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

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

Dr hab. Wojciech Trąbka
Krakowska Akademia im. Andrzeja Frycza Modrzewskiego
Wydział Lekarski i Nauk o Zdrowiu, Katedra Bioinformatyki i Zdrowia Publicznego
wojciech.trabka@uj.edu.pl

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

NOWE PRAWA PACJENTA WYNIKAJĄCE Z RODO W DZIAŁALNOŚCI PODMIOTÓW LECZNICZYCH

Wprowadzenie

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[1] (ogólne rozporządzenie o ochronie danych) zwanego dalej w tekście RODO, przyznało szereg praw każdej osobie, której dane są przetwarzane, przy czym nie ma tu znaczenia fakt, czy przetwarzanie to odbywa się na podstawie przepisów prawa, czy też zgody lub umowy. Część praw jest bowiem wspólna dla wszystkich osób, których dane są przetwarzane. W przypadku przetwarzania na podstawie zgody katalog praw jest szerszy (patrz Rysunek 1).

1. Nowe prawa w regulacji RODO

Pacjent, którego dane są przetwarzane w związku z wizytą w podmiocie świadczącym usługi medyczne, ma szereg praw zagwarantowanych przepisami obowiązującymi w ochronie

[1] 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), https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A32016R0679 (data dostępu: 06.2018).

zdrowia, jak i RODO, w zakresie uprawnień do danych o nim przetwarzanych. Jako pacjent ma on prawo do informacji o stanie zdrowia i prawo dostępu do dokumentacji medycznej. Jako osoba, której dane są przetwarzane, ma określone uprawnienia wynikające z przepisów o ochronie danych. Prawo dostępu do swoich danych i prawo do ich sprostowania danych, to prawa znane z poprzedniej regulacji. Dotyczą one danych osób przetwarzanych zarówno na podstawie przepisów prawa, jak i na podstawie zgody, czy umowy.

Pojawiły się jednak nowe prawa, do których realizacji trzeba się odpowiednio przygotować. Chodzi tu przede wszystkim o prawo do przenoszenia danych, prawo do bycia zapomnianym, prawo do ograniczenia przetwarzania danych. O tym, czy osoba może z tych praw skorzystać, decyduje fakt, czy dane są przetwarzane na podstawie zgody, czy przepisu prawa. Tylko dane przetwarzane przez podmiot leczniczy na podstawie zgody dają możliwość skorzystania z powyższych praw. Schemat katalogu praw pacjenta związanych z przetwarzaniem danych wg. RODO przedstawia Rysunek 1 zamieszczony poniżej.

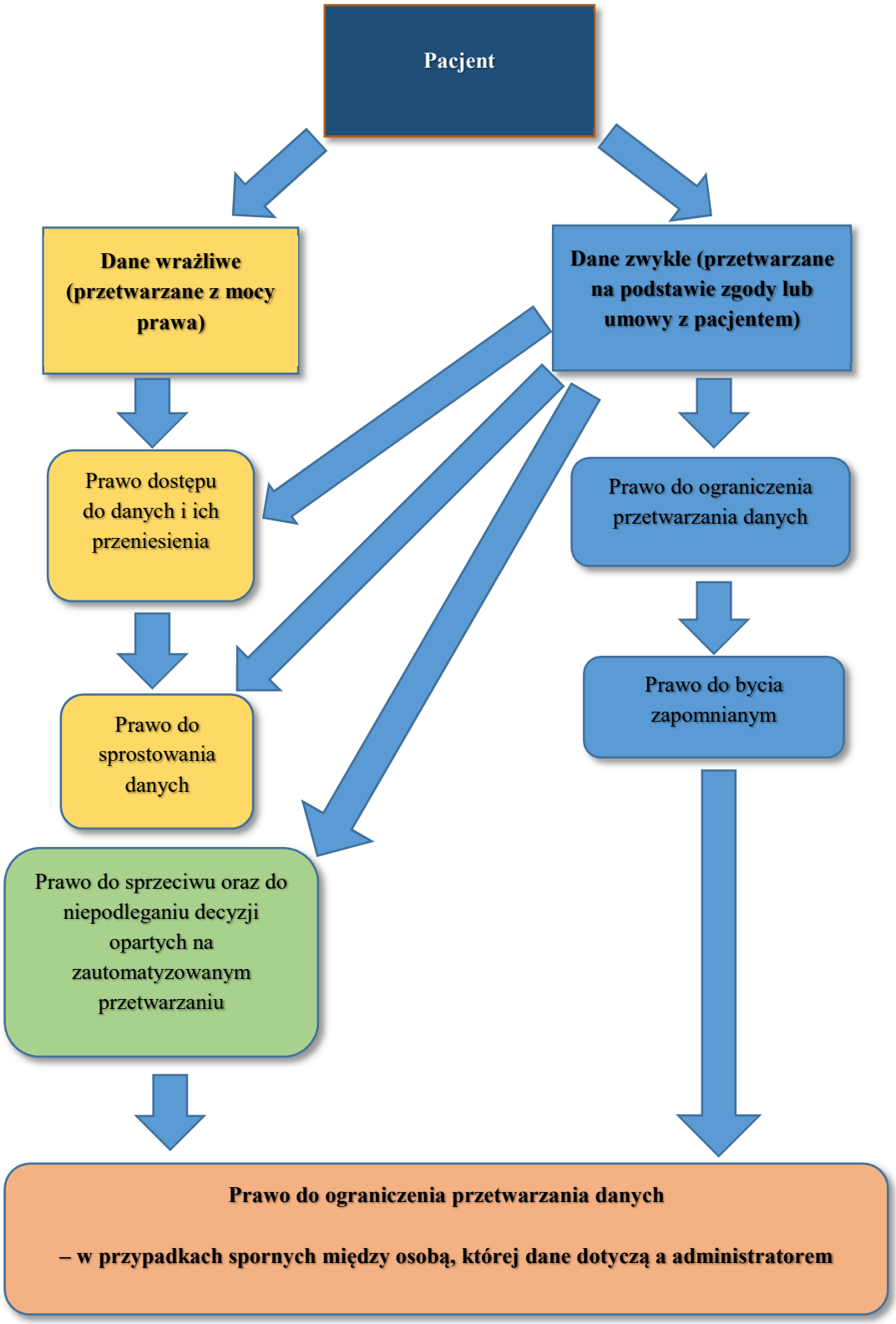
Istnieje konieczność uzyskania zgody na przetwarzanie danych pacjenta w takich przypadkach jak m.in.:

- realizacja celów marketingowych,
- prowadzenie badań klinicznych,
- realizacja innych celów naukowych,
- zautomatyzowane podejmowanie decyzji w indywidualnych sprawach,
- przekazywanie danych osobowych do państwa trzeciego, o ile administrator danych nie posiada innej podstawy prawnej przetwarzania danych osobowych pacjentów zgodnie z RODO.

Nie ma konieczności pozyskiwania zgody pacjenta, gdy przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem wskazanych w RODO warunków i zabezpieczeń[2].

[2] A. Plichta, *RODO: Czy zgoda pacjenta na przetwarzanie danych musi być na piśmie?,* https://www.zdrowie.abc.com.pl/artykuly/rodo-czy-zgoda-pacjenta-na-przetwarzanie-danych-musi-byc-na-pismie,119293.html (data dostępu: 06.2018).

Rysunek 1. Katalog praw pacjenta związanych z przetwarzaniem danych wg. RODO



Źródło: Opracowanie własne.

2. Realizacja prawa do informacji w podmiotach leczniczych

Niewątpliwie prawem, które w ochronie zdrowia będzie trudno wdrożyć w życie, jest prawo do informacji. Każda osoba fizyczna powinna mieć prawo dostępu do zebranych danych jej dotyczących oraz powinna mieć możliwość łatwego wykonywania tego prawa w rozsądnych odstępach czasu, by mieć świadomość przetwarzania i móc zweryfikować zgodność przetwarzania z prawem. Obejmuje to prawo dostępu osób, których dane dotyczą, do danych dotyczących ich zdrowia, na przykład do danych w dokumentacji medycznej zawierającej takie informacje jak diagnoza, wyniki badań, oceny dokonywane przez lekarzy prowadzących, stosowane terapie, czy przeprowadzone zabiegi. Dlatego też każda osoba, której dane dotyczą, powinna mieć prawo do wiedzy i informacji, w szczególności w zakresie celów, w jakich dane osobowe są przetwarzane, w miarę możliwości okresu przez jaki dane osobowe są przetwarzane, odbiorców danych osobowych, założeń ewentualnego zautomatyzowanego przetwarzania danych osobowych oraz, przynajmniej w przypadku profilowania, konsekwencji takiego przetwarzania. W miarę możliwości administrator danych powinien mieć możliwość udzielania zdalnego dostępu do bezpiecznego systemu, który zapewni osobie, której dane dotyczą, bezpośredni dostęp do jej danych osobowych[3].

Obowiązek informacyjny może być spełniany w formie elektronicznej na przykład za pomocą strony internetowej[4]. W szczególności powinno to dotyczyć sytuacji, gdy duża liczba podmiotów i złożoność technologiczna działań sprawiają, że osobie, której dane dotyczą, trudno będzie dowiedzieć się i zrozumieć, czy dotyczące jej dane są zbierane, przez kogo oraz w jakim celu. Jeżeli danych nie uzyskuje się od osoby, której dane dotyczą, lecz z innego źródła, należy poinformować ją o tym w rozsądnym terminie, jednak nie później, niż w ciągu miesiąca[5]. Jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą, obowiązek informacyjny powinniśmy spełnić najpóźniej przy pierwszej takiej komunikacji[6]. Ponadto obowiązek informacyjny jest wymagany przy zmianie celu

[3] Motyw 63, 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, RODO).
[4] Motyw 58, GDPR.
[5] art. 14 ust. 3 lit. a GDPR oraz motywem 61 Preambuły GDPR.
[6] art. 14 ust. 3 lit. b GDPR.

przetwarzania danych. Należy poinformować o tym osobę, której dane dotyczą, przed rozpoczęciem przetwarzania jej danych[7].

Udzielenie informacji nie jest jednak konieczne (niezależnie od źródła pozyskanych danych), jeżeli osoba, której dane dotyczą, dysponuje już tymi informacjami[8]. Od obowiązku informacyjnego można odstąpić jeżeli:

- okaże się to niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku. Sytuacja ta może zachodzić w szczególności w przypadku, gdy przetwarzanie służy celom archiwalnym w interesie publicznym, celom badań naukowych lub historycznych lub celom statystycznym, o ile obowiązek informacyjny może uniemożliwić lub poważnie utrudnić realizację celów przetwarzania[9];
- pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem unijnym lub prawem państwa członkowskiego, któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą[10];
- dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy[11].

Zagwarantowanie praw osób wiąże się często z wykonaniem szeregu czynności organizacyjno-technicznych. Wśród praw dotyczących osób korzystających ze świadczeń zdrowotnych duże problemy są związane z zagwarantowaniem prawa do informacji. Ochrona zdrowia to ten obszar, gdzie praktyczna realizacja tego obowiązku jest niezwykle skomplikowana. Rodzi się bowiem pytanie, jak wypełnić obowiązek informacyjny w stosunku do milionów osób korzystających ze świadczeń ochrony zdrowia. Każda z osób, której dane znajdują się w zbiorze, powinna być bowiem odpowiednio poinformowana zarówno o tym, że jej dane są tam przetwarzane, jak też o prawach, które w związku z tym posiada.

Niektóre podmioty w drodze regulacji prawnej zostały zwolnione z obowiązku informacyjnego m.in.:

- przepisy zezwoliły Narodowemu Funduszowi Zdrowia na nieinformowanie osób, których dane NFZ pozyskał w związku ze zgłoszeniem do ubezpieczenia

[7] art. 13 ust. 4 oraz art. 14 ust. 5 lit. a GDPR.
[8] art. 13 ust. 3 oraz art. 14 ust. 4 GDPR.
[9] art. 14 ust. 5 lit. b GDPR.
[10] art. 14 ust. 5 lit. c GDPR.
[11] art. 14 ust. 5 lit. d GDPR.

zdrowotnego i opłacaniem składek (m.in. od świadczeniodawców udzielających świadczeń opieki zdrowotnej, ZUS, czy KRUS) o każdym przypadku przetwarzania danych, jeśli przetwarzane dane osobowe były pozyskane od podmiotów innych niż osoby, których te dane dotyczą. Zwolnienie z obowiązku informowania osób, których dane NFZ przetwarza, jest możliwe, o ile przepisy prawa krajowego wydane na podstawie art. 23 Rozporządzenia 2016/679 rozwiązanie takie przewidują, a przetwarzanie danych (informacji) jest związane z interesem publicznym w obszarze zdrowia publicznego i zabezpieczenia społecznego;

- usunięto obowiązek informacyjny nałożony na podmiot prowadzący rejestr medyczny[12] w stosunku do osób, których dane dotyczą i są przetwarzane w rejestrze. Podmioty prowadzące rejestry medyczne, tj. podmioty lecznicze, w których niejednokrotnie znajduje się dziesiątki tysięcy i więcej danych osobowych, nie mają fizycznej możliwości poinformowania osób, których dane są przetwarzane w rejestrze, o przetwarzaniu w tych rejestrach danych dotyczących pacjentów. Nie dysponują bowiem aktualnymi danymi adresowymi pacjentów, a koszty tej operacji, przy bazach danych zawierających nawet kilkaset tysięcy pacjentów byłyby nieproporcjonalne w stosunku do przewidywanych korzyści.

3. Przeniesienie i archiwizacja danych medycznych

Zbiory danych o pacjentach występują zarówno w postaci papierowej, jak i elektronicznej. Do niedawna rozróżnienie to było istotne do rozstrzygnięcia o tym, czy dane podlegały ochronie, czy też nie. Dane na nośnikach papierowych były chronione tylko wówczas, jeżeli były częścią kartotek, ewidencji, itd. Obecnie rozróżnienie ma znaczenie przede wszystkim, jeżeli chodzi o realizację niektórych praw. Prawo do przeniesienia danych dotyczy tylko dokumentacji w postaci elektronicznej.

W zbiorach dotyczących dokumentacji medycznej, dokumentacja w postaci papierowej będzie dalej funkcjonowała w ochronie zdrowia do czasu upływu ustawowych okresów przechowywania. Po jego upływie dokumentacja jest niszczona lub przekazywana osobie upoważnionej[13].

[12] Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, Dz.U. 2011 nr 113 poz. 657.
[13] Wprowadzono w 2008 roku w ustawie o prawach pacjenta.

