie na podmiot otrzymujący dane wszelkie obowiązki związane z zabezpieczeniem danych.

1 Komunikat dotyczący regulacji prawnych w zakresie elektronicznej dokumentacji medycznej 05.05.2017 https://www.csioz.gov.pl/aktualnosci/szczegoly/komunikat-dotyczacy-regulacji-prawnych-w-zakresie-elektronicznej-dokumentacji-medycznej/

Obydwa rozwiązania zawierają różne warianty zarówno od strony technicznej, jak i prawno-administracyjnej. Biorąc po uwagę specyfikę danych medycznych, ich prawne uwarunkowania, jak też specyfikę funkcjonowania różnych jednostek opieki zdrowotnej, przetwarzanie własne wydaje się na pierwszy rzut oka rozwiązaniem dobrym. Podmiot świadczący usługi zdrowotne ma pełną kontrolę nad sprzętem, oprogramowaniem, jak i przetwarzanymi danymi. Oznacza to także pełna odpowiedzialność za wiarygodność, integralność, bezpieczeństwo i poufność danych medycznych.

Wobec specyfiki danych medycznych (dane osobowe i wrażliwe) oraz prawnych i organizacyjnych wymagań stawianych systemom przetwarzania danych medycznych tworzenie oraz utrzymywanie lokalnego ośrodka komputerowego jest dużym wyzwaniem logistycznym i finansowym. Odpowiednie lokum, budowa sieci, zakup odpowiedniego sprzętu, jak i oprogramowania – włączając w to skomplikowane systemy ochrony danych - oraz utrzymywanie wysokokwalifikowanego personelu IT generuje duże koszty. Wydaje się, że to rozwiązanie może być realne w dużych jednostkach opieki zdrowotnej. Znakomita większość świadczeniodawców, poradnie Podstawowej Opieki Zdrowotnej, gabinety specjalistyczne, grupowe praktyki lekarskie, pielęgniarskie czy rehabilitacyjne nie będą w stanie sprostać przedstawionym powyżej wymaganiom. Idea budowy zintegrowanego systemu informacyjnego opieki zdrowotnej, współpraca z Systemem Informacji Medycznej (SIM), platformami obsługującymi system opieki zdrowotnej nakłada dodatkowe wymagania na funkcjonowanie istniejących systemów.

W tej sytuacji dla większości podmiotów świadczących usługi zdrowotne rozwiązaniem może być *outsourcing* w różnych jego formach, jak i obecnie bardzo prężnie rozwijające się rozwiązania chmurowe (*cloud computing*).

Wykorzystywanie usług podmiotów zewnętrznych - przede wszystkim usług kolokacji, usług hostingowych, a w szczególności chmury obliczeniowej jako rozwiązania do przetwarzania, przechowywania danych oraz miejsca ulokowania swojego oprogramowania i baz danych - przestały być nowością, a coraz częściej stają się standardowym sposobem prowadzenia i archiwizacji dokumentacji medycznej. W związku z tym należy spróbować odpowiedzieć na pytanie: jak w obecnej chwili wygląda problem powierzania danych o stanie zdrowia z punktu widzenia prawa oraz wspierających go norm oraz standardów opracowanych na potrzeby bezpiecznego przetwarzania w chmurach obliczeniowych?

Autorzy podejmą próbę uporządkowania problemu pod kątem praktycznym, którego celem jest pomoc osobom zarządzającym podmiotami świadczącymi usługi zdrowotne w podjęciu decyzji o miejscu przetwarzania danych zawartych w dokumentacji medycznej. Natomiast w przypadku, kiedy decyzja o przetwarzaniu danych dotyczących stanu zdrowia została już podjęta, zostaną wskazane istotne uwagi, które należy uwzględnić podpisując lub zmieniając zawartą umowę z dostawcą tego rodzaju usług.

