Krzysztof Świtała[1]

Obowiązki prawne podmiotów przetwarzających dane medyczne w kontekście wdrażania rozwiązań e-zdrowia w Polsce[2]

1. Wstęp

Problematyka ochrony danych medycznych i zachowania prywatności pacjentów wydaje się szczególnie aktualnym zagadnieniem w erze upowszechniania się technologii informacyjno-komunikacyjnych w ochronie zdrowia, związanym z coraz szerszym wykorzystaniem elektronicznej dokumentacji medycznej i wdrażaniem kompleksowych rozwiązań informatycznych e-zdrowia[3] na poziomie regionalnym i krajowym. W kontekście wyzwań demograficznych stojących przed Europą, związanych ze starzeniem się społeczeństw i systematycznie wzrastającymi wydatkami na opiekę zdrowotną, technologie informacyjno-komunikacyjne mogą pozwolić na zwiększenie sprawności i efektywności publicznych systemów ochrony zdrowia oraz dostępności świadczeń zorientowanych na potrzeby pacjenta[4]. Nadal jednak jedną ze zidentyfikowanych podstawowych barier rozwoju e-zdrowia jest brak zaufania do tych rozwiązań zarówno pacjentów, jak i osób wykonujących zawody medyczne, wynikający

[1] Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie, Wydział Prawa i Administracji.

[2] Publikacja powstała w ramach projektu badawczego Preludium finansowanego przez Narodowe Centrum Nauki (2014/13/N/HS5/03523).

[3] Pojęcie to jest rozumiane jako „wykorzystanie technologii informacyjno-komunikacyjnych (ICT) w ochronie zdrowia w takich celach, jak na przykład: leczenie pacjentów, prowadzenie badań, kształcenie studentów, wykrywanie chorób oraz monitorowanie stanu zdrowia społeczeństwa". K. Korczak, *Internetowe narzędzia wspomagające opiekę zdrowotną*, Wolters Kluwer, Warszawa 2014, s. 44, cyt. za: www.who.int/topics/ehealth/en (data odczytu: 05.07.2010).

[4] C. Di Iorio, F. Carinci, *Privacy and Health Care Information Systems: Where Is the Balance?*, w: *eHealth: Legal, Ethical and Governance Challenges*, red. C. George, D. Whitehouse, P. Duquenoy, Springer-Verlag, Berlin–Heidelberg 2013, s. 77.

z przekonania o fragmentaryczności i nieadekwatności obowiązujących instrumentów prawnych w zakresie ochrony prywatności[5].

Biorąc pod uwagę znaczenie tej problematyki, w niniejszym artykule zaprezentowano podstawowe instrumenty normatywne i standardy techniczne ochrony danych medycznych w Polsce, do których stosowania są zobowiązane podmioty odpowiedzialne za ich przetwarzanie.

2. Pojęcie danych medycznych

Zgodnie z definicją zawartą w art. 6 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 1997 r. Nr 133, poz. 883), a także w art. 4 pkt 2 nowego ogólnego rozporządzenia UE o ochronie danych[6] za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Nie ulega wątpliwości, że dane medyczne pacjentów przetwarzane w elektronicznej dokumentacji medycznej i systemie informacji w ochronie zdrowia mają charakter takich danych[7]. W większości przypadków informacje te dotyczą stanu zdrowia osoby, a zatem powinny być kwalifikowane do kategorii szczególnie chronionych sensytywnych danych osobowych, ustanowionej na podstawie art. 27 ustawy o ochronie danych osobowych[8], a także art. 9 ogólnego rozporządzenia UE o ochronie danych. W opinii ekspertów Grupy Roboczej (art. 29) „wszelkie dane zawarte w dokumentacji medycznej, w elektronicznej dokumentacji zdrowotnej oraz w systemach EHR należy traktować jako dane osobowe szczególnie chronione”[9].

Już w rekomendacji Rady Europy R (97) 5 dotyczącej danych medycznych zaproponowano rozumienie pojęcia danych dotyczących zdrowia, które odnoszą się do wszelkich danych osobowych dotyczących stanu zdrowia danej osoby.

---

5 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Plan działania w dziedzinie e-zdrowia na lata 2012–2020 – Innowacyjna opieka zdrowotna w XXI wieku”, COM(2012) 736, s. 11–12.

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 (Dz. Urz. UE L z 4.5.2016 Nr 119/1).

7 M. Jackowski, *Ochrona danych medycznych*, Wolters Kluwer, Warszawa 2011, s. 28.

8 *Dokumentacja medyczna*, red. U. Drozdowska, Cegedim, Warszawa 2012, s. 39.

9 Dokument roboczy w sprawie przetwarzania danych osobowych dotyczących zdrowia w elektronicznej dokumentacji zdrowotnej (EHR), 00323/07/PL WP 131, Bruksela 2007, s. 4.

W podobny sposób zdefiniowano ten termin w treści nowych ram ochrony danych osobowych w Unii Europejskiej, uzupełniając jego zakres przedmiotowy o dane związane ze świadczeniem usług opieki zdrowotnej na rzecz osoby, której te dane dotyczą (art. 4 pkt 15 ogólnego rozporządzenia UE o ochronie danych).

W aktualnym stanie prawnym w art. 2 pkt 7 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. z 2011 r. Nr 113, poz. 657) wprowadzono również definicję pojęcia jednostkowych danych medycznych, rozumianych jako dane osobowe oraz inne dane osób fizycznych dotyczące uprawnień do udzielonych, udzielanych i planowanych świadczeń opieki zdrowotnej, stanu zdrowia, a także inne dane przetwarzane w związku z planowanymi, udzielanymi i udzielonymi świadczeniami opieki zdrowotnej oraz profilaktyką zdrowotną i realizacją programów zdrowotnych. Konstrukcja tego przepisu jest poddawana krytyce przedstawicieli doktryny ze względu na niekonsekwentne różnicowanie danych osobowych i jednostkowych danych medycznych w treści tej ustawy, przez co wykładnia zakresów znaczeniowych tych pojęć może być niespójna. Kontrowersyjne jest również wyodrębnienie kategorii innych danych osób fizycznych dotyczących świadczeń zdrowotnych, w przypadku których biorąc pod uwagę zindywidualizowany charakter usług opieki zdrowotnej i dokumentacji medycznej, należy stwierdzić, że w większości mieszczą się w zakresie definicji danych osobowych[10]. Trzeba się jednak zgodzić ze stwierdzeniem, że termin „jednostkowe dane medyczne" ma szerszy zakres znaczeniowy niż pojęcie danych o stanie zdrowia *sensu stricto*[11].

3. Ochrona danych medycznych na podstawie przepisów dotyczących ochrony danych osobowych

Treść normatywna art. 36 ustawy o ochronie danych osobowych, a także art. 24 i 32 ogólnego rozporządzenia UE o ochronie danych obliguje administratora danych, którym w przypadku dokumentacji medycznej jest podmiot prowadzący działalność leczniczą, a w przypadku systemu informacji medycznej minister właściwy do spraw zdrowia, do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych

[10] D. Wąsik, *Ustawa o systemie informacji w ochronie zdrowia. Komentarz*, Wolters Kluwer, Warszawa 2015, s. 34.

[11] M. Jackowski, op.cit., s. 37–38.

odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności do zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Szczegółowe wymagania bezpieczeństwa w zakresie ochrony danych osobowych nałożone na administratora danych uregulowano w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024)[12]. Akt ten w par. 3 zobowiązuje administratora danych do wdrożenia podstawowych zabezpieczeń organizacyjnych w postaci dokumentacji przetwarzania danych, składającej się z następujących obligatoryjnych elementów:

- polityki bezpieczeństwa;
- instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

Zgodnie z par. 6 dane wrażliwe o stanie zdrowia są przetwarzane w systemach teleinformatycznych o poziomie bezpieczeństwa podwyższonym lub wysokim – w przypadku połączenia rozwiązań służących do przetwarzania danych z publiczną siecią telekomunikacyjną. Szczegółowy katalog i opis środków bezpieczeństwa stosowany na poszczególnych poziomach określa załącznik do omawianego rozporządzenia.

Przy podejmowaniu decyzji dotyczących wyboru zabezpieczeń administrator danych powinien wziąć pod uwagę przede wszystkim: koszt ich implementacji, charakter chronionych danych i związanych z nimi zagrożeń oraz rozmiary ewentualnej szkody powiązanej z nieuprawnionym przetwarzaniem danych[13].

4. Ochrona danych medycznych na podstawie przepisów dotyczących prowadzenia dokumentacji medycznej

Podmiot prowadzący dokumentację medyczną jest obowiązany, na podstawie art. 24 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw

[12] M. Polok, *Bezpieczeństwo danych osobowych*, Wydawnictwo C.H. Beck, Warszawa 2008, s. 262–263.

[13] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Wolters Kluwer, Warszawa 2011, s. 620.

Pacjenta (Dz. U. z 2009 r. Nr 52, poz. 417), do zapewnienia ochrony danych zawartych w tej dokumentacji. Szczegółowe obowiązki w tym zakresie nałożone na te podmioty zostały uregulowane w rozporządzeniu Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz. U. z 2015 r. poz. 2069). Zgodnie z par. 74 tego aktu podmiot przetwarzający tę dokumentację zapewnia odpowiednie warunki zabezpieczające ją przed zniszczeniem, uszkodzeniem lub utratą i dostępem osób nieupoważnionych, a także umożliwiające jej wykorzystanie bez zbędnej zwłoki. Szczególne wymagania bezpieczeństwa odnoszą się do przetwarzania dokumentacji w postaci elektronicznej. W par. 80 tego rozporządzenia wskazano, że powinna być ona prowadzona w systemie teleinformatycznym zapewniającym m.in.:

- zabezpieczenie dokumentacji przed uszkodzeniem lub utratą;
- zachowanie integralności dokumentacji i powiązanych z nią metadanych;
- stały dostęp do dokumentacji osób uprawnionych oraz zabezpieczenie przed dostępem osób nieuprawnionych.

Przepis par. 86 rozporządzenia zawiera z kolei katalog warunków, które muszą zostać spełnione, aby dokumentacja medyczna mogła być uznana za zabezpieczoną. Zawarto w nim wskazanie, że powinno się stosować metody i środki ochrony dokumentacji, których skuteczność w czasie ich zastosowania jest powszechnie uznawana (par. 86 ust. 1 pkt 3). Wydaje się, że wskazany *in fine* warunek należy zrekonstruować w kontekście par. 85 rozporządzenia, nakazującego sporządzanie dokumentacji medycznej z uwzględnieniem postanowień norm technicznych (w szczególności polskich norm), których przedmiotem są zasady gromadzenia i wymiany informacji w ochronie zdrowia. Poza przepisami prawa, na podstawie treści tych dokumentów powinien być dobierany i ustalony katalog uznanych za skuteczne metod i środków ochrony dokumentacji medycznej przetwarzanej w postaci elektronicznej. Zagadnienie to zostanie rozwinięte w części artykułu poświęconej analizie podstawowych norm technicznych z zakresu bezpieczeństwa danych medycznych.

Redakcja par. 85 wydaje się problematyczna z dwóch powodów: nie wyznacza choćby przykładowego katalogu norm technicznych, jakie powinny być uwzględniane przez podmioty sporządzające dokumentację medyczną, oraz stoi w sprzeczności z wyrażoną w przepisach polskiego prawa zasadą dobrowolności uczestnictwa w procesie normalizacji.

W pierwszym wypadku lapidarność tego przepisu utrudnia zrekonstruowanie katalogu obowiązków w zakresie zabezpieczenia przetwarzanej dokumentacji medycznej, co wydaje się sprzeczne z zasadą przyzwoitej legislacji

i pewności prawa, wywodzoną z zawartej w art. 2 Konstytucji RP zasady demokratycznego państwa prawnego[14]. W orzecznictwie Trybunału Konstytucyjnego wskazano, że „zasada zaufania obywatela do państwa i stanowionego przez nie prawa opiera się na pewności prawa, a więc takim zespole cech przysługujących prawu, które zapewniają jednostce bezpieczeństwo prawne; umożliwiają jej decydowanie o swoim postępowaniu w oparciu o pełną znajomość przesłanek (…) oraz konsekwencji prawnych, jakie jej działania mogą pociągnąć za sobą"[15]. Z zasady lojalności państwa wobec adresata norm prawnych wynika zaś konieczność zagwarantowania przez ustawodawcę adresatom unormowań prawnych najwyższego stopnia obliczalności i przewidywalności możliwych interpretacji i rozstrzygnięć[16].

Druga uwaga wiąże się ze sprzecznością treści par. 85 rozporządzenia w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania z wyrażoną w art. 4 pkt 3 ustawy z dnia 12 września 2002 r. o normalizacji (Dz. U. z 2002 r. Nr 169, poz. 1386) zasadą dobrowolności stosowania norm. Jej treść uzupełnia reguła zawarta w art. 5 ust. 3 wspomnianej ustawy, w którym wyraźnie wskazano, że stosowanie polskich norm jest dobrowolne. Postawiona tu teza znajduje swoje potwierdzenie w orzecznictwie sądów administracyjnych: „(…) w świetle przepisów ustawy z 2002 r. o normalizacji opracowywane przez komitety techniczne Polskie Normy nie pełnią roli przepisów prawa. Nadanie im takiego waloru wymaga regulacji szczególnej, zawartej w przepisie rangi ustawowej, natomiast przywołanie Polskich Norm w rozporządzeniu nie skutkuje nałożeniem obowiązku ich stosowania. Akt niższego rzędu nie może zmienić postanowień aktu wyższego rzędu, jakim jest ustawa z 2002 r. o normalizacji"[17].

Wśród szczegółowego katalogu warunków bezpiecznego przetwarzania dokumentacji medycznej w postaci elektronicznej, zawartego w par. 86 ust. 2 rozporządzenia w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania, należy zwrócić uwagę na obowiązki:

- systematycznego dokonywania analizy zagrożeń (par. 86 ust. 2 pkt 1) i stosowania do nich adekwatnych środków bezpieczeństwa (par. 86 ust. 2 pkt 3) oraz

[14] L. Garlicki, *Polskie prawo konstytucyjne*, Liber, Warszawa 2006, s. 62.

[15] Wyrok TK z dnia 14 czerwca 2000 r., sygn. P 3/00, OTK ZU nr 5/2000, poz. 138.

[16] Wyrok TK z dnia 11 maja 2004 r., sygn. K 4/03; wyrok TK z dnia 20 stycznia 2009 r., sygn. P 40/07.

[17] Wyrok Wojewódzkiego Sądu Administracyjnego w Krakowie z dnia 23 lipca 2012 r., sygn. II SA/Kr 745/12, LEX nr 1228983.

- bieżącego kontrolowania funkcjonowania wszystkich organizacyjnych i techniczno-informatycznych sposobów zabezpieczenia dokumentacji medycznej, a także okresowego dokonywania oceny skuteczności tych sposobów (par. 86 ust. 2 pkt 4).

W pierwszym przypadku mamy do czynienia z regulacją podstawowych powinności związanych z przeprowadzaniem procesu zarządzania ryzykiem[18]. Jest on jednak ograniczony do kwestii dotyczących analizy zagrożeń, definiowanych jako potencjalne przyczyny „niepożądanego incydentu, którego skutkiem może być szkoda dla systemu"[19], a nie oznacza kompleksowego rozumienia pojęcia ryzyka w bezpieczeństwie informacji, związanego z rozpoznaniem zagrożeń i środowiska (istniejących w nim podatności i zidentyfikowanych wymagań bezpieczeństwa)[20]. Zapewniające efektywność, rzetelność i skuteczność podejmowanych działań zintegrowane podejście w tym zakresie zdefiniowano w normie ISO 27005, dotyczącej zarządzania ryzykiem w bezpieczeństwie informacji[21]. Zgodnie z regułami ustanowionymi w tym standardzie katalog szczegółowych obowiązków związanych z bieżącą kontrolą i oceną skuteczności zabezpieczeń dokumentacji medycznej wynika z powszechnie uznanej koncepcji ciągłego doskonalenia procesów w ramach systemu zarządzania bezpieczeństwem informacji (SZBI).

5. Zapewnianie bezpieczeństwa danych na podstawie przepisów dotyczących minimalnych wymagań w przypadku publicznych systemów teleinformatycznych

W przypadku podmiotów publicznych należących do sektora ochrony zdrowia, oprócz wcześniej omówionych obowiązków prawnych w zakresie ochrony danych medycznych, konieczne do spełnienia są również wymagania ustanowione

---

[18] M. Byczkowski, J. Zawiła-Niedźwiecki, *Analiza ryzyka w zarządzaniu bezpieczeństwem danych osobowych. Zarządzanie ryzykiem w kontekście ochrony informacji*, „Dodatek do Monitora Prawniczego" 2014, nr 9, s. 47–48.

[19] A. Białas, *Podstawy bezpieczeństwa systemów teleinformatycznych*, Wydawnictwo Pracowni Komputerowej Jacka Skalmierskiego, Gliwice 2002, s. 22.

[20] K. Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Wydawnictwo Naukowe PWN, Warszawa 2009, s. 78–79.

[21] G. Kuta, *Zarządzanie ryzykiem bezpieczeństwa informacji niejawnych – obecnie i w przyszłości*, w: *Przeszłość, teraźniejszość i przyszłość ochrony informacji niejawnych w zapewnieniu bezpieczeństwa narodowego*, red. J. Sobczak, KSOIN i UŚ, Katowice 2014, s. 129–142.

w par. 20 i 21 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2012 r. poz. 526), dotyczące zasad prowadzenia w takiej jednostce SZBI oraz szczegółowych rozwiązań zapewniających jego rozliczalność. Pierwszy przywołany przepis zobowiązuje podmioty publiczne do prowadzenia SZBI zgodnego ze szczegółowymi wymaganiami, uregulowanymi w ust. 2, oraz koncepcją ciągłego doskonalenia jego procesów, opartą na modelu cyklu Deminga i podejściu wykorzystującym zarządzanie ryzykiem[22]. Zgodnie z par. 20 ust. 3 wspomniane wymagania uznaje się za spełnione, jeżeli SZBI został opracowany zgodnie z normą ISO 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audyty są realizowane w zgodzie z wytycznymi zawartymi w normach: ISO 27002 (dawniej 17799), ISO 27005 i ISO 24762. Nie jest w tym wypadku bezwzględnie wymagane przeprowadzenie kosztownego i czasochłonnego procesu certyfikacji zgodności z przedstawionymi standardami.

6. Wymagania dotyczące bezpieczeństwa w przypadku dokumentacji medycznej przetwarzanej w systemie informacji medycznej

Istotnym aktem z punktu widzenia zapewniania bezpieczeństwa danych osobowych przetwarzanych w systemie informacji w ochronie zdrowia jest rozporządzenie Ministra Zdrowia z dnia 28 marca 2013 r. w sprawie wymagań dla Systemu Informacji Medycznej (Dz. U. z 2013 r. poz. 463). