CBKE
e-BIULETYN

Prowadzenie dokumentacji medycznej w formie elektronicznej na podstawie rozporządzenia Ministra Zdrowia z dnia 21 grudnia 2006 r.[1] w kontekście prawa pacjenta do ochrony danych medycznych

dr Arkadiusz Bieliński
dr Urszula Drozdowska

Niesamodzielni pracownicy Katedry Prawa Cywilnego

Wydziału Prawa Uniwersytetu w Białymstoku

ul. Mickiewicza 1. 15-213 Białystok

Wprowadzenie

Analiza zasad prowadzenia dokumentacji medycznej w formie elektronicznej w kontekście poszanowania prawa pacjenta do poufności medycznej wydaje się szczególnie doniosłą i aktualną w dobie społeczeństwa opanowanego przez nowoczesne globalne technologie. Doniosłą, gdyż zbieranie, przetwarzanie oraz udostępnianie informacji na temat stanu zdrowia pacjenta oznacza poważną ingerencję w sferę jego prywatności, aktualną zaś dlatego, iż przepisy wymienionego w tytule rozporządzenia - w zakresie prowadzenia dokumentacji medycznej w formie elektronicznej - wchodzą w życie z dniem 28 czerwca 2007 r.

Niewątpliwie występuje tu problem prawidłowego wyważenia konkurujących ze sobą interesów, z jednej strony powstaje konieczność zapewnienia pacjentowi ochrony jego danych medycznych, z drugiej zaś potrzeba wprowadzenia w zakładach opieki zdrowotnej nowoczesnych systemów operowania tymi danymi. Należy podkreślić, iż potrzeba ta wywołana jest nie tylko

[1] Rozporządzenie w sprawie rodzajów i zakresu dokumentacji medycznej w zakładach opieki zdrowotnej oraz sposobu jej przetwarzania (Dz. U. Nr 247 poz. 1819). Rozporządzenie to było poprzedzone rozporządzeniem Ministra Zdrowia z dnia 10 sierpnia 2001 r. (Dz. U. Nr 88, poz. 966 ze zm.), które utraciło moc w związku z wyrokiem Trybunału Konstytucyjnego z dnia 28 listopada 2005 r. (K 22/05), Dz. U. Nr 239, poz. 2020.

oczywistymi ułatwieniami natury organizacyjnej, usprawniającymi funkcjonowanie opieki zdrowotnej, lecz także związana jest z koniecznością transmisji danych medycznych do innych podmiotów prawa. Zakłady opieki zdrowotnej są zobowiązane m. in. do przekazywania informacji oddziałom Narodowego Funduszu Zdrowia[2], rejestrom usług medycznych[3], organom kontrolującym ich działalność, organom statystycznym czy Państwowej Inspekcji Sanitarnej[4]. Niewątpliwie zatem bezpieczna transmisja danych już wkrótce stanie się zadaniem priorytetowym dla sprawnie działającego zakładu opieki zdrowotnej.

I. Treść prawa pacjenta do ochrony danych zawartych w dokumentacji medycznej

Na wstępie rozważań należy zwrócić uwagę na fakt, iż napięcie pomiędzy obowiązkiem zapewnienia bezpieczeństwa danym medycznym a koniecznością odpowiedniego ich przetwarzania jest szczególnie wyraziste. W stanie faktycznym będącym kanwą orzeczenia Sądu Okręgowego w Katowicach z dnia 12 grudnia 2003 r.[5], przyczyną dokonania zbędnego zabiegu operacyjnego, okaleczającego pacjenta był błąd sekretarki medycznej, która wprowadzając dane do komputera połączyła dwie różne diagnozy pacjentów.

Dane medyczne są przekazywane i przetwarzane przez coraz liczniejszy i bardziej wyspecjalizowany personel. Paradoksalnie największe zagrożenia dla sfery poufności pacjenta występują w państwach wysoko rozwiniętych i wiążą się nie tylko z postępem technicznym, lecz także z upowszechnianiem się systemów ubezpieczeń zdrowotnych oraz zabezpieczeń socjalnych[6]. Szeroki dostęp wielu podmiotów do danych medycznych oraz techniczne możliwości wykorzystania tego dostępu spowodował na tyle silne zagrożenie dla sfery dóbr osobistych pacjenta, że poświęcono temu zagadnieniu oddzielne regulacje prawne w prawie europejskim.

Na uwagę zasługuje zwłaszcza jako standard o charakterze traktatowym Konwencja nr 108 z dnia 28 stycznia 1981 r.[7] o ochronie osób w kontekście automatycznego przetwarzania danych osobowych w systemach informatycznych. Celem Konwencji jest zabezpieczenie poszanowania sfery osobistej w związku z zagrożeniami, jakie niesie automatyczne przetwarzanie danych

[2] Zob. rozporządzenie Ministra Zdrowia z dnia 27 czerwca 2006 r. w sprawie niezbędnych informacji gromadzonych przez świadczeniodawców, szczegółowego sposobu rejestrowania tych informacji oraz ich przekazywania podmiotom zobowiązanym do finansowania świadczeń ze środków publicznych (Dz. U. Nr 114, poz. 780).
[3] Zob. art. 18 ust. 3 pkt 7 ustawy z dnia 30 sierpnia 1991 r. o zakładach opieki zdrowotnej (tj. Dz. U. z 2007 r., Nr 14, poz. 89 ze zm.) dalej zwana jako ustawa o zoz.
[4] Ustawa z dnia 14 marca 1985 r. o Państwowej Inspekcji Sanitarnej (tj. Dz. U. z 2006 r., Nr 122 poz. 851 ze zm.)
[5] Sygn. akt II C 911/01/5, Prawo i Medycyna 2005, nr 2 z glosą M. Nesterowicza.
[6] Zob. szerzej M. Safjan, Prawo do prywatności i ochrona danych osobowych w społeczeństwie informatycznym, Państwo i Prawo 2002, z. 6, s. 5 i nast.
[7] Dz. U. 2003, Nr 3, poz. 25. Konwencja została przez Polskę ratyfikowana dnia 24 kwietnia 2002 r., weszła w życie dnia 1 września 2002 r.