Nowe regulacje prawne w przetwarzaniu danych medycznych

Podejmowaniu decyzji o sposobie przetwarzania danych zawartych w dokumentacji medycznej towarzyszą często informacje dotyczące bezpieczeństwa danych o stanie zdrowia przetwarzanych w postaci elektronicznej. Dotyczy to wszystkich systemów służących do przetwarzania danych zlokalizowanych zarówno w szpitalach, przychodniach, gabinetach oraz w organizacjach grupujących podmioty lecznicze. Chodzi również o systemy, w których przetwarza się dane powierzone przez podmioty świadczące usługi medyczne. Jednak opublikowane raporty wskazują na złe zabezpieczenie danych przetwarzanych przede wszystkim w szpitalach. Problem jest poważny, ponieważ zgodnie z przewidywaniami Europolu w 2017 r. pierwszoplanowym obiektem ataków będą wrażliwe dane medyczne pacjentów przechowywane w słabo zabezpieczonych systemach szpitalnych.

W 2015 r. w USA zanotowano około 111 milionów cyberataków w sektorze ochrony zdrowia, które dotknęły w sumie 35% amerykańskiego społeczeństwa. W największym do tej pory tego typu zdarzeniu – ataku na firmę Anthem – doszło do jednorazowego wycieku ponad 78 milionów danych pacjentów. Szacuje się, że w latach 2017-2021 globalna wartość strat wynikających z działalności cyberprzestępców na świecie wyniesie 6 bilionów USD, a konieczne wydatki związane z zapewnieniem cyberbezpieczeństwa w tym okresie pochłoną, co najmniej 1 bilion USD[2].

Akty prawne regulujące omawianą problematykę to przede wszystkim:

- ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta,[3]
- ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia,[4]

[2] Krakowiak J., *Dane osobowe: Cyberbezpieczeństwo a sektor ochrony zdrowia*, http://www.rp.pl/Zadania/302079937-Dane-osobowe-Cyberbezpieczenstwo-a-sektor-ochrony-zdrowia.html#ap+1

[3] Dz. U. 2009 nr 52 poz. 417

[4] Dz. U. 2011 nr 113 poz. 657; art. Art. 9a. 1.

- ustawa o ochronie danych osobowych / Rozporządzenie UE o ochronie danych (GDPR)[5].

W związku z wejściem w życie nowych regulacji UE (od maja 2018 roku) należy w chwili obecnej uwzględniać przepisy rozporządzeń GDPR w zakresie, w jakim będą miały zastosowanie. W przypadku ochrony danych osobowych - w tym danych o stanie zdrowia - ważnym źródłem wiedzy z zakresu bezpieczeństwa danych są wytyczne tzw. Grupy art. 29[6], niezależnego europejskiego organu doradczego Komisji Europejskiej w zakresie ochrony danych osobowych i prywatności.

Z punktu widzenia omawianego tematu warto również zauważyć przepisy Dyrektywy NIS czyli Dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego, wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Europejskiej. Regulacji będzie podlegał wybór operatorów usług kluczowych (w tym dotyczących ochrony zdrowia) oraz dostawców usług cyfrowych (internetowych platform handlowych, wyszukiwarek internetowych, usług przetwarzania w chmurze). Innymi słowy dostawcy usług dla ochrony zdrowia, w tym obsługujący rozwiązania chmurowe, będą wskazani przez państwo[7].

Dużym problemem w przypadku wykorzystywania zasobów chmurowych jest fakt wieloletnich sporów między UE a USA w sprawie zapewnienia bezpieczeństwa danych osobowych należących do obywateli państw należących do Europejskiego Obszaru Gospodarczego. Należy bowiem mieć na uwadze fakt, że zasoby chmurowe znajdują się często poza Europą i należą do podmiotów stosujących inne regulacje prawne (m.in. USA). Od 12 lipca 2016 roku obowiązują nowe zasady przekazywania danych z obszaru UE do USA. - tzw. tarcza prywatności (ang. *privacy shield*)[8].

