

Powierzenie przetwarzania osobowych danych medycznych a perspektywy prowadzenie dokumentacji medycznej w postaci elektronicznej

Mateusz Kamiński

28 czerwca 2007 r. wejdą w życie przepisy o prowadzeniu dokumentacji medycznej w postaci elektronicznej. Regulację taką zawarto w rozdziale siódmym rozporządzenia Ministra Zdrowia z dnia 21 grudnia 2006 r. w sprawie rodzajów i zakresu dokumentacji medycznej w zakładach opieki zdrowotnej oraz sposobu jej przetwarzania (Dz.U. 2006 nr 247 poz. 1819). Nowe przepisy określają ramy prawne dla zastosowania technik informatycznych do rejestrowania i przechowywania informacji o stanie zdrowia pacjenta i przebiegu leczenia. Samo ustalenie zasad prowadzenia dokumentacji medycznej w postaci elektronicznej było unormowaniem długo oczekiwanym przez osoby zarządzające zakładami opieki zdrowotnej. Kierujący takimi podmiotami chcieli mieć możliwość archiwizowania na nośnikach informatycznych ogromnej ilości dokumentów medycznych przechowywanych dotąd w formie papierowych wydruków. Liczono m.in. na to, że uda się ograniczyć koszty związane z koniecznością utrzymywania w zakładach opieki zdrowotnej pomieszczeń przeznaczonych na archiwa. Obecnie, gdy znamy już ostateczny kształt uregulowań prawnych prowadzenia dokumentacji medycznej w postaci elektronicznej, możemy pokusić się o próbę oceny perspektyw wdrożenia nowych rozwiązań w praktyce.

Jednym z istotnych aspektów stosowania technologii informatycznych w służbie zdrowia jest przetwarzanie danych wrażliwych. Możliwość zastosowania określonych rozwiązań informatycznych w tej dziedzinie musi być zawsze oceniana przez pryzmat przepisów o ochronie

danych osobowych. Nie ulega wątpliwości, że zakłady opieki zdrowotnej wdrażając, ale i korzystając z systemów informatycznych służących do prowadzenia dokumentacji medycznej w postaci elektronicznej, będą często opierać się na rozwiązaniach oferowanych przez podmioty zewnętrzne. Przemawiać będą za tym nie tylko względy finansowe, ale i organizacyjne. W praktyce będzie to wymagało ujawnienia takim podmiotom informacji o pacjentach, które zawarte są w dokumentacji medycznej. Dojdzie tym samym do wyjawienia przedsiębiorstwom informatycznym danych wrażliwych – czyli osobowych danych medycznych. Ujawnienie takie w relacjach outsourcingowych¹ następuje w drodze powierzenia przetwarzania danych. Jednak w odniesieniu do danych wrażliwych odwołanie się do tej instytucji prawnej może wzbudzać poważnie wątpliwości. Celem niniejszego opracowania jest zbadanie:

- czy w świetle obowiązujących przepisów dopuszczalne jest powierzenie przetwarzania osobowych danych medycznych zawartych w dokumentacji medycznej,
- jeśli tak, to jakie warunki powinny zostać spełnione, aby takie powierzenie mogło mieć miejsce,
- ocena możliwości zastosowania w praktyce istniejących regulacji prawnych sposobu prowadzenia dokumentacji medycznej w postaci elektronicznej.

Analiza zagadnienia wymaga na wstępie wskazania aktów prawnych, które odnoszą się do przetwarzania osobowych danych medycznych oraz prowadzenia dokumentacji medycznej w zakładach opieki zdrowotnej. Do unormowań o charakterze ogólnym należą w tym przypadku Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych oraz ustawa o ochronie danych osobowych z 29 sierpnia 1997 r. (Dz. U. 1997 nr 133 poz. 833 z późn. zm.). Przepisy szczególne normujące omawianą kwestię znajdują się natomiast w ustawie o zakładach opieki zdrowotnej (Dz. U. 1991 nr 91 poz. 408 z późn. zm.) oraz rozporządzeniu Ministra Zdrowia z dnia 21 grudnia 2006 r. w sprawie rodzajów i zakresu dokumentacji medycznej w zakładach opieki zdrowotnej oraz sposobu jej przetwarzania (Dz.U. 2006 nr 247 poz. 1819), ustawie z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (Dz. U. 1997 nr 28 poz. 152 z późn. zm.), ustawie o zawodach pielęgniarki i położnej z 5 lipca 1996 r. (Dz. U. 1996 nr 91 poz. 410 z późn. zm.). Znaczenie dla oceny dopuszczalności powierzenia przetwarzania danych wrażliwych mają również uregulowania ustawy z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego (Dz.U. 1994 poz. 111 poz. 535 z późn. zm.). Nie ma więc aktu prawnego, który kompleksowo regulowałby kwestię przetwarzania danych

¹**Outsourcing** - wykorzystywanie zasobów zewnętrznych, zlecenie wyspecjalizowanym podmiotom zewnętrznym procesów niezbędnych dla funkcjonowania własnego przedsiębiorstwa, które zostaną tam zrealizowane efektywniej niż byłoby to możliwe we własnym zakresie <http://pl.wikipedia.org/wiki/Outsourcing> (2007-06-09)

osobowych pacjentów. Unormowania prawne odnoszące się do poruszanego zagadnienia dotyczą bezpośrednio danych wrażliwych (sensytywnych), dokumentacji medycznej i tajemnic zawodowych zawodów medycznych.