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

osobowych. Konwencja ma zastosowanie jedynie w sferze publicznoprawnej, dotyczy bowiem obowiązków państw - stron Konwencji w zakresie zapewnienia odpowiedniego poziomu ochrony danych osobowych. W stosunku do danych medycznych wymaga, aby dane te nie podlegały automatycznemu przetwarzaniu, chyba, że prawo krajowe zagwarantuje ich właściwe zabezpieczenie[8].

Szczegółowe uregulowanie problematyki ochrony danych osobowych w medycynie znajduje się w rekomendacji wydanej dnia 13 lutego 1997 r. przez Komitet Ministrów Rady Europy (rekomendacja nr 5). Rekomendacja ta próbuje pogodzić z jednej strony potrzebę zapewnienia jakości i dostępności informacji medycznych dla upoważnionych specjalistów, z drugiej zaś z potrzebę ochrony poufności danych[9], wskazuje szczegółowo na zasady przetwarzania danych medycznych i przesyłania danych za granicę, określając konieczne do zachowania środki bezpieczeństwa. Rekomendacja ta ma zastosowanie do zbierania i przetwarzania danych medycznych, o ile ustawodawstwo wewnętrzne państw członkowskich nie przewiduje właściwych gwarancji[10].

W prawie polskim *expressis verbis* ochronę danych zawartych w dokumentacji medycznej przewiduje art. 18 ust. 2 ustawy o zoz. Przez dokumentację medyczną należy rozumieć określone w ustawie o zoz oraz przepisach odrębnych dane i informacje medyczne odnoszące się do stanu zdrowia pacjenta lub udzielonych mu w zakładzie świadczeń zdrowotnych[11].

Zgodnie z art. 18 ust. 2a ustawy o zoz, dokumentacja medyczna zawiera co najmniej: oznaczenie pacjenta, pozwalające ustalić jego tożsamość, oznaczenie zakładu opieki zdrowotnej ze wskazaniem odpowiedniej komórki organizacyjnej, która udzieliła świadczeń, opis stanu zdrowia pacjenta, opis udzielonych świadczeń zdrowotnych, datę sporządzenia. Dokumentacja medyczna powinna także zawierać informacje istotne z punktu widzenia prawidłowości wykonywania zawodu przez lekarza i podległy mu personel medyczny, w tym zwłaszcza informacje dotyczące wyrażenia zgody przez pacjenta (art. 34 ust. 1 ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty[12]) oraz zakresu udzielonej mu informacji (art. 31 ust. 1 ustawy). Ustawa ta przewiduje obowiązek odnotowania w dokumentacji medycznej konieczności podjęcia czynności medycznych bez zgody pacjenta lub jego przedstawiciela ustawowego w sytuacji zagrożenia życia (art. 33 ust. 3, art. 34 ust. 8), informacji odnoszących się do zmiany zakresu zabiegu, metody leczenia lub diagnostyki (tzw. sytuacja rozszerzonego pola operacyjnego –

[8] Szerzej A. Mednis, Ochrona danych osobowych w Konwencji Rady Europy i dyrektywy UE, Państwo i Prawo 1997, nr 6, s. 29 i nast.
[9] Za M. Jackowskim, Ochrona danych medycznych, Dom Wydawniczy ABC 2002, s. 71.
[10] Szerzej J. Barta, R. Markiewicz, Ochrona danych osobowych. Komentarz, Kraków 2004, s. 83.
[11] Zob. art. 18d ust. 1 pkt 5 ustawy o zoz.
[12] Dz. U. z 2005 r. Nr 226, poz. 1943 ze zm., dalej zwana ustawą o zawodzie lekarza.

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

art. 35 ust. 2 ustawy), a także odnotowania i uzasadnienia odstąpienia od leczenia (art. 38 ust. 4 ustawy) oraz powstrzymania się od wykonywania świadczenia zdrowotnego niezgodnego z sumieniem lekarza (art. 39 ustawy). Szeroki zakres informacji zawartych w dokumentacji medycznej wskazuje, iż mają one służyć nie tylko dobru pacjenta poprzez zapewnienie mu ciągłości udzielania świadczeń zdrowotnych, lecz także zakładowi opieki zdrowotnej, który będąc właścicielem dokumentacji może kontrolować (i być kontrolowanym) - w zakresie prawidłowości udzielenia świadczeń zdrowotnych.