Zakresy niektórych z tych zbiorów zostały uregulowane prawnie. W przypadku dokumentacji medycznej i innych zbiorów danych pacjentów można wskazać podstawę prawną zbioru. Również regulacje dotyczące innych dziedzin życia wskazują precyzyjnie jakie dane można gromadzić. Tak np. w przypadku Kodeksu Pracy określono szczegółowo zakres danych, które pracodawca może gromadzić o pracowniku. W stosunku do poprzednio obowiązujących przepisów zakres ten został ograniczony m.in. o brak adresu zamieszkania czy imion rodziców[14].

Ponieważ administrator danych osobowych (ADO) odpowiada za wdrożenie zasad przewidzianych w RODO, a do nich należy zasada ograniczenia przechowywania, ciągłe nadzorowanie dokumentacji w postaci papierowej jest obowiązkiem wymagającym systematycznej pracy osób za to odpowiedzialnych. Nieco lepiej sytuacja wygląda w zbiorach dokumentów elektronicznych, gdzie systemy automatycznie wskazują na dokumentację, której zbliża się upłynięcie okresu przechowywania. Również inna dokumentacja, niż dotycząca pacjenta, podlega przeglądowi oraz tzw. brakowaniu[15] i archiwizacji. Zgodnie z ustawą o narodowym zasobie archiwalnym i archiwach dokumentacja stanowiąca materiał archiwalny jest przekazywana po upływie 25 lat od jej wytworzenia do właściwego archiwum państwowego, o ile organ lub jednostka organizacyjna nie przekazały wcześniej materiałów archiwalnych do archiwum państwowego (dotyczy dokumentów papierowych)[16]. Dokumenty elektroniczne natomiast, które zostały zakwalifikowane jako materiały archiwalne podlegają procesowi archiwizacji i muszą być przekazane do właściwego archiwum po upływie 10 lat od ich wytworzenia (jednak mogą zdarzyć się odstępstwa od tej reguły)[17]. Warto również w tym miejscu zauważyć, że przepisy regulują procedury przygotowania dokumentacji archiwalnej do jej przekazania do właściwego archiwum.

[14] Art.5 projekt ustawy z dnia 12 września 2017 r. https://legislacja.rcl.gov.pl/docs//2/12302951/12457706/12457707/dokument308373.pdf (data dostępu: 06.2018).

[15] **Brakowanie dokumentacji niearchiwalnej** jest to wydzielenie i przekazanie do zniszczenia tej części dokumentacji niearchiwalnej, której okres przechowywania (określony w jednolitym rzeczowym wykazie akt lub kwalifikatorze dokumentacji, o których mowa w art. 6 ust. 2 pkt 2 ustawy archiwalnej) upłynął oraz po uznaniu przez organ lub jednostkę organizacyjną, że dokumentacja niearchiwalna utraciła dla nich znaczenie, w tym wartość dowodową - Brakowanie dokumentacji niearchiwalnej w archiwum zakładowym (składnicy akt) – *Archiwum Narodowe w Krakowie*, http://www.ank.gov.pl/nadzor-archiwalny/glowne-zadania-nadzoru-archiwalnego/brakowanie-dokumentacji-niearchiwalnej-w-archi (data dostępu: 06.2018).

[16] Art. 5 Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach. Dz.U. 1983 nr 38 poz. 173.

[17] *Przekazywanie dokumentów elektronicznych do archiwum państwowego*. Archiwista 24, https://archiwista24.wordpress.com/2014/07/03/przekazywanie-dokumentow-elektronicznych-do-archiwum-panstwowego/ (data dostępu: 06.2018).

Ochrona zdrowia to obszar krzyżowania się przepisów prawnych o charakterze ogólnym oraz szczególnych (*lex specialis*) dotyczących postępowania z danymi o stanie zdrowia pacjenta. Przykładem jest np. instytucja powierzania danych uregulowana w RODO i polskich przepisach dotyczących dokumentacji medycznej. Umowa jest zawierana np. pomiędzy podmiotem świadczącym usługi z zakresu medycyny pracy a pracodawcą, który musi zapewnić badania swoim pracownikom i kandydatom na pracowników. W tym przypadku zawierana jest obok umowy głównej umowa powierzenia danych pracowników. Jeżeli pracodawca po pewnym czasie zmieni świadczeniodawcę, będzie mógł wnioskować o przeniesienie danych do innego świadczeniodawcy. Jednak dane pracowników, którzy podlegali badaniom okresowym i którym założono dokumentację medyczną, będą przetwarzane w podmiocie, który pierwotnie otrzymał dane przez 20 lat[18].

Na podstawie przykładu powyższego widać, że bardzo często podmiot leczniczy będzie miał status administratora danych osobowych mimo, że początkowo (do czasu wizyty pacjenta) otrzymał dane osobowe jako podmiot przetwarzający. Wiąże się to oczywiście z faktem, że w zależności od tego, w jakiej roli będą funkcjonowały podmioty (ich administratorzy) mimo, że będą zobligowane do przestrzegania zasady zakresu przetwarzania danych, to jednak w praktyce administrator ma do wykonania więcej zadań m.in. przy prowadzeniu różnych dokumentów (np. rejestru czynności przetwarzania lub rejestru kategorii przetwarzania) czy obowiązkach w stosunku do osób, których dane przetwarza. Jednym z kluczowych problemów, z którym musi się zmierzyć administrator podmiotu leczniczego przy przygotowaniu swojego modelu przetwarzania danych jest problem organizacji danych pod kątem podstawy prawnej przetwarzania danych. Generalnie dane w podmiotach ochrony zdrowia są przetwarzane wtedy, gdy m.in:

- przetwarzanie wynika z przepisu prawa,
- uzasadniają to cele zdrowotne, związane z zarządzaniem usługami opieki,
- dzieje się to w interesie publicznym w dziedzinie zdrowia publicznego,
- pacjent (potencjalny pacjent) wyraził zgodę[19].

[18] par.21.1 Rozporządzenie Ministra Zdrowia z dnia 29 lipca 2010 r. w sprawie rodzajów dokumentacji medycznej służby medycyny pracy, sposobu jej prowadzenia i przechowywania oraz wzorów stosowanych dokumentów Dz.U. 2010 nr 149 poz. 1002.
[19] Artykuł 9, RODO.

4. Przetwarzanie danych wrażliwych

Zakaz przetwarzania danych wrażliwych nie jest bezwzględny. Oznacza to, że w pewnych sytuacjach istnieje możliwość ich przetwarzania.

W grupie regulacji upoważniających podmiot do przetwarzania danych o stanie zdrowia należą przepisy RODO. Uregulowanie to jest o tyle istotne, że generalnie zakazane jest przetwarzanie danych wrażliwych, w tym o stanie zdrowia, kodzie genetycznym, seksualności lub orientacji seksualnej.

Dane wrażliwe dotyczące stanu zdrowia można przetwarzać zgodnie z RODO, gdy jest to niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, (do oceny zdolności pracownika do pracy), diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia.

Przetwarzanie jest możliwe także jeżeli jest to niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową.

Podział na dane osobowe: zwykłe i wrażliwe, ma istotne znaczenie, jeżeli chodzi o zapewnienie odpowiednich środków i metod zabezpieczenia danych w procesie ich przetwarzanie (m.in. sankcje, powoływanie administratora). Wśród danych przetwarzanych za zgodą znajdują się zarówno tzw. dane zwykłe, jak też dane wrażliwe. Jednak ochrona zdrowia - jak już pisano powyżej - ma daleko idącą specyfikę. Dotyczy ona problemu celu przetwarzania danych o stanie zdrowia. Jeżeli osoba bierze udział w jakimkolwiek badaniu lub w dobrowolnym eksperymencie, to staje się pacjentem. Część pozyskanych o niej danych zostanie wykorzystana do opisu samego badania i stają się one częścią dokumentacji medycznej i przez określony czas podlegają przepisom szczególnym, natomiast część może być wykorzystywana w innym celu, np. marketingowym. Zbiory tworzone do tego celu są tworzone na podstawie zgody lub umowy, z której wynika powiadamianie pacjenta o np. nowych metodach leczenia lub lekach.

Może zaistnieć sytuacja, w której pacjent sprzedaje lub przekazuje dane o stanie zdrowia do przetwarzania, przez podmioty, które prowadzą działalność gospodarczą polegającą na analizie danych. Wówczas dane osobowe będące w dyspozycji pacjenta i przekazane do przetwarzania przez podmiot przetwarzający dane w celach komercyjnych lub naukowych będzie musiał respektować instytucje RODO w zakresie przekazywania lub usunięcia danych. Należy również zauważyć fakt, że przepisy RODO nie mają zastosowania do przetwarzania danych osobowych przez osobę fizyczną w ramach działalności czysto osobistej lub domowej tj. bez związku z działalnością zawodową lub handlową. Rozporządzenie ma jednak zastosowanie do administratorów lub podmiotów przetwarzających, którzy udostępniają środki przetwarzania danych osobowych na potrzeby takiej działalności osobistej lub domowej[20] (np. udostępniają oprogramowanie w chmurze umożliwiające gromadzenie i przetwarzania danych o stanie zdrowia). Taki zapis jednoznacznie wyklucza sytuacje, w których pozyskiwano dane o stanie zdrowia udostępniając „bezpłatnie" miejsce na dane na platformach chmurowych.