Dla jasności dalszego wywodu niezbędne jest dokonanie pewnych ustaleń terminologicznych, bowiem zarówno pozaustawowy termin „osobowe dane medyczne” jak i ustawowe określenia „powierzenie przetwarzania danych osobowych”, „udostępnienie danych osobowych” oraz „udostępnienie dokumentacji medycznej” wymagają kilku słów komentarza.

W tytule niniejszego opracowania użyto terminu „osobowe dane medyczne”. Nie jest to termin języka prawnego. W niniejszym tekście mianem tym określa się dane osobowe o „stanie zdrowia, nałogach, kodzie genetycznym i życiu seksualnym”. Przyjęcie tak szerokiego zakresu znaczeniowego pojęcia uzasadnia treść art. 27 ust. 1 ustawy o ochronie danych osobowych oraz to, iż celem niniejszej analizy jest ocena możliwości powierzenia przetwarzania informacji o pacjentach przez podmioty działające na terenie Rzeczypospolitej Polskiej. Fakt, iż w Dyrektywie 95/46 WE wśród danych sensytywnych nie wymieniono danych o nałogach i kodzie genetycznym nie ma kluczowego znaczenia dla prowadzonych poniżej rozważań. Posłużenie się pojęciem „osobowych danych medycznych”, a nie używanym niekiedy w literaturze terminem „dane medyczne”² podyktowane jest zarówno troską o precyzję wywodu, jak i względami praktyki. Pojęcie „dane medyczne” ma zbyt szeroki zakres znaczeniowy, gdyż obejmuje nie tylko informacje o osobach. Za „dane medyczne” trzeba bowiem uznać zarówno dane osobowe pacjentów, jak i np. dane o ilości opakowań leku znajdujących się w szpitalu. Względami praktyki także przemawiają za posługiwaniem się w niniejszym tekście pojęciem „osobowych danych medycznych”, jako danych osób żyjących. Jest wprawdzie oczywiste, że podmioty świadczące usługi medyczne są obowiązane przechowywać zarówno dane osobowe pacjentów żyjących, jak i informacje o zmarłych, których polska ustawa o ochronie danych osobowych nie chroni³. Jednak w praktyce racjonalne jest przyjęcie, iż w odniesieniu do przetwarzania wszystkich danych o pacjentach jednostka służby zdrowia z ostrożności powinna przestrzegać przepisów o ochronie danych osobowych. Niekiedy bowiem informacje o zmarłym mogą zawierać dane osobowe żyjących członków jego rodziny. Z tej to przyczyny w dalszych rozważaniach używane będzie pojęcie – „osobowe dane medyczne”.

Inne użyte w tytule pojęcie to „powierzenie przetwarzania danych osobowych”. Nie ma wprawdzie definicji legalnej tego terminu, jednak art. 17 Dyrektywy 95/46 oraz w art. 31 ustawy o ochronie danych osobowych, pozwalają na wskazanie istotnych cech powierzenia

² M. Jackowski, *Ochrona danych medycznych*

³ Szerzej na ten temat J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Kraków 2007, s. 350-351, A. Drozd, *Ustawa o ochronie danych osobowych. Komentarz*, W-wa 2004, s 46.

przetwarzania danych osobowych. W prawie wspólnotowym rozumiane jest ono jako przetwarzanie danych w imieniu administratora. To on powinien wybrać na przetwarzającego podmiot, który gwarantuje odpowiedni poziom zabezpieczenia danych. Zgodnie z art. 17 ust. 3 Dyrektywy 95/46/WE, podstawą powierzenia powinna być umowa lub akt prawny, dla celów dowodowych sporządzony na piśmie lub w innej równorzędnej formie. Z aktu stanowiącego podstawę powierzenia przetwarzania danych powinno wynikać, że przetwarzający będzie działać wyłącznie na polecenie administratora danych. Przetwarzający ma również obowiązek wprowadzić odpowiednie środki techniczne i organizacyjne w celu ochrony danych. Podobnie instytucję „powierzenia przetwarzania danych” reguluje art. 31 ustawy o ochronie danych osobowych. W ustępie 1 tego przepisu zaznaczono jednak, że podstawą powierzenia może być tylko umowa. Podmiot, któremu dane powierzono może je, zgodnie z ustępem 2, przetwarzać „wyłącznie w zakresie i celu przewidzianym w umowie”. Powierzenie może dotyczyć tylko określonych w umowie czynności związanych z przetwarzaniem danych. Rolą administratora jest zaś decydowanie nie tylko o celach i środkach przetwarzania powierzonych danych, a więc i określenie czynności, które powierza. Cechą charakterystyczną powierzenia jest to, że administrator ujawniając dane innemu podmiotowi, nie traci nad nimi kontroli. Tym różni się powierzenie od udostępnienia danych osobowych, które polega również na ujawnieniu danych osobowych innemu podmiotowi. Jednak w przypadku udostępnienia administrator danych nie może już decydować o celach i środkach przetwarzania udostępnionych danych. Oczywiście dane z natury swojej pozostają także i u udostępniającego, ale to jak będzie postępował z tymi danymi podmiot, któremu te dane udostępniono, nie podlega już kontroli administratora danych. W tym przypadku podmiot, któremu dane udostępniono sam staje się bowiem drugim administratorem tych samych danych.

Dla dalszych rozważań istotne jest także przybliżenie pojęcia „udostępnienia dokumentacji medycznej”. Terminu tego nie należy mylić z „udostępnieniem danych osobowych”. Samo pojęcie „dokumentacji medycznej”, zgodnie z art. 18 d ust. 1 pkt 5 ustawy o zakładach opieki zdrowotnej, oznacza „określone w ustawie (o zakładach opieki zdrowotnej) oraz przepisach odrębnych dane i informacje medyczne odnoszące się do stanu zdrowia pacjenta lub udzielonych mu w zakładzie opieki zdrowotnej świadczeń zdrowotnych”. O tym, że w dokumentacji medycznej znajdują się dane wrażliwe stanowi zaś, art. 18 ust. 2 a wspomnianej ustawy, zgodnie z którym, taka dokumentacja „zawiera co najmniej:

- 1) oznaczenie pacjenta, pozwalające na ustalenie jego tożsamości;
- 2) oznaczenie zakładu opieki zdrowotnej ze wskazaniem komórki organizacyjnej zakładu, w której udzielono świadczeń zdrowotnych;

3) opis stanu zdrowia pacjenta, o którym mowa w pkt 1, lub udzielonych mu świadczeń zdrowotnych;

4) datę sporządzenia”.

Właśnie opis stanu zdrowia pacjenta zawiera „osobowe dane medyczne”. Ustawodawca nie zdefiniował natomiast samego pojęcia „udostępnienia dokumentacji medycznej”. Dlatego też w myśl powszechnie przyjętych zasad wykładni, trzeba w tym przypadku definiować „udostępnienie”, zgodnie z przyjętym w języku potocznym rozumieniem tego słowa.⁴ „Udostępnieniem dokumentacji” będzie wobec tego „umożliwienie jej poznania”⁵ podmiotowi innemu niż dysponujący nią. W przypadku „udostępnienia dokumentacji medycznej” dochodzi więc do ujawnienia osobowych danych medycznych. Przepisy ustawy o zakładach opieki zdrowotnej nie odwołują się jednak do pojęcia „udostępnienia danych osobowych”, ani też do pojęcia „powierzenia przetwarzania” takich danych. Z unormowań tej ustawy nie wynika charakter prawny takiego ujawnienia informacji o osobie. Wskazane wyżej przepisy ustawy o zakładach opieki zdrowotnej nie są *sensu stricto* przepisami szczególnymi regulującymi ochronę danych osobowych. Unormowania te dotyczą ujawniania dokumentów, a nie zawartych w nich danych. Oceniając je jednak przez pryzmat zasad ochrony danych osobowych należy uznać, że w niektórych przypadkach takie ujawnienie może zostać zakwalifikowane jako „udostępnienie danych osobowych”, w innych zaś jako „powierzenie przetwarzania” takich danych.

Truizmem jest stwierdzenie, że prowadzenie dokumentacji medycznej w postaci elektronicznej będzie wymagało ujawnienia zawartych w niej danych informatykom. Okoliczność ta wymaga jednak w tym przypadku podkreślenia. „Osobowe dane medyczne” stanowią bowiem specyficzną kategorię danych. Przetwarzający je to głównie przedstawiciele zawodów medycznych, na których, poza obowiązkiem zachowania danych osobowych w tajemnicy, określonym w art. 39 ust. 2 ustawy o ochronie danych osobowych, ciążyą także obowiązki zachowania tajemnicy zawodowej. Wynikają one w przypadku zawodów lekarza i lekarza dentysty z art. 40 ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (Dz. U. 1997 nr 28 poz. 152 z późn. zm.), a w przypadku zawodów pielęgniarki i położnej z art. 21 ustawy o zawodach pielęgniarki i położnej z 5 lipca 1996 r. (Dz. U. 1996 nr 91 poz. 410 z późn. zm.). Lekarz, pielęgniarka i położna mają „obowiązek do zachowania w tajemnicy informacji związanych z pacjentem, a uzyskanych w związku z wykonywaniem zawodu”. Do zachowania tych tajemnic zobowiązują także deontologie zawodowe. Stosowne regulacje znajdują się w Kodeksie Etyki Lekarskiej⁶

⁴ Por. L. Morawski, *Zasady wykładni prawa*, Toruń 2006, s. 89-93.

⁵ Definicje PWN wersja 6.0.

⁶ Por. http://www.nil.org.pl/xml/nil/wladze/str_zl/zjazd7/kel (2007-06-09)

oraz w Kodeksie Etyki Zawodowej Pielęgniarki i Położnej Rzeczypospolitej Polskiej⁷. Świadomość istnienia tych tajemnic jest w środowisku medycznym dużo większa niż obowiązku wynikającego z art. 39 ust. 2 ustawy o ochronie danych osobowych. Jednak oczywistym jest, że personelu niemedycznego zakładów opieki zdrowotnej tajemnice zawodowe nie obowiązują. Informatyk, pracownik rejestracji, czy też pracownik archiwum szpitala nie są związani takimi tajemnicami. Tym bardziej tajemnice te nie wiążą informatyków zatrudnionych w podmiotach zewnętrznych świadczących usługi zakładom opieki zdrowotnej. Należy więc zastanowić się, jak wobec tego kształtuje się możliwość powierzenia przetwarzania „osobowych danych medycznych” takim osobom.

Odpowiedź na pytanie o dopuszczalność powierzenia przetwarzania osobowych danych medycznych musi poprzedzić wskazanie kręgu podmiotów, które mają prawo do przetwarzania takich informacji w świetle przepisów o ochronie danych osobowych. Podmiot, któremu dane zostaną powierzone powinien bowiem dysponować takim uprawnieniem. Trzeba zaznaczyć, że dokonywanie jakichkolwiek operacji na takich danych objęte jest generalnym zakazem. Tylko w ściśle określonych przypadkach w drodze wyjątku wolno takie informacje przetwarzać. Wspomniany zakaz wprowadzono zarówno w prawie polskim, jak i w unormowaniach Wspólnot Europejskich. Przyjęte w obu porządkach prawnych są do siebie bardzo podobne, ale nie tożsame. Artykuł 8 ust. 3 Dyrektywy 46/95 WE stanowi, że statuującego zakaz „Ustępu pierwszego nie stosuje się w przypadku, gdy przetwarzanie danych wymagane jest dla celów medycyny zapobiegawczej, diagnostyki medycznej, świadczenia opieki lub leczenia, administrowania opieką zdrowotną i kiedy takie dane przetwarzane przez podmiot służby zdrowia, zgodnie z przepisami prawa krajowego lub zasadami określonymi przez właściwe krajowe instytucje podlegający obowiązkowi zachowania tajemnicy zawodowej lub inny podmiot, na którym ciąży równorzędny obowiązek zachowania tajemnicy”⁸. Prawodawca wspólnotowy wyznacza tym samym bardzo wysoki poziom ochrony danych. Uregulowanie to uchyla mianowicie zakaz przetwarzania osobowych danych medycznych ze względu na cel *sensu stricto* medyczny lub cel, jakim jest administrowanie służbą zdrowia, któremu przetwarzanie miałyby służyć i to wyłącznie w przypadku, gdy na podmiocie, który takie dane przetwarza, spoczywa co najmniej obowiązek

⁷ Por. <http://www.izbapiel.org.pl/index.php?id=8> (2007-06-09)

⁸ Tłumaczenie artykułu 8 ust. 3 Dyrektywy dokonane przez autora na podstawie tekstów autentycznych Dyrektywy 95/46 WE w językach niemieckim i angielskim. Oficjalne tłumaczenie tej dyrektywy na język polski jest niezgodne z tłumaczeniami w innych językach. Nie wynika z niego bowiem, że przetwarzać dane medyczne mogą tylko podmioty służby zdrowia, zgodnie z przepisami prawa krajowego lub zasadami określonymi przez właściwe krajowe instytucje podlegające obowiązkowi zachowania tajemnicy zawodowej lub inne podmioty, na których ciąży równorzędny obowiązek zachowania tajemnicy, ale pod warunkiem, że przetwarzanie takie dokonywane jest w celu medycznym lub w celu administrowania opieką zdrowotną. Z tłumaczenia oficjalnego można błędnie wnosić, iż możliwe jest przetwarzanie takich danych również w innych celach, o ile tylko podmioty będą podlegały obowiązkowi zachowania tajemnicy. Z tłumaczenia tego nie wynika również i to, że obowiązek zachowania tajemnicy ciążyący na podmiocie nie będącym podmiotem służby zdrowia powinien być równorzędny obowiązkowi zachowania tajemnicy zawodowej.

zachowania tych danych w tajemnicy, równorzędny obowiązkowi zachowania tajemnicy zawodowej. Należy podkreślić, że art. 8 ust. Dyrektywy 95/46 nie wyklucza możliwości przetwarzania osobowych danych medycznych przez podmioty nie będące podmiotami służby zdrowia, ale tylko wtedy, gdy dokonuje tego w wymienionych wyżej celach.

Przedstawione wyżej unormowanie Dyrektywy 95/46 zostało wdrożone do prawa polskiego w art. 27 ust. 2 ustawy o ochronie danych osobowych. Przepis ten, w punkcie 7, uchyla zakaz przetwarzania danych wrażliwych, w tym nie tylko osobowych danych medycznych, gdy „jest (ono) prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych”. Tym samym polski ustawodawca przyzwala na przetwarzanie m.in. osobowych danych medycznych w dwóch przypadkach:

- 1) w celu *sensu stricto* medycznym, o ile przetwarzanie to jest dokonywane przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, pod warunkiem, że „są stworzone pełne gwarancje ochrony danych osobowych”,
- 2) w celu zarządzania udzieleniem usług medycznych, pod warunkiem, że „są stworzone pełne gwarancje ochrony danych osobowych”.

Przedstawione rozwiązanie znacząco różni się od unormowania przyjętego w art. 8 ust. 3 Dyrektywy 95/46. Ustawodawca polski w pierwszym przypadku ograniczył możliwość przetwarzania danych osobowych w celu medycznym do z góry określonego kręgu – kręgu „osób trudniących się zawodowo leczeniem lub świadczeniem innych usług medycznych”. Wszystkie trzy przesłanki – przedmiotowe przetwarzania w celu medycznym i „pełnych gwarancji ochrony” oraz podmiotowa – przetwarzania przez osoby profesjonalnie zajmujące się świadczeniem usług medycznych muszą być spełnione łącznie. Takiego ograniczenia podmiotowego nie formułuje prawodawca wspólnotowy w art. 8 ust. 3 Dyrektywy 95/46. Dopuszcza on bowiem przetwarzanie danych w celu medycznym przez każdego, na kim spoczywa co najmniej obowiązek zachowania osobowych danych medycznych w tajemnicy, równorzędny obowiązkowi zachowania tajemnicy zawodowej. Oczywiście z punktu widzenia oceny dopuszczalności powierzenia przetwarzania danych medycznych to ograniczenie podmiotowe nie ma znaczenia pierwszorzędnego, gdyż przetwarzanie danych w celu *sensu stricto* medycznym ze swej natury nie jest powierzane (zabiegi lecznicze i pielęgnacyjne oraz ich dokumentowanie powinno być dokonywane osobiście przez osoby trudniące się świadczeniem usług medycznych zawodowo).

Drugi przypadek uchylenia zakazu przetwarzania osobowych danych medycznych wymaga spełnienia łącznie tylko dwóch przesłanek przedmiotowych – przetwarzania w celu „zarządzania

udzielaniem usług medycznych” oraz stworzenia „pełnych gwarancji ochrony” danych. Obie przesłanki wymagają szczegółowej analizy. W języku polskim termin ten oznacza „wykonywanie czynności administracyjnych, sprawowanie nad czymś zarządu, kierowanie czymś”⁹. Zakres znaczeniowy wskazanego terminu jest dość szeroki, jednak należy zauważyć, że w wyjaśnieniach słownikowych zarządzanie jest kojarzone przede wszystkim z kierowaniem i podejmowaniem decyzji. W świetle tego unormowania nie ulega wątpliwości, że osoby pełniące funkcje kierownicze w zakładzie opieki zdrowotnej mogą przetwarzać dane pacjentów ze względu na tę okoliczność. Dużo mniej uzasadnione jest wskazywanie tej samej podstawy faktycznej, gdy chodzi o uchylenie zakazu przetwarzania danych wrażliwych pracownikom rejestracji, statystyki medycznej, archiwum szpitala, czy też zatrudnionym w takiej jednostce informatykom. Ci ludzie *sensu stricto* nie kierują jednostką, ani nawet jej częścią. W praktyce nikt nie podważa jednak prawa tych osób do przetwarzania danych pacjentów. Uznaje się, że na takich stanowiskach wykonywane są czynności administracyjne.¹⁰ Pogląd taki, w świetle definicji słownikowych „zarządzania” zdaje się być podyktowany bardziej względami praktyki, niż dogłębną analizą art. 27 ust. 2 pkt 7 ustawy o ochronie danych osobowych. Trzeba bowiem zauważyć, że przepis ten jest unormowaniem szczególnym, a wobec tego stosowanie wykładni rozszerzającej nie jest uprawnione. Okoliczność ta poddaje w wątpliwość możliwość przetwarzania osobowych danych medycznych przez podmiot, któremu takie dane zostałyby powierzone. Podmiot taki nie zarządzałby bowiem „udzielaniem usług medycznych”. Sam fakt, iż to administrator danych, a nie przetwarzający powierzone dane ma decydować o celach i środkach, wskazuje na to, że to nie po stronie przetwarzającego leży w tym przypadku zarządzanie. Dlatego też tylko szerokie rozumienie „celu zarządzania” i założenie, że cały prawie personel niemedyczny zakładu działa na rzecz realizacji tego celu, pozwala na uznanie, że osoby te mają prawo przetwarzać takie dane. Takie samo spojrzenie na interpretację przepisu miałyby uzasadniać dopuszczalność powierzenia przetwarzania osobowych danych medycznych zawartych w dokumentacji medycznej.

Druga przesłanka uchylenia zakazu z art. 27 ust. 1 ustawy o ochronie danych osobowych zasługuje także na kilka słów komentarza. Rozumienie sformułowania „zapewnienie pełnych gwarancji ochrony” określonego w art. 27 ust 2 pkt 7 „może w konkretnych przypadkach być przedmiotem sporów”¹¹. Z uwagi na to, że ustawa o ochronie danych osobowych jest aktem implementującym Dyrektywę 95/46 WE do prawa polskiego, przy interpretacji omawianego artykułu należy uwzględnić odpowiednią regulację prawa wspólnotowego. Jest nią art. 8 ust. 3

⁹ Definicje PWN wersja 6.0.

¹⁰ J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Kraków 2007, s. 534.

¹¹ Tamże s. 526. Uwaga została wprowadzona poczyniona w odniesieniu do art. 27 ust. 2 pkt 2, jednak z uwagi na wprowadzenie takiego samego warunku w tym punkcie, jak w punkcie 7 zasadne jest przywołanie tego poglądu.

Dyrektywy 95/46 WE. Przepis ten, jak już wspomniano, wprowadza zupełnie inne rozwiązanie służące zagwarantowaniu należytej ochrony osobowych danych medycznych. Jako drugą przesłankę uchylenia zakazu ich przetwarzania statuuje podleganie podmiotu, który takie dane przetwarza, obowiązkowi zachowania tajemnicy zawodowej albo podleganie innemu równorzędnemu obowiązkowi zachowania tajemnicy. Zawarte w art. 8 ust. 3 Dyrektywy 95/46 WE określenie warunku uchylenia zakazu przetwarzania osobowych danych medycznych jest dużo bardziej precyzyjne, niż uregulowanie przyjęte w prawie polskim. Oczywiście przy implementacji dyrektyw państwa członkowskie nie muszą dokonywać transpozycji dosłownej przepisów wspólnotowych.¹² Jednak wdrożenie powinno być kompletne i powinno precyzyjnie oddawać, chociaż z uwzględnieniem specyfiki krajowego porządku prawnego, istotę dyrektywy. Niestety przyjęte w art. 27 ust 2 pkt 7 uregulowanie zdaje się tego wymogu nie spełniać. W konsekwencji, niektórzy przedstawiciele doktryny, aby wyjaśnić, na czym polega warunek „stworzenia pełnych gwarancji ochrony” danych, odwołują się do art. 8 ust. 3 Dyrektywy 95/46 WE i wskazują, że osobowe dane medyczne powinny być przetwarzane „wyłącznie przez osoby zobowiązane do zachowania tajemnicy”.¹³ Wyrażają przy tym trafny pogląd, iż samo powoływanie się przez osoby przetwarzające takie dane na generalny obowiązek zachowania tajemnicy danych osobowych przez osoby upoważnione do ich przetwarzania, wynikający z art. 39 ust. 2 ustawy o ochronie danych osobowych nie wystarczy.¹⁴ Ustawodawca polski nie określił w art. 27 ust. 2 pkt 7 ustawy o ochronie danych osobowych precyzyjnego kryterium oceny poziomu gwarancji ochrony osobowych danych medycznych. Jeśli jednak przyjąć, że tym kryterium jest podleganie osób przetwarzających takie dane obowiązkowi zachowania tajemnicy zawodowej, to poza przedstawicielami zawodów medycznych, trudno znaleźć grupę zawodową, która podlegałaby równorzędnemu obowiązkowi wynikającemu z przepisów powszechnie obowiązujących. Osoby rejestrujące pacjentów, pracownicy archiwum szpitala, informatycy szpitalni, a także osoby pełniące funkcje kierownicze (o ile nie są także przedstawicielami zawodów medycznych) nie podlegają takim obowiązkom wynikającym z ustaw, czy rozporządzeń. Oczywiście można stać na stanowisku, że obowiązek zachowania tajemnicy nie musi wynikać z przepisów prawa powszechnie obowiązującego. Przyjmując jednak, że taki obowiązek mógłby mieć źródło w umowie,¹⁵ należy zastanowić się, czy wtedy stworzone byłyby pełne gwarancje ochrony. O ile w przypadku przetwarzania danych przez personel niemedyczny zakładów opieki zdrowotnej można pokusić się o stwierdzenie, że po wprowadzeniu do umów zawieranych stanowiących

¹²Dopuszcza się ten sposób implementacji, ale spotyka się to z krytyką. Por. B. Kurcz, *Dyrektywy Wspólnoty Europejskiej i ich implementacja do prawa krajowego*, Kraków 2004, s. 177 i s. 182-185.

¹³Por. A. Drozd, *Ustawa o ochronie danych osobowych. Komentarz*, W-wa 2004, s. 174.

¹⁴Tamże.

¹⁵Szerzej na ten temat: M. Rusinek, *Tajemnica zawodowa i jej ochrona w polskim procesie karnym*, Kraków 2007, s. 51-52.

podstawy zatrudnienia tych osób szczególnego obowiązku zachowania tajemnicy, byłoby to możliwe, o tyle w przypadku powierzenia przetwarzania osobowych danych medycznych pojawiają się poważne wątpliwości¹⁶. Głównym problemem jest w tym przypadku to, że ustawodawca polski nie zapewnił Generalnemu Inspektorowi Ochrony Danych Osobowych otrzymywania aktualnej informacji na temat podmiotów, którym administratorzy powierzyli przetwarzanie osobowych danych medycznych.¹⁷ Trzeba w tym miejscu przypomnieć, że same zakłady opieki zdrowotnej, zgodnie z art. 43 ust. 1 pkt 5 ustawy o ochronie danych osobowych, zwolnione są z obowiązku rejestracji zbiorów danych osób korzystających z ich usług medycznych, a podmiot, któremu mianoby powierzyć takie dane nie ma obowiązku dokonania takiej rejestracji. Zgodnie z art. 40 ustawy o ochronie danych osobowych, obowiązek taki spoczywa tylko na administratorze. Generalny Inspektor Ochrony Danych Osobowych może oczywiście kontrolować podmioty, którym powierzono przetwarzanie osobowych danych medycznych, ale aby przeprowadzić kontrolę musi najpierw dysponować wiedzą o tym, że określony podmiot takie dane przetwarza. Wobec braku obowiązku informowania Generalnego Inspektora Ochrony Danych Osobowych o takich podmiotach, organ ten nie mógłby efektywnie sprawować nad nimi kontroli. Nie miałby w związku z tym w praktyce możliwości sprawdzania, czy stwarzałyby one „pełne gwarancje ochrony” danych. W świetle tych uwag, należy uznać, że powierzenie przetwarzania osobowych danych medycznych na gruncie polskiej ustawy o ochronie danych osobowych może rodzić wiele trudności.

Oczywiście nie oznacza to, że możliwość taka absolutnie nie istnieje. Powierzenia przetwarzania osobowych danych medycznych jest możliwe za zgodą pacjentów na podstawie art. 27 ust. 2 pkt 1 ustawy o ochronie danych osobowych. Teoretycznie zakład opieki zdrowotnej mógłby odbierać od każdego nowego pacjenta oświadczenie o wyrażeniu zgody na powierzenie przetwarzania jego osobowych danych medycznych innemu podmiotowi np. przedsiębiorcy świadczącemu usługi w zakresie archiwizacji danych. Problemy pojawiłyby się wtedy, gdy chociażby jeden z pacjentów odmówiłby wyrażenia takiej zgody. W konsekwencji utrudniłoby to funkcjonowanie całego systemu prowadzenia dokumentacji medycznej, opartego o powierzenie przetwarzania danych innemu podmiotowi. Nie sposób też nie zauważyć, że w praktyce możliwość występowania o zgodę pacjenta na powierzenie przetwarzania danych ma wartość czysto teoretyczną, gdyż nie rozwiązuje także problemu przechowania informacji o osobach leczonych w przeszłości, których dane znajdują się już archiwum zakładu.

¹⁶Por. A. Mednis, *Ustawa o ochronie danych osobowych. Komentarz*, W-wa 1999, s. 90.

¹⁷ GIODO może oczywiście kontrolować podmioty, którym powierzono przetwarzanie osobowych danych medycznych, ale aby przeprowadzić kontrolę musi najpierw dysponować wiedzą o tym, że określony podmiot takie dane przetwarza.

Powyżej przeanalizowana została kwestia samej dopuszczalności przetwarzania osobowych danych medycznych przez podmiot, któremu takie dane miałyby zostać powierzone. Dla oceny dopuszczalności powierzenia przetwarzania danych istotne jest jednak nie tylko to, czy taki podmiot mógłby dane przetwarzać, ale także to, czy takiemu podmiotowi wolno takie dane wyjawiać. W odniesieniu do osobowych danych medycznych odpowiedzi na to pytanie należy szukać w art. 18 ust. 3 ustawy o zakładach opieki zdrowotnej. Przepis ten zawiera zamknięty katalog podmiotów, którym wolno udostępnić¹⁸ dokumentację, a co za tym idzie i zawarte w niej osobowe dane medyczne. Mogą je otrzymać:

- pacjenci lub ich przedstawiciele ustawowi bądź osoby upoważnione przez pacjenta,
- zakłady opieki zdrowotnej, jednostki organizacyjne tych zakładów i osoby wykonujące zawód medyczny poza zakładami opieki zdrowotnej, jeżeli dokumentacja ta jest niezbędna do zapewnienia ciągłości świadczeń zdrowotnych,
- właściwe do spraw zdrowia organy państwowe oraz organy samorządu lekarskiego w zakresie niezbędnym do wykonywania kontroli i nadzoru,
- minister właściwy do spraw zdrowia, sądy i prokuratorzy oraz sądy i rzecznicy odpowiedzialności zawodowej, w związku z prowadzonym postępowaniem,
- uprawnione na mocy odrębnych ustaw organy i instytucje, jeżeli badanie zostało przeprowadzone na ich wniosek.
- organy rentowe oraz zespoły do spraw orzekania o stopniu niepełnosprawności, w związku z prowadzonym przez nie postępowaniem,
- rejestry usług medycznych, w zakresie niezbędnym do prowadzenia rejestrów,
- zakłady ubezpieczeń na zasadach określonych w przepisach o działalności ubezpieczeniowej.

Wśród podmiotów, którym wolno ujawnić dokumentację nie wymieniono przedsiębiorców profesjonalnie zajmujących się przetwarzaniem danych osobowych na podstawie umów outsourcingowych. Przepis generalnie nie uwzględnia możliwości udostępnienia dokumentacji medycznej, bez zgody pacjenta, przedsiębiorcom innym niż przedstawiciele zawodów medycznych świadczący usługi medyczne, zakłady opieki zdrowotnej oraz zakłady ubezpieczeniowe. W konsekwencji omawiany artykuł ustawy o zakładach opieki zdrowotnej uniemożliwiając, bez upoważnienia pacjenta, wyjawienie osobowych danych medycznych, pośrednio istotnie ogranicza powierzenie przetwarzania takich danych.

¹⁸ Udostępnienia dokumentacji medycznej nie należy utożsamiać z pojęciem udostępnienia danych osobowych, o którym mowa w ustawie o ochronie danych osobowych.

Barierą dla powierzania przetwarzania osobowych danych medycznych jest także unormowanie zawarte w rozporządzeniu Ministra Zdrowia z dnia 21 grudnia 2006 r. w sprawie rodzajów i zakresu dokumentacji medycznej w zakładach opieki zdrowotnej oraz sposobu jej przetwarzania. Paragraf 44 pkt 1 tego rozporządzenia stanowi bowiem, że „Dokumentacja wewnętrzna jest przechowywana w zakładzie, w którym została sporządzona”. Obowiązek ten w wielu przypadkach niweczyłby sens powierzenia przetwarzania danych o pacjentach. Często powierzenie jest dokonywane w celu przechowywania prowadzonej danych na serwerze zlokalizowanym poza siedzibą administratora danych. Rozwiązanie takie stosowane jest z różnych względów. Czasem służy tylko obniżeniu kosztów przechowywania danych poprzez skorzystanie z zewnętrznego serwera. Niekiedy chodzi wyłącznie o zabezpieczenie kopii danych poprzez przechowywanie ich poza siedzibą administratora u wyspecjalizowanego w archiwizowaniu danych podmiotu zewnętrznego. Wreszcie mogłoby być i tak, że za przechowywaniem danych poza zakładem opieki zdrowotnej miałyby przemawiać względy organizacyjne. Już dzisiaj na polskim rynku istnieją spółki handlowe zarządzające kilkoma zakładami opieki zdrowotnej. Niektóre z takich spółek chciałyby stworzyć dla wszystkich zakładów jedno centrum administracyjno - informatyczne, które m.in. zajmowałoby się zabezpieczaniem i przechowywaniem prowadzonej w postaci elektronicznej dokumentacji medycznej poza tymi zakładami. Wszystkie te koncepcje opierają się jednak na założeniu, że taką dokumentację byłoby można przechowywać poza zakładem opieki zdrowotnej. W tym kontekście treść §44 pkt 1 rozporządzenia utrudnia powierzenie przetwarzania „osobowych danych medycznych”. Oczywiście sformułowanie - „Dokumentacja wewnętrzna jest przechowywana w zakładzie, w którym została sporządzona” - można interpretować różnie. Jednym ze sposobów rozumienia tego przepisu może być uznanie, że dokumentacja powinna być przechowywana wyłącznie w zakładzie opieki zdrowotnej i że istnieje zakaz przechowywania dokumentacji poza zakładem. Inny pogląd może opierać się natomiast na założeniu, że celem unormowania jest tylko zapewnienie, aby dokumentacja była zawsze dostępna w miejscu, w którym została wytworzona. Nie jest natomiast istotne, czy jej kopia znajduje się również gdzie indziej, czy też nie. W tym przypadku obowiązek przechowywania dokumentacji medycznej spoczywałby na zakładzie, ale mógłby on zachowując u siebie dokumentację prowadzoną w postaci elektronicznej powierzyć przechowywanie tych samych danych podmiotowi zewnętrznemu. W tym przypadku bowiem, co wynika z natury dokumentu elektronicznego,¹⁹ oryginał znajdowałby się nadal u podmiotu, który go wytworzył. W świetle takiej interpretacji możliwe byłoby zabezpieczenie kopii dokumentacji medycznej poprzez jej przechowanie na serwerze podmiotu zewnętrznego. Nadal jednak za niedopuszczalne należałoby