W ustawodawstwie polskim prawo do ochrony danych medycznych można wywieść nie tylko z przepisów ustawy o zoz, lecz także ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[13]. Na gruncie ustawy przez dane medyczne rozumie się dane pozwalające na ustalenie stanu zdrowia zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej oraz informacje, z których tego rodzaju wiadomości przeciętny odbiorca może wyprowadzić z dużą dozą prawdopodobieństwa[14]. Pojęcie to odnosić należy nie tylko do informacji, które pozwalają na ustalenie szeroko pojętego stanu zdrowia zarówno teraźniejszego, przeszłego jak i przyszłego jednostki, ale także do informacji o stylu życia, nałogach, czy nawet życiu seksualnym, pod warunkiem, że są to informacje nieupublicznione. Do danych medycznych zalicza się także dane genetyczne[15].

Przetwarzanie danych osobowych jest możliwe jedynie, wtedy, gdy spełnione są ogólne zasady jakości przetwarzania danych tj. zasada legalności, oznaczająca przetwarzanie danych jedynie zgodnie z obowiązującym prawem; zasada celowości, wskazująca na możność zbierania danych wyłącznie dla celów oznaczonych i zgodnie z prawem; zasada poprawności i adekwatności, polegająca na zapewnieniu merytorycznej poprawności danych i adekwatności dla celów, dla których zostały zebrane oraz zasada ograniczenia czasowego przechowywania danych, co oznacza przechowywanie danych w postaci umożliwiającej identyfikację, nie dłużej niż to jest niezbędne dla celu przetworzenia. W związku z tą ostatnią zasadą należy wskazać, iż okres przechowywania dokumentacji medycznej przez zakłady opieki zdrowotnej jest stosunkowo długi, wynosi on z reguły dwadzieścia lat, licząc od końca roku kalendarzowego, w którym sporządzono ostatni wpis o udzielonych świadczeniach zdrowotnych (art. 18 ust. 4f ustawy o zoz). Terminy przechowywania dokumentacji zostały przedłużone do lat trzydziestu w sytuacji zgonu pacjenta na skutek uszkodzenia ciała lub zatrucia. Termin ten liczony jest od końca roku kalendarzowego,

[13] Dz. U. z 2002 r., Nr 101, poz. 926 ze zm Ustawa ma charakter subsydiarny (art. 5 ustawy), co oznacza, iż przyjmuje się możliwość zastosowania przepisów innych ustaw, które w sposób dalej idący przewidują ochronę. Ustawa ta w dalszej części tekstu zwana jest ustawą o ochronie danych osobowych.

[14] Por. art. 6 ustawy o ochronie danych osobowych w brzmieniu ustalonym przez ustawę z dnia 25 sierpnia 2001 r. o zmianie ustawy o ochronie danych osobowych (Dz. U. Nr 100, poz. 1087.).

[15] Przepis art. 27 ustawy odrębnie wyróżnia dane o stanie zdrowia, dane o kodzie genetycznym, życiu seksualnym i nałogach. Wyodrębnienie tych danych ma na celu podkreślenie ich sensytywności i pewnej odrębności.

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

w którym nastąpił zgon. Krótsze terminy przewidziano dla zdjęć rentgenowskich (lat 10) i oraz skierowań na badania oraz zleceń lekarskich (lat 5).

Ochrona danych medycznych na podstawie komentowanej ustawy przejawia się przede wszystkim w zaliczeniu danych medycznych do kategorii danych sensytywnych i poddaniu ich - w porównaniu z innymi danymi osobowymi - bardziej rygorystycznej regulacji w zakresie ich przetwarzania[16].

Zakaz przetwarzania danych sensytywnych doznaje wyłączenia jedynie w sytuacjach określonych w art. 27 ust. 2 ustawy. Na mocy tego przepisu przetwarzanie danych jest możliwe m. in. w sytuacji, gdy osoba, której dane dotyczą wyrazi zgodę, a także wtedy, jeśli przepis szczególny innej ustawy zezwala na to przetwarzanie bez takiej zgody (w przypadku danych medycznych będzie to przede wszystkim art. 18 ust. 3 ustawy o zoz) i stwarza pełne gwarancje ich ochrony. Ponadto istnieje możliwość uchylenia zakazu przetwarzania danych ze względu na ochronę żywotnych interesów osoby, której dane dotyczą lub nawet innej osoby, gdy osoba, której dane dotyczą nie jest fizycznie lub prawnie zdolna do wyrażenia zgody - do czasu ustanowienia opiekuna prawnego lub kuratora. Spośród innych wymienionych w komentowanym przepisie wyjątków na uwagę zasługuje punkt siódmy, który bezpośrednio wskazuje na legalność przetwarzania danych w celu ochrony zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub zarządzaniem udzielaniem usług medycznych. Na podkreślenie zasługuje fakt, iż ustawodawca ponownie nakazuje stworzenie pełnej gwarancji ochrony danych osobowych. Powstaje zatem pytanie o rodzaj i zakres tych gwarancji.

Niewątpliwie zabezpieczeniami o charakterze prawnym są: tajemnica zawodowa i służbowa osób[17] mających dostęp do danych medycznych. Osoby te są zobowiązane – w myśl rozwiązań zawartych w ustawie - do zachowania w tajemnicy informacji, z którymi się zapoznały nawet po ustaniu zatrudnienia (art. 39 ust. 1 ustawy o ochronie danych osobowych).

Tajemnica zawodowa personelu medycznego, a zwłaszcza tajemnica lekarska jest uregulowana przez ustawodawcę bardzo rygorystycznie. Tajemnicą objęte są wszelkie informacje, jakie zostały pozyskane w związku z wykonywaniem czynności zawodowych (art. 40 ustawy o zawodzie lekarza). Lekarz jest związany tajemnicą również po śmierci pacjenta. Należy zwrócić uwagę na fakt, iż zakres wiadomości, objętych tajemnicą zawodową jest zdecydowanie szerszy w porównaniu do zakresu informacji objętych dokumentacją medyczną. Lekarz jest zobowiązany do zachowania w tajemnicy wszystkiego, co uzyskał w związku z udzielaniem

[16] Pojęcie przetwarzania danych osobowych obejmuje zarówno: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, jak i usuwanie danych (art. 7 pkt 2 ustawy o ochronie danych osobowych).
[17] Tajemnica ta czasem zbiorczo jest nazywana tajemnicą informatyczną, choć odnosi się ona również do danych przetwarzanych poza systemami elektronicznymi.

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

świadczenia zdrowotnego, a zatem także informacji, niezwiązanych ze zdrowiem pacjentem. Prawem do ochrony danych medycznych objęte są zaś tylko te dane, które zostały utrwalone na nośniku papierowym lub elektronicznym, określanym jako dokumentacja medyczna. Ten węższy zakres informacji objętych prawem do ochrony danych medycznych w dużej mierze tłumaczy szerszy krąg podmiotów mających dostęp do dokumentacji medycznej na gruncie art. 18 ust. 3 ustawy o zoz[18].

Problematyka dostępu do dokumentacji medycznej przez inny podmiot, niż sam pacjent ma ścisły związek z prawem pacjenta do ochrony danych medycznych. Im więcej podmiotów ma dostęp do informacji medycznych, tym węższy jest pozytywny zakres ochrony pacjenta. W tej płaszczyźnie przepis art. 18 ust. 3 ustawy o zoz można potraktować jako ograniczenie prawa do ochrony danych medycznych[19].

Dostęp do danych zawartych w dokumentacji medycznej zgodnie z art. 18 ust. 3 mają osoby wykonujące zawód medyczny, jeżeli dokumentacja ta jest niezbędna do zapewnienia ciągłości świadczeń zdrowotnych, następnie właściwe do spraw zdrowia organy państwowe, organy samorządu lekarskiego w zakresie niezbędnym do wykonywania kontroli i nadzoru, minister zdrowia, sądy, prokuratur, sądy zawodowe i rzecznicy odpowiedzialności zawodowej - w związku z prowadzonym postępowaniem. Do grona podmiotów, które nie uczestniczą w procesie leczenia należą także: uprawnione na mocy odrębnych ustaw organy i instytucje, jeżeli badanie zostało przeprowadzone na ich wniosek, organy rentowe, zakłady ubezpieczeniowe oraz zespoły do spraw orzekania o stopniu niepełnosprawności w związku z prowadzonym przez nie postępowaniem, rejestry usług medycznych, w zakresie niezbędnym do prowadzenia rejestrów, szkoły wyższe lub jednostki badawczo-rozwojowe w celach naukowych, bez ujawniania nazwiska i innych danych umożliwiających identyfikację osoby, której dokumentacja dotyczy.

Wyżej wymienione podmioty mogą żądać dostępu jedynie we wskazanych w ustawie okolicznościach. Udostępniając dane, zakład - jako administrator danych jest, naszym zdaniem[20], zobligowany do zweryfikowania przesłanek powstania obowiązku udostępnienia oraz zakresu przekazywanych danych pod kątem ich ochrony[21]. Stosownie bowiem do treści przepisu art. 26 ust.

[18] Porównując przepisy ustawy o zoz i ustawy o ochronie danych osobowych w zakresie wyjątków od zasady poszanowania prawa do ochrony danych medycznych z uregulowaniami ustawy o zawodzie lekarza w zakresie wyjątków od zachowania tajemnicy lekarskiej można dojść do wniosku, iż sfera poufności pacjenta jest bardziej chroniona na gruncie tajemnicy lekarskiej. Zadecydował o tym zarówno aspekt przedmiotowy (zakres informacji) jak i aspekt podmiotowy (nośnik informacji).

[19] Por. T. Kolasiński, Ochrona dóbr osobistych w prawie medycznym, Prawo i Medycyna 2002, nr 11, s. 37.

[20] Odmiennie M. Dercz, T. Rek, Komentarz do ustawy o zakładach opieki zdrowotnej, Kraków 2007, s. 104.

[21] Dla przykładu, domaganie się w przeszłości przez firmy ubezpieczeniowe informacji o stanie zdrowia pacjenta od wszystkich placówek służby zdrowia i lekarzy, u których leczył się pacjent w związku z projektowanym zawarciem lub kontynuowaniem umowy ubezpieczenia było sprzeczne z zasadą ochrony danych. W chwili obecnej zasady udzielania informacji reguluje rozporządzenie Ministra Zdrowia z dnia 23 marca 2004 r. w sprawie szczegółowego zakresu i trybu udzielania zakładom ubezpieczeń informacji o stanie zdrowia ubezpieczonych lub osób, na rzecz których ma zostać zawarta umowa ubezpieczenia oraz sposobu ustalania wysokości opłat za udzielenie tych informacji (Dz. U. Nr 71, poz. 654).

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

1 ustawy o ochronie danych osobowych przetwarzając dane administrator powinien dołożyć **szczególnej staranności** dla zapewnienia ochrony interesów osób, których dane dotyczą. Zwraca uwagę fakt, iż ustawa nie operuje pojęciem należytej staranności, tak jak to czyni kodeks cywilny (art. 355 § 1 k.c.[22]), lecz pojęciem szczególnej staranności. Jest to najwyższa staranność jakiej można oczekiwać od osoby prowadzącej cudze sprawy (*diligentia exactissima*), co uzasadnia wniosek, iż naruszeniem obowiązku jest nawet drobne niedbalstwo czy opieszałość[23]. **Administrator danych jest zatem zobowiązany działać ze szczególną starannością przy udostępnianiu danych.**

Oprócz prawnych gwarancji ochrony danych medycznych na gruncie ustawodawstwa polskiego wyróżnia się gwarancje pod postacią odpowiednich zabezpieczeń technicznych i organizacyjnych. Tego zagadnienia będzie dotyczyła druga część artykułu poświęcona zabezpieczeniom dokumentacji prowadzonej w formie elektronicznej zgodnie z rozporządzeniem z dnia 21 grudnia 2006 r. w sprawie rodzajów i zakresu dokumentacji medycznej w zakładach opieki zdrowotnej oraz sposobu jej przetwarzania[24].

II. Prowadzenie dokumentacji medycznej w postaci elektronicznej

Zgodnie z § 1 ust. 2 rozporządzenia w sprawie rodzajów i zakresu dokumentacji medycznej, dokumentacja indywidualna i zbiorowa jest prowadzona w postaci pisemnej i elektronicznej w rozumieniu ustawy z dnia 17 lutego 2005r. o informatyzacji działalności podmiotów realizujących zadania publiczne[25]. Ustawodawca w § 54 określił warunki, po spełnieniu których zbiory informacji objętych dokumentacją mogą być sporządzane w postaci elektronicznej. Przede wszystkim musi być zachowany warunek selektywności dostępu do zbioru informacji, czyli zapewnienie możliwości wyboru danych do których dostęp chcemy uzyskać. Następnie należy zapewnić zabezpieczenie zbioru informacji przed dostępem osób nieuprawnionych, przed ich zniszczeniem, uszkodzeniem lub utratą oraz rejestrować historię zmian i ich autorów[26]. Dodatkowo system informatyczny służący do prowadzenia dokumentacji w postaci elektronicznej powinien umożliwiać wygenerowanie dokumentów indywidualnych i zbiorowych w postaci pisemnej[27]. Chodzi zatem o zapewnienie ochrony przetwarzanych danych, a jakiekolwiek zmiany muszą mieć swoje odzwierciedlenie w systemie informatycznym służącym do sporządzania

[22] Ustawa z dnia 23 kwietnia 1964 r. (Kodeks cywilny, Dz.U. z 1964 r., Nr 16, poz. 93 ze zm.).
[23] Zob. A. Szewc, Z problematyki ochrony danych, cz. II, Radca Prawny 1999, nr 4.
[24] Dalej w skrócie zwane rozporządzeniem w sprawie rodzajów i zakresu dokumentacji medycznej.
[25] Dz. U. Nr 64, poz. 565.
[26] Por. § 54 ust. 1 rozporządzenia w sprawie rodzajów i zakresu dokumentacji medycznej.
[27] Por. § 54 ust. 2 rozporządzenia w sprawie rodzajów i zakresu dokumentacji medycznej.

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

zbiorów danych objętych dokumentacją. W tym miejscu należy nadmienić, iż zgodnie z delegacją zawartą w § 55 ust. 6 rozporządzenia w sprawie rodzajów i zakresu dokumentacji medycznej w sprawach nieuregulowanych stosuje się przepisy wydane na podstawie art. 18 ust. 1 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne[28]. Zbiory informacji objętych dokumentacją prowadzoną w postaci elektronicznej powinny być sporządzane z uwzględnieniem postanowień Polskich Norm, których przedmiotem są zasady gromadzenia i wymiany informacji w ochronie zdrowia przenoszących normy europejskie lub normy innych państw członkowskich Europejskiego Obszaru Gospodarczego przenoszących te normy[29].

Z punktu widzenia cechy zapewnienia integralności i niezmienialności danych zawartych w dokumentacji prowadzonej w postaci elektronicznej niezwykle istotne znaczenie ma ust. 1 § 55 rozporządzenia zgodnie z którym sporządzenie i podpisanie dokumentacji prowadzonej w postaci elektronicznej polega na zapisaniu sekwencji danych na informatycznym nośniku danych[30] i podpisaniu tych danych, zgodnie z ustawą z dnia 18 września 2001 r. o podpisie elektronicznym[31]. Używając sformułowania „podpisaniu tych danych" minister zdrowia nie określił jednak, o jaki rodzaj podpisu chodzi. Czy ma to być **podpis elektroniczny (tzw. zwykły)**, czy też może **bezpieczny podpis elektroniczny**? Podpis elektroniczny to bowiem dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby go składającej[32]. Podpis spełniający powyższe wymagania nazywany jest zwykłym podpisem elektronicznym. Posługiwanie się takim podpisem jest najtańszym i najprostszym rozwiązaniem w zakresie bezpiecznej transmisji danych przy użyciu systemów teleinformatycznych (spełnia on bowiem funkcje potwierdzenia tożsamości danej osoby fizycznej