5. Tajemnice a ochrona danych

Tajemnica, to określona przez przepisy wiadomość, której poznanie lub ujawnienie jest zakazane przez prawo[21]. Obszar ochrony zdrowia to miejsce, w którym funkcjonują osoby objęte różnymi rodzajami tajemnic. Ma to na celu zapewnienie bezpieczeństwa danych pacjenta przetwarzanych w podmiotach leczniczych. Pacjent ma prawo do zachowania w tajemnicy przez osoby wykonujące zawód medyczny, w tym udzielające mu świadczeń zdrowotnych, informacji z nim związanych, a uzyskanych w związku z wykonywaniem zawodu medycznego. Tajemnice zostały uregulowane prawnie przepisami dotyczącymi funkcjonowania zawodów medycznych tj.: lekarzy i dentystów, pielęgniarek i położnych, diagnostów, fizjoterapeutów, aptekarzy, felczerów i psychologów[22].

Tajemnica dotyczy również danych i informacji zawartych w dokumentacji medycznej. Do przetwarzania danych zawartych w dokumentacji medycznej w celu ochrony zdrowia, udzielania oraz zarządzania udzielaniem świadczeń zdrowotnych, utrzymania systemu

[20] Motyw 18 RODO.
[21] *Słownik PWN*, https://sjp.pwn.pl/slowniki/tajemnica.html (data dostępu: 06.2018).
[22] lekarz i lekarz dentysta – art. 40 ustawy z 5.12.1996 r. o zawodach lekarza i lekarza dentysty[7]; – pielęgniarka i położna – art. 17 ustawy z 15.7.2011 r. o zawodach pielęgniarki i położnej[8]; – felczer – art. 7 ustawy z 20.7.1950 r. o zawodzie felczera[9]; – diagnosta laboratoryjny – art. 29 ustawy z 27.7.2001 r. o diagnostyce laboratoryjnej[10]; – farmaceuta – art. 21 pkt 2 ustawy z 19.4.1991 r. o izbach aptekarskich[11]; – psycholog – art. 14 ustawy z 8.6.2001 r. o zawodzie psychologa i samorządzie zawodowym psychologów.

teleinformatycznego, w którym przetwarzana jest dokumentacja medyczna, i zapewnienia bezpieczeństwa tego systemu, są uprawnione:

1) osoby wykonujące zawód medyczny;
2) inne osoby wykonujące czynności pomocnicze przy udzielaniu świadczeń zdrowotnych, a także czynności związane z utrzymaniem systemu teleinformatycznego, w którym przetwarzana jest dokumentacja medyczna, i zapewnieniem bezpieczeństwa tego systemu, na podstawie upoważnienia administratora danych. Osoby te są związane tajemnicą także po śmierci pacjenta.

Tak więc, poza osobami wykonującymi zawód medyczny, także inne osoby mogą być dopuszczone do przetwarzania danych, ale tylko na podstawie upoważnienia wydanego przez administratora danych. Jest to jednocześnie jeden w wymogów bezpieczeństwa, by dostęp do danych osobowych miały wyłącznie osoby fizyczne działające z upoważnienia administratora lub podmiotu przetwarzającego.

6. Dostęp do dokumentacji medycznej

Problem praktyczny dostępu do dokumentacji medycznej w podmiotach zatrudniających wiele osób objętych tajemnicą zawodową, może dotyczyć dostępu do dokumentacji pacjentów tylko przez osoby, które świadczą usługi „swoim pacjentom". Jeżeli dostęp dotyczy pacjentów zapisanych do jednej poradni, gdzie zatrudnionych jest kilku lekarzy np. specjalistów, dokumentacja jest uzupełniana przez różne osoby i nie ma problemu z dostępem wszystkich świadczących usługi w poradni. Inaczej wygląda sytuacja dostępu do danych zawartych w dokumentacji znajdującej się w innych poradniach niż ta, gdzie zatrudniony jest lekarz lub inna osoba świadcząca usługi medyczne. W tym przypadku musi być to uzasadnione albo dobrem terapii, albo obowiązkami nie mającymi związku z leczeniem pacjenta np. tworzeniem analizy prowadzonej pod katem wymagań prawnych dokumentacji przez uprawnionego pracownika. W takim przypadku potrzebne jest upoważnienie administratora danych. Dotyczy to również sytuacji, gdy ktoś w ramach pracy zawodowej musi uzyskać dostęp do dokumentacji innych pacjentów (np. prezesi ds. medycznych w spółkach prowadzących podmioty lecznicze). Upoważnienie jest również niezbędne w przypadku dostępu do danych dotyczących osób świadczących usługi zdrowotne np. dla kierownika poradni zatrudniającej lub mającej umowy cywilnoprawne z osobami świadczącymi usługi zdrowotne.

W przypadku powierzenia danych o stanie zdrowia podmiotom zewnętrznym, podmiot, który otrzymuje dane, zostaje zobowiązany do zapewnienia tajemnicy. Zarówno przepisy

RODO, jak i ustawy o prawach pacjenta regulują problem objęcia tajemnicą osób występujących po stronie podmiotu przetwarzającego na podstawie umowy z administratorem.

Podmiot ten przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora. Obok innych wymogów, które przewidują przepisy, zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy. Bezpośrednio do przepisów RODO odwołuje się ustawa o prawach pacjenta. Podmiot udzielający świadczeń zdrowotnych może w drodze umowy powierzyć przetwarzanie danych podmiotowi przetwarzającemu. Umowa taka powinna spełniać wymagania RODO[23].

Ustawa o systemie informacji w ochronie zdrowia[24] zobowiązuje do tajemnicy podmioty wyspecjalizowane w zapewnianiu obsługi technicznej systemów teleinformatycznych, w przypadku powierzania danych o stanie zdrowia (m.in. wszystkie moduły systemu, oraz rejestry). Tajemnica dotyczy informacji związanych ze świadczeniobiorcami uzyskany w związku z powierzeniem przetwarzania danych przetwarzanych w systemach. Podmioty te są związane tajemnicą także po śmierci świadczeniobiorcy.

Do niedawana funkcjonowała także tzw. tajemnica informatyczna[25] - osoby, które zostały upoważnione do przetwarzania danych, były obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia.

Obecnie RODO wymaga, aby dane osobowe były przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność. Osoby upoważnione do przetwarzania danych są zobowiązane do zachowania ich poufności, nawet jeśli nie złożyły stosownych oświadczeń. Taki obowiązek wynika bowiem wprost z przepisów RODO. Każda osoba, która działa z upoważnienia administratora lub podmiotu przetwarzającego i ma dostęp do danych osobowych, może je bowiem przetwarzać wyłącznie na polecenie administratora danych[26].

W stosunku do pracowników tajemnica została uregulowana w Kodeksie Pracy. Obowiązkiem pracownika jest zachowanie w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę[27]. Obowiązek został sformułowany dość ogólnie,

[23] w art. 24 ust. 4, RODO
[24] Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia Dz.U. 2011 nr 113 poz. 657.
[25] Art. 39 ust 2 uchylonej Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
[26] A. Kręcisz-Sarna, *Oświadczenia o zachowaniu danych osobowych w tajemnicy – czy aktualizować je w związku z RODO*?, https://www.poradyodo.pl/administracja-publiczna/oswiadczenia-o-zachowaniu-danych-osobowych-w-tajemnicy-czy-aktualizowac-je-w-zwiazku-z-rodo-8332.html# (data dostępu. 06.2018).
[27] 100 § 2 pkt 4 Kodeks Pracy.

jednak przyjmuje się, iż dotyczy on takich informacji, do których pracownik ma dostęp, a ich ujawnienie mogłoby sprowadzić, choćby potencjalne, niebezpieczeństwo spowodowania szkody dla pracodawcy. Tajemnica wiąże pracownika od momentu zawarcia umowy o pracę i nie jest w tym zakresie bezwzględnie wymagane podejmowanie przez pracodawcę dodatkowych czynności (np. zawieranie umów o zachowaniu poufności), co nie oznacza, iż strony stosunku pracy nie mogą zawrzeć takiej umowy. W interesie pracodawcy jest to, aby pracownik wiedział, jakie konkretnie dane i informacje są dla pracodawcy na tyle istotne, że ich ujawnienie mogłoby narazić pracodawcę na szkodę. W związku z powyższym pracodawca powinien wskazać (przykładowo w umowie o pracę lub w regulaminie pracy) rodzaj (zakres) wiadomości, których nie należy ujawniać[28]. Podsumowując, należy stwierdzić, że pracownik musi zostać poinformowany, że przyjęte dla celów bezpieczeństwa rozwiązania wdrożone przez firmę są dla niej istotne a ich ujawnienie mogłoby przynieść szkodę.

W związku z tym, że przepis umożliwiający zobowiązanie wszystkich osób upoważnionych do przetwarzania danych w podmiocie do zachowania w tajemnicy również sposobów zabezpieczenia i zastosowanych rozwiązań technicznych przestał obowiązywać, można odwołać się w tym przypadku do tajemnicy przedsiębiorstwa.

Podsumowanie

RODO przyznało szereg praw każdej osobie, której dane są przetwarzane. Prawo dostępu do danych i prawo do sprostowania danych, to prawa znane z poprzedniej regulacji. Dotyczą one danych osób przetwarzanych zarówno na podstawie przepisów prawa, jak i na podstawie zgody, czy umowy. Pojawiły się jednak nowe prawa, do których realizacji trzeba się odpowiednio przygotować. Chodzi tu przede wszystkim o prawo do przenoszenia danych, prawo do bycia zapomnianym i prawo do ograniczenia przetwarzania danych.

Wśród praw dotyczących osób korzystających ze świadczeń zdrowotnych, duże problemy są związane z zagwarantowaniem prawa do informacji. Ochrona zdrowia, to ten obszar, gdzie praktyczna realizacja tego obowiązku jest niezwykle skomplikowana. Rodzi się bowiem pytanie, jak wypełnić obowiązek informacyjny w stosunku do milionów osób korzystających ze świadczeń ochrony zdrowia. Każda z osób, której dane znajdują się w

[28] M. Szuszczyński, *Jak zobowiązać pracownika do zachowania poufności?*, Biuletyn Prawo Pracy i HR, https://www.bdo.pl/pl-pl/publikacje/biuletyn-prawo-pracy-i-hr/2017/jak-zobowiazac-pracownika-do-zachowania-poufnosci (data dostępu: 06.2018).

zbiorze, powinna być bowiem odpowiednio poinformowana zarówno o tym, że jej dane są tam przetwarzane, jak też o prawach, które w związku z tym posiada.