[5] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych; Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – GDPR, *General Data Protection Regulation*

[6] powołana na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_pl.pdf

[7] Grzybowski M., *Dziewięć faktów o Dyrektywie NIS, które powinieneś znać.* http://itwadministracji.pl/numery/pazdziernik-2016/9-faktow-o-dyrektywie-nis-ktore-powinienes-znac.html

[8] Komisja Europejska uruchamia Tarczę Prywatności UE-USA: lepsza ochrona transatlantyckiego przepływu danych Bruksela, decyzja Komisji Europejskiej nr C(2016) 4176 12 lipca 2016 r. http://europa.eu/rapid/press-release_IP-16-2461_pl.htm

Warto zwrócić uwagę na tworzenie w tym obszarze silnych podmiotów europejskich. Z jednej strony tworzy to warunki do bezproblemowego przetwarzania danych osobowych na terenie UE, z drugiej umożliwia wykorzystywanie narzędzi przygotowanych przez GDPR do zapewnienia standardów bezpieczeństwa przetwarzanych danych - w tym danych o stanie zdrowia. W związku z tym należy odnotować fakt, że dostawcy usług infrastruktury chmurowej w Europie (*Cloud Infrastructure Services Providers in Europe, CISPE*) - nowo utworzona koalicja ponad dwudziestu dostawców usług chmurowych działających na terenie Europy - ogłosiła wprowadzenie pierwszego w historii kodeksu postępowania w dziedzinie ochrony danych. Zgodnie z tym dokumentem dostawcy usług infrastruktury chmurowej zobowiązani są do oferowania swoim klientom możliwości przetwarzania i magazynowania danych wyłącznie w obrębie terytorium Unii Europejskiej oraz Europejskiego Obszaru Gospodarczego[9].

Umowa powierzenia danych

Ostateczną formą powierzenia danych podmiotowi zewnętrznemu i zarazem jedyną dopuszczalną jest zawarcie z nim umowy. Jednak jej zawarcie musza poprzedzać działania przede wszystkim w zakresie zgromadzenia informacji o podmiocie dostarczającym usługi i technologii przez ten podmiot stosowanej. Oczywiście kierownik podmiotu świadczącego usługi medyczne, który podejmuje decyzję o wykorzystywaniu do przetwarzania danych pacjenta zawartych w elektronicznej dokumentacji medycznej usługi chmurowej, nie jest w stanie sprawdzić bez profesjonalnej pomocy możliwości technicznych oferowanej usługi i jej funkcji użytkowych oraz poziomu zapewnianego bezpieczeństwa. Może jednak przy pomocy profesjonalnego wsparcia uzyskać dokumenty lub oświadczenia dostawcy usług dotyczących stosowanych rozwiązań oraz do oświadczenia w umowie, że przy przetwarzaniu danych o stanie zdrowia zastosowano odpowiednie, wymagane prawem standardy. Jeżeli jest to możliwe należy zapoznać się z dokumentacją techniczną wykorzystanych przez dostawcę usług rozwiązań i poddać je ocenie osób lub podmiotów przygotowanych do tego procesu merytorycznie[10].

[9]https://www.csioz.gov.pl/fileadmin/user_upload/rekomendacje_bezpieczenstwo_projekt_kwiecien2017_58e6909f16b49.pdf

[10] np. zgodności z normą 27001/27002: 2013, która jest powszechnie stosowaną międzynarodową normą dotyczącą zarządzania bezpieczeństwem informacji, ISO/IEC 27018 w aspekcie ochrony danych PII czy *atestCloud Security Alliance* (CSA) *Cloud Controls Matrix* (CCM) opisujący podstawowe zasady zabezpieczeń, którymi powinni kierować się dostawcy