[28] Zastosowanie znajdzie rozporządzenie Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz. U. Nr 212, poz. 1766). Zgodnie z § 2 tego rozporządzenia systemy teleinformatyczne używane przez podmioty publiczne do realizacji zadań publicznych:
1) powinny spełniać właściwości i cechy w zakresie funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, określone w normach ISO zatwierdzonych przez krajową jednostkę normalizacyjną, na etapie projektowania, wdrażania i modyfikowania tych systemów,
2) powinny zostać wyposażone w składniki sprzętowe i oprogramowanie,
a) umożliwiające wymianę danych z innymi systemami teleinformatycznymi używanymi do realizacji zadań publicznych za pomocą protokołów komunikacyjnych i szyfrujących określonych w załączniku nr 1 do rozporządzenia, stosownie do zakresu działania tych systemów,
b) zapewniające dostęp do zasobów informacji udostępnianych przez systemy teleinformatyczne używane do realizacji zadań publicznych przy wykorzystaniu formatów danych określonych w załączniku nr 2 do rozporządzenia.
[29] Por. § 59 ust. 1 rozporządzenia. W przypadku braku Polskich Norm przenoszących normy europejskie lub normy innych państw członkowskich Europejskiego Obszaru Gospodarczego przenoszących te normy uwzględnia się: normy międzynarodowe, polskie normy, europejskie normy tymczasowe.
[30] Zgodnie z art. 3 pkt 1 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, informatyczny nośnik danych oznacza materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej lub analogowej.
[31] Dz. U. Nr 130, poz. 1450 ze zm.
[32] Zob. art. 3 pkt 1 ustawy o podpisie elektronicznym.

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

oraz z reguły ich poufności (szyfrowanie)[33]. Natomiast bezpieczny podpis elektroniczny jest to podpis elektroniczny, który:

1. jest przyporządkowany wyłącznie do osoby składającej ten podpis,
2. jest sporządzany za pomocą podlegających wyłącznej kontroli osoby składającej podpis elektroniczny bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania podpisu elektronicznego,
3. jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna[34].

Podkreślić należy, iż szczególnie istotna jest treść punktu trzeciego, mianowicie bezpieczny podpis elektroniczny powinien być powiązany z danymi, do których został dołączony, w taki sposób aby jakakolwiek późniejsza zmiana tych danych mogła być rozpoznawalna. Oznacza to, że nie tyle zapewnia on wykrycie treści zmiany, ile umożliwia wykrycie zmiany w ogóle[35].

Należy pamiętać także o treści art. 8 ustawy o podpisie elektronicznym, zgodnie z którym nie można odmówić ważności i skuteczności podpisowi elektronicznemu tylko na tej podstawie, że istnieje w postaci elektronicznej lub dane służące do weryfikacji podpisu nie mają kwalifikowanego certyfikatu lub z tego powodu, że nie został złożony za pomocą bezpiecznego urządzenia służącego do składania podpisu elektronicznego[36]. Podkreślić należy, iż przepis ten odnosi się do każdego podpisu, nie tylko kwalifikowanego. Zakaz dyskryminacji jest skierowany zarówno do organów stosujących prawo (sądów, urzędów), jak i uczestników obrotu prawnego. Podpisowi elektronicznemu nie można odmówić ważności czy skuteczności, powołując się wyłącznie na wyliczone powyżej przyczyny[37].

Rozporządzenie w sprawie rodzajów i zakresu dokumentacji medycznej nie określa także, czy użyty podpis elektroniczny ma być opatrzony certyfikatem, a jeżeli taki jest wymagany, to jaki ma być jego rodzaj: **zwykły**[38], czy też **kwalifikowany**[39]? Certyfikat służy bowiem identyfikacji osoby posługującej się podpisem elektronicznym[40]. Jest on czymś w rodzaju

[33] M. Świerczyński, w: Prawo Internetu, pod. red. P. Podreckiego, wyd. 2, Warszawa 2007, s. 74-75.
[34] Zob. art. 3 pkt 2 ustawy o podpisie elektronicznym.
[35] R. Podpłoński, P. Popis, Podpis elektroniczny. Komentarz, Warszawa 2004, s. 47.
[36] Patrz także: D. Szostek, M. Świerczyński, Prawne możliwości poszerzenia rynku podpisu elektronicznego w Polsce, w: Prawo umów elektronicznych, pod red. J. Gołaczyńskiego, Kraków 2006, s. 176-177.
[37] A. Bieliński, Charakter podpisu w polskim prawie cywilnym materialnym i procesowym, Warszawa 2007, s. 119.
[38] Zgodnie z art. 3 pkt 10 ustawy o podpisie elektronicznym pod pojęciem certyfikatu należy rozumieć elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji podpisu elektronicznego (klucz publiczny) są przyporządkowane do osoby składającej podpis elektroniczny i które umożliwiają identyfikację tej osoby.
[39] Art. 3 pkt 12 ustawy o podpisie elektronicznym definiuje go jako certyfikat spełniający warunki określone w ustawie, wydany przez kwalifikowany podmiot świadczący usługi certyfikacyjne, spełniający warunki określone w ustawie.
[40] Ustawa o podpisie elektronicznym w art. 3 pkt 3 definiuje osobę składającą podpis elektroniczny jako osobę fizyczną posiadającą urządzenie służące do składania podpisu elektronicznego, która działa w imieniu własnym albo w imieniu innej osoby fizycznej, prawnej albo jednostki organizacyjnej nie posiadającej osobowości prawnej.

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

„elektronicznego dowodu osobistego" użytkownika sieci komputerowej[41]. Pojawia się zatem oczywiste pytanie, który rodzaj podpisu elektronicznego z użyciem jakiego certyfikatu powinien być użyty przy podpisywaniu dokumentacji prowadzonej w postaci elektronicznej?

Z materii regulowanej komentowanym rozporządzeniem[42] oraz kardynalnych zasad obrotu takimi danymi można wysnuć wniosek, iż jedynie posłużenie się bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu jest w stanie zadośćuczynić wymogom bezpieczeństwa w odniesieniu do tak wrażliwych danych, jakimi są informacje zawarte w dokumentacji medycznej. Wyłącznie opatrzenie oświadczenia woli złożonego w postaci elektronicznej bezpiecznym podpisem elektronicznym weryfikowanym ważnym kwalifikowanym certyfikatem jest zrównane z oświadczeniem woli złożonym w formie pisemnej (art. 78 § 2 k.c.) oraz uznanie danych w postaci elektronicznej opatrzonych bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu z dokumentami opatrzonymi podpisami własnoręcznymi (art. 5 ust. 2 ustawy o podpisie elektronicznym).

Dodatkowym argumentem jest fakt, iż w przypadku, gdy do dokumentacji konieczne jest załączenie innych dokumentów, np. wyników badań, zdjęć radiologicznych oraz dokumentów podpisanych odręcznie, osoba wskazana przez kierownika zakładu przenosi te dokumenty na informatyczny nośnik danych oraz potwierdza zgodność z oryginałem materiałów przetworzonych do postaci elektronicznej, opatrując je własnym podpisem elektronicznym, a następnie umieszcza w elektronicznych zbiorach danych w sposób zapewniający dostęp i powiązanie pomiędzy dokumentami[43].

Dla oznaczenia daty sporządzenia dokumentu, złożenia podpisu na dokumencie oraz w celu zachowania chronologii wpisów w dokumentacji zbiorczej wewnętrznej stosuje się **znacznik czasu**[44]. Wydaje się, iż pod pojęciem znacznika czasu można rozumieć zdefiniowaną w art. 3 pkt 16 ustawy o podpisie elektronicznym usługę znakowania czasem polegającą na dołączaniu do danych w postaci elektronicznej logicznie powiązanych z danymi opatrzonymi podpisem lub poświadczeniem elektronicznym, oznaczenia czasu w chwili wykonania tej usługi oraz poświadczenia elektronicznego tak powstałych danych przez podmiot świadczący tę usługę. Instytucja znakowania czasem jest wyczerpująco uregulowana w art. 7 ustawy o podpisie

[41] M. Świerczyński, Prawo Internetu, op. cit. , s. 78.
[42] Warto zwrócić szczególnie uwagę na związek § 1 ust. 2 i § 2 rozporządzenia, który przewidując możliwość prowadzenia dokumentacji medycznej w postaci pisemnej i elektronicznej jednocześnie wymaga, aby dokumentację prowadzoną w formie pisemnej podpisywał pracownik zakładu zgodnie z uprawnieniami zawodowymi i ustalonym w zakładzie zakresie czynności. Ma on zatem obowiązek złożenia podpisu własnoręcznego, z czego zatem można wnosić, iż dokumentacja prowadzona w postaci elektronicznej wymaga opatrzenia takim podpisem elektronicznym, który pod względem skutków prawnych będzie równoważny podpisowi własnoręcznemu.
[43] Por. § 55 ust. 4 rozporządzenia w sprawie rodzajów i zakresu dokumentacji medycznej.
[44] Por. § 55 ust. 3 rozporządzenia w sprawie rodzajów i zakresu dokumentacji medycznej.

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

elektronicznym, razem w wymogami jakie musi spełnić, aby wywołać skutki daty pewnej. Podkreślić należy, iż znakowane czasem mogą być same dane w postaci elektronicznej logicznie powiązane z danymi opatrzonymi podpisem lub poświadczeniem elektronicznym oraz sam podpis elektroniczny i to każdy, nie tylko bezpieczny. Przede wszystkim, aby znakowanie czasem wywołało skutki daty pewnej usługa ta świadczona przez kwalifikowany podmiot świadczący usługi certyfikacyjne. W takiej sytuacji domniemywa się, że podpis elektroniczny znakowany czasem przez kwalifikowany podmiot świadczący usługi certyfikacyjne został złożony nie później, niż w chwili dokonywania tej usługi[45].

Utrwalenie dokumentacji prowadzonej w postaci elektronicznej polega na jej zapisaniu na informatycznym nośniku danych w sposób zapewniający sprawdzenie jej integralności, możliwość weryfikacji podpisu elektronicznego lub danych identyfikujących oraz możliwość odczytania wszystkich informacji zawartych w tej dokumentacji, aż do zakończenia okresu przechowywania dokumentacji (§ 56 rozporządzenia). Takie sformułowanie przepisu niejako automatycznie wymusza posłużenie się bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu.

Udostępnianie dokumentacji prowadzonej w postaci elektronicznej następuje przez:

1. przekazanie informatycznego nośnika danych z zapisaną kopią dokumentacji;
2. dokonanie elektronicznej transmisji dokumentacji;
3. przekazanie papierowych wydruków — na żądanie podmiotów lub organów, o których mowa w § 52 ust. 1.