¹⁹ Dokumentem elektronicznym są dane, a nie informatyczny nośnik tych danych.

uznać przechowywanie dokumentacji medycznej wyłącznie na informatycznych nośnikach danych znajdujących się poza zakładem opieki zdrowotnej, bo w tym przypadku w zakładzie takiej dokumentacji nie byłoby w ogóle. Niezależnie jednak od sposobu interpretacji § 44 wskazanego wyżej rozporządzenia przepis ten w obecnym kształcie stanowi także barierę dla stosowania rozwiązań outsourcingowych w zakresie przetwarzania osobowych danych medycznych.

Podsumowując rozważani trzeba zauważyć, że:

- 1) obowiązujące uregulowania prawa wspólnotowego nie wykluczają możliwości powierzenia przetwarzania osobowych danych medycznych podmiotom nie będącym podmiotami służby zdrowia,
- 2) prawo polskie nie zapewnia wystarczających gwarancji ochrony osobowych danych medycznych podmiotom nie będącym podmiotami służby zdrowia,
- 3) prawo polskie nie zezwala, bez upoważnienia pacjenta, na udostępnienie dokumentacji medycznej przedsiębiorcom profesjonalnie zajmującym się przetwarzaniem danych osobowych na podstawie umów outsourcingowych,
- 4) prawo polskie nie zezwala na nie przechowywanie dokumentacji medycznej w zakładzie opieki zdrowotnej, w którym została ona sporządzona,
- 5) możliwe jest, za zgodą pacjenta, powierzenie przetwarzania osobowych danych medycznych zawartych w jego dokumentacji medycznej innemu podmiotowi, o ile pacjent upoważni zakład opieki zdrowotnej do udostępnienia dokumentacji takiemu podmiotowi, a oryginał dokumentacji nadal będzie przechowywany w zakładzie opieki zdrowotnej, w którym został sporządzony.

Wobec powyższego należy stwierdzić, iż w obecnym stanie prawnym zastosowanie rozwiązań outsourcingowych w zakresie prowadzenia dokumentacji medycznej w postaci elektronicznej jest bardzo utrudnione. Barierami są w tym przypadku brak możliwości powierzenia przetwarzania osobowych danych medycznych podmiotom zewnętrznym bez uzyskania stosownych oświadczeń od pacjenta oraz obowiązek przechowywania dokumentacji medycznej w zakładzie opieki zdrowotnej, w którym została ona sporządzona. Poprawa tego stanu wymagałaby co najmniej dokonania zmian w art. 27 ust. 2 ustawy o ochronie danych osobowych, art. 18 ust. 3 ustawy o zakładach opieki zdrowotnej oraz § 44 rozporządzenia Ministra Zdrowia z dnia 21 grudnia 2006 r. w sprawie rodzajów i zakresu dokumentacji medycznej w zakładach opieki zdrowotnej oraz sposobu jej przetwarzania. To proste wyliczenie przepisów, które należałoby ewentualnie znowelizować nie powinno jednak prowadzić do mylnego wniosku, że umożliwienie stosowania rozwiązań outsourcingowych w zakresie powierzenia przetwarzania

osobowych danych medycznych jest sprawą prostą. Trzeba bowiem pamiętać, że w tym przypadku dotyka się kwestii ujawnienia szczególnie wrażliwych danych stanowiących jednocześnie informacje chronione tajemnicami zawodowymi oraz w niektórych przypadkach również tajemnicą psychiatryczną²⁰. Dopuszczenie powierzenia przetwarzania danych w tym przypadku wymaga przemyślanych i wyważonych rozwiązań uwzględniających interesy pacjentów, ale i zakładów opieki zdrowotnej. Odpowiednie regulacje powinny powstać, gdyż w przeciwnym razie niezgodne z prawem powierzenie przetwarzania osobowych danych medycznych prawdopodobnie i tak będzie miało miejsce. Zakład opieki zdrowotnej może być bowiem zmuszony do skorzystania z pomocy podmiotu zewnętrznego przy usuwaniu awarii systemu teleinformatycznego. Państwo powinno więc zapewnić efektywną kontrolę nad podmiotami, którym powierzałoby osobowe dane medyczne. Bez przeprowadzenia jednak odpowiednich zmian w obowiązujących unormowaniach perspektywy zgodnego z prawem powierzenia przetwarzania takich danych oraz prowadzenia dokumentacji medycznej w postaci elektronicznej są bardzo niepomysłne

²⁰ Por. Rozdział 6 ustawy z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego (Dz.U. 1994 poz. 111 poz. 535 z późn. zm.).