Dobrym rozwiązaniem jest zapewnienie możliwości dokonywania audytu dostawcy chmurowego najlepiej przez certyfikowany podmiot. Podmioty te, w ramach oferty, powinny przedstawić informacje na temat składu zespołu audytorskiego, w tym doświadczenie, kwalifikacje oraz posiadane certyfikaty w zakresie bezpieczeństwa[11]. Umowa powinna zawierać postanowienia zapewniające zachowanie bezpieczeństwa danych pozyskanych przez audytorów, określać warunki audytu oraz czas, w jakim audyt ma być przeprowadzony[12]. Nie zawsze jest możliwe negocjowanie z dostawcą usług. Często umowy o świadczenie usług chmurowych (najczęściej) nie podlegają przy tym negocjacji i zawierane są przez prostą akceptację regulaminu i często nie chronią należycie klienta. Dużym problemem są również konsekwencje normalnych procesów rynkowych takich, jak przejęcie, bankructwo czy likwidacja podmiotów przetwarzających na podstawie umowy dane podmiotów leczniczych[13].

Umowa powierzenia -uregulowania prawne

Ustawodawca zareagował na ten stan rzeczy. Uregulowano możliwość korzystania z usług podmiotów zewnętrznych w zakresie przetwarzania danych o stanie zdrowia. W przypadku rejestrów wskazano, że usługi te można powierzyć podmiotom wyspecjalizowanym w świadczeniu usług związanych z obsługą danych wrażliwych dotyczących zdrowia.

Przede wszystkim rozwiązano problem możliwości wykorzystywania usług przetwarzania danych uzyskanych w związku ze świadczeniem usług medycznych oferowanych przez podmioty zewnętrzne przez podmioty udzielający świadczeń zdrowotnych. Generalnie korzystanie z tego typu usług jest możliwe. Warunkiem legalności korzystania z usług zewnętrznych, w tym m.in usług chmurowych, jest zawarcie umowy powierzenia uregulowanej w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.[14] Niektóre

[11] Zaleca się aby osoba przeprowadzająca audyt bezpieczeństwa posiadała certyfikat CISA (*Certified Information Systems Auditor*), natomiast inni członkowi zespołu audytującego posiadali certyfikaty potwierdzające kompetencje z obszaru bezpieczeństwa IT, np.: CISSP (*Certified Information Systems Security Professional*); CISM (*Certified Information Security Manager*), lub równoważne. Wykonanie audytu powinno poprzedzać zawarcie umowy z podmiotem audytującym.
[12] Rekomendacje Centrum Systemów Informacyjnych Ochrony Zdrowia w zakresie bezpieczeństwa oraz rozwiązań technologicznych stosowanych podczas przetwarzania dokumentacji medycznej w postaci elektronicznej Załącznik nr 5 https://csioz.gov.pl/fileadmin/user_upload/zalacznik_nr_5_58e690a2325ef.pdf
[13] Bezpieczeństwo danych w chmurze: Dane przesyłane są do USA? Nie wiadomo; Źródło: gazetaprawna.pl Artykuł z dnia: 2015-10-18 Autor: T. Jurczak http://www.giodo.gov.pl/plik/id_p/9866/j/pl/
[14] art. 31 ust. 1

publikacje[15] wskazują na przeszkodę prawną, jaką stanowi brak możliwości wprowadzenia w uregulowanych prawnie dokumentach bezpieczeństwa[16] obszaru przetwarzania danych. Jeżeli nawet był to problem to zostanie on rozwiązany wraz z wejściem w życie GDPR.

Z powierzeniem przetwarzania danych w podmiocie leczniczym mamy do czynienia zarówno w przypadku skorzystania ze stałego „wyprowadzenia" danych do podmiotów zewnętrznych w celu ich stałego przetwarzania (np. korzystanie z usługi oprogramowania do tworzenia dokumentacji medycznej), ale również w doraźnych sytuacjach, takich jak serwisowanie sprzętu zawierającego dane pacjentów czy powierzenie danych pracowników podmiotom leczniczym świadczącym usługi z zakresu medycyny pracy.