Udostępnianie dokumentacji medycznej jest odpłatne. Zgodnie z art. 18 ust. 4f ustawy o zoz opłata nie może przekraczać 0,001 przeciętnego wynagrodzenia w poprzednim kwartale ogłoszonego przez Prezesa GUS.

Ustawodawca wyraźnie stwierdza, iż dokumentacja udostępniana uprawnionym do tego podmiotom prawa powinna być opatrzona bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu (§ 57 ust. 3 rozporządzenia). Skoro zatem w szczególnym przypadku przetwarzania danych, jakim jest ich udostępnianie, istnieje obowiązek posłużenia się bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu, to zupełnie traci na znaczeniu posługiwanie się zwykłym podpisem elektronicznym.

Dokumentacja prowadzona w postaci elektronicznej może być także udostępniona w formie papierowych wydruków, wówczas powinna być opatrzona podpisem odręcznym osoby

[45] A. Bieliński, Charakter podpisu, op. cit., s. 203; D. Szostek, Elektroniczna data pewna, Przegląd Prawa Handlowego 2003, Nr 3.

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

uprawnionej. Podmiot, któremu udostępniono w ten sposób dokumentację ma obowiązek potwierdzenia jej otrzymania podpisem odręcznym lub podpisem elektronicznym[46].

Dokumentację prowadzoną w postaci elektronicznej udostępnia się z zachowaniem jej integralności oraz ochrony danych osobowych (§ 57 ust. 2 rozporządzenia), co oznacza iż w przypadku tzw. dokumentacji medycznej zbiorczej należy udostępnić tylko dane dotyczące konkretnego pacjenta.

Przechowywana w postaci elektronicznej może być tylko dokumentacja, która została utrwalona zgodnie z § 56 rozporządzenia. W czasie przechowywania należy zapewnić ustalenie daty jej utrwalenia. Ponadto przechowywanie dokumentacji w postaci elektronicznej opatrzonej właściwym rodzajem podpisu elektronicznego powinno być realizowane zgodnie z postanowieniami art. 7 ustawy o podpisie elektronicznym[47]. Wyraźnie zatem zostało uczynione odesłanie do omówionej wcześniej usługi znakowania czasem. Po upływie wymaganego okresu przechowywania dokumentacja prowadzona w postaci elektronicznej zostaje usunięta w sposób nieodwracalny.

Dokumentację prowadzoną w postaci elektronicznej uważa się za zabezpieczoną, jeżeli w sposób ciągły są spełnione łącznie następujące warunki:

1. Zapewniona jest jej dostępność wyłącznie dla osób uprawnionych;
2. Chroniona jest przed przypadkowym lub nieuprawnionym zniszczeniem;
3. Zastosowane są metody i środki ochrony dokumentacji, których skuteczność w czasie ich zastosowania jest powszechnie uznawana[48].

Wnioski

Z przedstawionej tu analizy wynikają następujące wnioski. Niewątpliwie zostały zapewnione warunki dla prowadzenia dokumentacji medycznej w postaci elektronicznej. O poważnym podejściu do tego zagadnienia przez ustawodawcę świadczy fakt późniejszego wejścia w życie rozdziału 7 rozporządzenia. Jak się wydaje celem przedłużonego *vacatio legis* było danie zakładom opieki zdrowotnej odpowiedniego czasu do wdrożenia rozwiązań technicznych umożliwiających obieg dokumentów w tej postaci. Martwi jednak użycie w niektórych rozwiązaniach nieprecyzyjnych sformułowań, które mogą budzić uzasadnione wątpliwości.

W literaturze podkreśla się, iż forsowanie poglądów, zgodnie z którymi powinno stosować się tzw. bezpieczny podpis elektroniczny weryfikowany przy użyciu ważnego kwalifikowanego

[46] Zob. § 57 ust. 5 komentowanego rozporządzenia.
[47] Zob § 58 rozporządzenia.
[48] Zob. § 60 ust. 1 rozporządzenia w sprawie rodzajów i zakresu dokumentacji medycznej.

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone

certyfikatu skutkuje niskim stopniem zainteresowania podpisem elektronicznym ze względu na koszty jego wdrożenia[49]. Argument ten niewątpliwie ważki nie może przesłaniać jednak faktu, iż w przypadku dokumentacji medycznej obowiązek ochrony danych w niej zawartych plasuje się na pierwszym miejscu. Wydaje się, iż ciężar gatunkowy prawa pacjenta do ochrony danych medycznych przeważa interesy zakładów opieki zdrowotnej. Ustawodawca dał temu wyraz regulując kwestię obowiązku udostępniania danych przy użyciu tylko tzw. bezpiecznego podpisu elektronicznego. Ponieważ zakład opieki zdrowotnej jest zobowiązany do udostępniania danych medycznych licznym podmiotom prawa wydaje się, iż tylko zainwestowanie w technologię, która uwzględnia instytucję bezpiecznego podpisu elektronicznego faktycznie przyczyni się do usprawnienia działalności zakładów.

[49] Zob. D. Szostek, M. Świerczyński, Prawne możliwości, op. cit., s. 175-176.

Prawa autorskie :: CBKE :: Wszystkie prawa zastrzeżone