Niezwykle istotne dla systemu opieki zdrowotnej są regulacje RODO związane z przetwarzaniem danych wrażliwych. Generalnie zakazane jest przetwarzanie danych wrażliwych, w tym o stanie zdrowia, kodzie genetycznym, seksualności lub orientacji seksualnej. Regulacje RODO dopuszczają możliwość przetwarzania takich danych pod określonymi warunkami np. gdy jest to niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, (do oceny zdolności pracownika do pracy) diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej.

Literatura

[1] *Archiwum Narodowe w Krakowie*, http://www.ank.gov.pl/nadzor-archiwalny/glowne-zadania-nadzoru-archiwalnego/brakowanie-dokumentacji-niearchiwalnej-w-archi
[2] Kręcisz-Sarna A., *Oświadczenia o zachowaniu danych osobowych w tajemnicy – czy aktualizować je w związku z RODO*?, https://www.poradyodo.pl/administracja-publiczna/oswiadczenia-o-zachowaniu-danych-osobowych-w-tajemnicy-czy-aktualizowac-je-w-zwiazku-z-rodo-8332.html#
[3] Plichta A., *RODO: Czy zgoda pacjenta na przetwarzanie danych musi być na piśmie?*, https://www.zdrowie.abc.com.pl/artykuly/rodo-czy-zgoda-pacjenta-na-przetwarzanie-danych-musi-byc-na-pismie,119293.html
[4] *Projekt ustawy o ochronie danych osobowych z dnia 12 września 2017 r. (Przepisy wprowadzające ustawę o ochronie danych osobowych)*, https://legislacja.rcl.gov.pl/docs//2/12302951/12457706/12457707/dokument308373.pdf
[5] Rozporządzenie Ministra Zdrowia z dnia 29 lipca 2010 r. w sprawie rodzajów dokumentacji medycznej służby medycyny pracy, sposobu jej prowadzenia i przechowywania oraz wzorów stosowanych dokumentów Dz.U. 2010 nr 149 poz. 1002
[6] 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, RODO).
[7] *Słownik PWN*, https://sjp.pwn.pl/slowniki/tajemnica.html
[8] Szuszczyński M., *Jak zobowiązać pracownika do zachowania poufności?*, Biuletyn Prawo Pracy i HR, https://www.bdo.pl/pl-pl/publikacje/biuletyn-prawo-pracy-i-hr/2017/jak-zobowiazac-pracownika-do-zachowania-poufnosci
[9] Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach. Dz.U. 1983 nr 38 poz. 173
[10] Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy, Dz.U. 1974 nr 24 poz. 141
[11] Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, Dz.U. 2011 nr 113 poz. 657

[12] *Przekazywanie dokumentów elektronicznych do archiwum państwowego*, Archiwista 24, https://archiwista24.wordpress.com/2014/07/03/przekazywanie-dokumentow-elektronicznych-do-archiwum-panstwowego/

Streszczenie

Pacjent, którego dane są przetwarzane w związku z wizytą w podmiocie świadczącym usługi medyczne, ma szereg praw zagwarantowanych przepisami obowiązującymi w ochronie zdrowia, jak i RODO, w zakresie uprawnień do danych o nim przetwarzanych.

Prawo dostępu do danych i prawo do sprostowania danych, to prawa znane z poprzedniej regulacji. Dotyczą one danych osób przetwarzanych zarówno na podstawie przepisów prawa, jak i na podstawie zgody czy umowy. Pojawiły się jednak nowe prawa, do których realizacji trzeba się odpowiednio przygotować. Chodzi tu przede wszystkim o prawo do przenoszenia danych, prawo do bycia zapomnianym, prawo do ograniczenia przetwarzania danych.

Wśród praw dotyczących osób korzystających ze świadczeń zdrowotnych duże problemy są związane z zagwarantowaniem prawa do informacji. Ochrona zdrowia to ten obszar, gdzie praktyczna realizacja tego obowiązku jest niezwykle skomplikowana.

Niezwykle istotne dla systemu opieki zdrowotnej są regulacje RODO związane z przetwarzaniem danych wrażliwych. Generalnie zakazane jest przetwarzanie danych wrażliwych w tym o stanie zdrowia, kodzie genetycznym, seksualności lub orientacji seksualnej. Regulacje RODO dopuszczają możliwość przetwarzania takich danych pod określonymi warunkami np. gdy jest to niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej.

Słowa kluczowe

RODO, katalog praw osób, których dane dotyczą, dane wrażliwe, dokumentacja medyczna, tajemnice zawodowe