Nie jest powierzeniem przekazywanie danych przez podmiot leczniczy w przypadkach wskazanych prawem, jak też przekazania danych przez podmioty prowadzące rejestry zawierające dane o stanie zdrowia do rejestrów, również tych prowadzonych w chmurach. Samo przekazanie danych do rejestrów odbywa się na podstawie obowiązku prawnego.[17]

Warunkami zawarcia takiej umowy przez administratora są: [18]

- zawarcie jej w formie pisemnej, wyłącznie w zakresie i celu przewidzianym w umowie zapewnienia ochrony danych osobowych oraz prawa do kontroli przez podmiot udzielający świadczeń zdrowotnych zgodności przetwarzania danych osobowych z tą umową przez podmiot przyjmujący te dane,
- niezakłócenie udzielania świadczeń zdrowotnych, w szczególności w zakresie zapewnienia, bez zbędnej zwłoki, dostępu do danych zawartych w dokumentacji medycznej,

[15] Rekomendacje Centrum Systemów Informacyjnych Ochrony Zdrowia w zakresie bezpieczeństwa oraz rozwiązań technologicznych stosowanych podczas przetwarzania dokumentacji medycznej w postaci elektronicznej

[16] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 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 Dz.U. 2004 nr 100 poz. 1024

[17] Art. 4. Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia Dz.U. 2011 nr 113 poz. 657

[18] Art. 31. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Dz.U. 1997 nr 133 poz. 883

- zachowanie w tajemnicy informacji (także po śmierci) pacjenta związanych z pacjentem uzyskanych w związku z realizacją umowy przez podmiot, któremu powierzono dane

W przypadku zaprzestania przetwarzania danych osobowych zawartych w dokumentacji medycznej przez podmiot, któremu powierzono takie przetwarzanie, w szczególności w związku z jego likwidacją, jest on zobowiązany do przekazania danych osobowych zawartych w dokumentacji medycznej podmiotowi, który powierzył przetwarzanie danych osobowych.

Dane o stanie zdrowia zgromadzone w rejestrach

O utworzeniu, prowadzeniu lub zlecaniu prowadzenia rejestrów medycznych przez podmiot do tego upoważniony decyduje Minister Zdrowia. Rejestr stanowi uporządkowany zbiór danych i informacji o zachorowaniach, chorobach, stanie zdrowia, metodach leczenia, diagnozowania, monitorowania postępów w leczeniu oraz zagrożeniach związanych z występowaniem niektórych chorób. Rola rejestrów rośnie wraz z wykorzystywaniem elektronicznych metod komunikacji.

Dane do rejestrów są przekazywane przez:

- usługodawców;
- podmioty prowadzące rejestry publiczne i rejestry medyczne.

Podmiot prowadzący rejestr w terminie 30 dni od dnia rozpoczęcia przetwarzania danych osobowych powinien 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 celu zapewnienia bezpieczeństwa danych w czasie eksploatacji systemu teleinformatycznego **administrator danych może upoważnić** podmiot prowadzący rejestr

medyczny **do powierzenia** przetwarzania danych zawartych w rejestrze podmiotom wyspecjalizowanym w utrzymywaniu infrastruktury techniczno-systemowej i zapewnianiu obsługi technicznej systemów teleinformatycznych.

Podmioty wyspecjalizowane w utrzymywaniu infrastruktury techniczno-systemowej i zapewnianiu obsługi technicznej systemów teleinformatycznych 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. Nie mogą powierzać innym podmiotom przetwarzania danych zawartych w rejestrach medycznych. Obowiązuje je obowiązek zachowania w tajemnicy informacji związanych ze świadczeniobiorcami uzyskanych w związku z powierzeniem przetwarzania danych. Podmioty te są związane tajemnicą także po śmierci świadczeniobiorcy. Do ich przetwarzania należy zapewnić zabezpieczenia na **poziomie wysokim**[19]. Administrator danych może kontrolować podmioty wyspecjalizowane w zapewnianiu obsługi technicznej systemów teleinformatycznych, w zakresie realizacji wymagań oraz sposobu realizacji celów powierzenia danych przetwarzanych w rejestrach medycznych.

W przypadku zaprzestania przetwarzania danych w rejestrach medycznych przez podmioty wyspecjalizowane w zapewnianiu obsługi technicznej systemów teleinformatycznych lub podmioty prowadzące rejestry medyczne, w szczególności w związku z ich likwidacją, są one obowiązane do przekazania tych danych administratorowi danych tzn. Ministrowi Zdrowia. Minister Zdrowia może upoważnić podmiot prowadzący rejestr medyczny do przyjęcia tych danych.

To, co jest istotne i co się zmieni wraz z wejściem w życie GDPR to problem odpowiedzialności za dane. W obecnym stanie prawnym jest to podmiot powierzający. W przypadku ochrony zdrowia przede wszystkim podmiot prowadzący przedsiębiorstwo podmiotu leczniczego. Podmiot otrzymujący dane w powierzenie (tzw. procesor) nie staje się ich administratorem. Oba podmioty: zarówno udostępniający, jak i podmiot, któremu udostępniono dane osobowe, są administratorami danych. Wprowadza się odrębną odpowiedzialność procesora i administratora. Również podmiot, któremu powierzono dane,

[19] o którym mowa w przepisach wydanych na podstawie art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych

będzie miał takie same obowiązki, jak podmiot powierzający (obecnie musi zabezpieczyć dane).

Administratora danych obowiązuje korzystanie wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi GDPR i chroniło prawa osób, których dane dotyczą. Jest to zatem snałożenie na administratora obowiązku dołożenia szczególnej staranności przy wyborze kontrahenta mającego w jego imieniu przetwarzać dane. Jak się wydaje, ocena spełniania przez „procesora" wymogów przewidzianych ww. przepisem GDPR, mogłaby zostać dokonana po przeprowadzeniu przez administratora danych kontroli stosowanych sposobów zabezpieczania danych. Brak było jednak wyraźnych przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (UODO) odnoszących się do tej możliwości. Powoduje to, że „procesorzy" niejednokrotnie blokują możliwość ich przeprowadzania. Biorąc pod uwagę olbrzymią ilość podmiotów przetwarzających w Polsce dane na zlecenie, zauważyć trzeba, że relatywnie niewielka ich część wdrożyła w organizacjach ochronę danych na takim poziomie, że perspektywa przeprowadzenia przez kontrahenta kontroli, od której być może uzależniona jest dalsza współpraca, nie powoduje ich sprzeciwu[20]. GDPR nakłada obowiązek umożliwienia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzania takich audytów.

Ponadto szczegółowo określono niezbędne elementy, które administrator będzie musiał precyzyjnie określić w umowie, tj.:

- przedmiot i czas trwania przetwarzania;
- charakter i cel przetwarzania;
- rodzaj danych osobowych oraz kategorie osób, których dane dotyczą;
- obowiązki i prawa administratora.

Wprowadza się szereg wymogów dla podmiotu przetwarzającego:

- przetwarzanie danych osobowych wyłącznie na udokumentowane polecenie administratora;

[20] Bargiel-Kaflik M., *Kilka słów o tym, jak na gruncie GDPR powierzyć dane do przetwarzania* http://gdpr.pl/slow-o-tym-gruncie-gdpr-powierzyc-dane-przetwarzania/

- zapewnianie, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
- wdrożenie odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych (środki te mogą obejmować np. pseudonimizację i szyfrowanie danych osobowych, zapewnienie poufności, integralności, dostępności i odporności systemów i usług przetwarzania, przywracanie dostępności danych w razie incydentu fizycznego lub technicznego, regularne testowanie i ocenianie skuteczności ww. środków);
- pomoc administratorowi w wywiązaniu się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III GDPR (a więc wsparcie w realizacji uprawnień osoby o charakterze informacyjnym, korekcyjnym i zakazowym) [21];

Piśmiennictwo:

[1.] Bargiel-Kaflik M., *Kilka słów o tym, jak na gruncie GDPR powierzyć dane do przetwarzania* http://gdpr.pl/slow-o-tym-gruncie-gdpr-powierzyc-dane-przetwarzania/

[2.] Bezpieczeństwo danych w chmurze: Dane przesyłane są do USA? Nie wiadomo; Źródło: gazetaprawna.pl Artykuł z dnia: 2015-10-18 Autor: T. Jurczak http://www.giodo.gov.pl/plik/id_p/9866/j/pl/

[3.] Dz. U. 2009 nr 52 poz. 417

[4.] Dz. U. 2011 nr 113 poz. 657; art. Art. 9a. 1.

[5.] Grzybowski M., *Dziewięć faktów o Dyrektywie NIS, które powinieneś znać.* http://itwadministracji.pl/numery/pazdziernik-2016/9-faktow-o-dyrektywie-nis-ktore-powinienes-znac.html

[6.] https://www.csioz.gov.pl/aktualnosci/szczegoly/komunikat-dotyczacy-regulacji-prawnych-w-zakresie-elektronicznej-dokumentacji-medycznej/

[7.] https://www.csioz.gov.pl/fileadmin/user_upload/rekomendacje_bezpieczenstwo_projekt_kwiecien2017_58e6909f16b49.pdf

[21] art. 28 ust 3. GDPR

[8.] Komisja Europejska uruchamia Tarczę Prywatności UE-USA: lepsza ochrona transatlantyckiego przepływu danych Bruksela, decyzja Komisji Europejskiej nr C(2016) 4176 12 lipca 2016 r. http://europa.eu/rapid/press-release_IP-16-2461_pl.html

[9.] Krakowiak J., *Dane osobowe: Cyberbezpieczeństwo a sektor ochrony zdrowia*, http://www.rp.pl/Zadania/302079937-Dane-osobowe-Cyberbezpieczenstwo-a-sektor-ochrony-zdrowia.html#ap-1

[10.] Rekomendacje Centrum Systemów Informacyjnych Ochrony Zdrowia w zakresie bezpieczeństwa oraz rozwiązań technologicznych stosowanych podczas przetwarzania dokumentacji medycznej w postaci elektronicznej Załącznik nr 5 https://csioz.gov.pl/fileadmin/user_upload/zalacznik_nr_5_58e690a2325ef.pdf

[11.] Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia Dz. U. 2011 nr 113 poz. 657

[12.] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Dz. U. 1997 nr 133 poz. 883

[13.] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych; Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE

Streszczenie

Wprowadzenie EDM jako obowiązującej formy dokumentacji medycznej stawia przed świadczeniodawcami konieczność podjęcia kluczowych decyzji dotyczących systemu przetwarzania elektronicznych danych medycznych. Osoby zarządzające podmiotami świadczącymi usługi zdrowotne mają dwa wyjścia: decydują się na przetwarzanie danych na terenie swojej firmy (podmiotu leczniczego) i w związku z tym godzą się na wykonywanie wielu czynności wynikających w przepisów prawa lub przekazują dane na podstawie odpowiednich umów do podmiotów profesjonalnie zajmujących się przetwarzaniem danych w innej lokalizacji, niż firma medyczna i cedują jednocześnie na podmiot otrzymujący dane wszelkie obowiązki związane z zabezpieczeniem danych.

Jedną z alternatyw mogą być, bardzo prężnie rozwijające się rozwiązania chmurowe (*cloud computing*). Uregulowano możliwość korzystania z usług podmiotów zewnętrznych w zakresie przetwarzania danych o stanie zdrowia. Jest nią powierzenie danych medycznych podmiotowi

zajmującemu się profesjonalnie przetwarzaniem danych. Ostateczną formą powierzenia danych podmiotowi zewnętrznemu i jedyną dopuszczalną jest zawarcie z nim umowy.

Bardzo istotnym elementem powierzenia danych medycznych jest odpowiedni wybór firmy świadczącej takie usługi oraz dokładne sprecyzowanie umowy ze szczególnym podkreśleniem mechanizmów zabezpieczenia danych o stanie zdrowia pacjenta zgodnym z obowiązującymi regulacjami krajowymi i unijnymi.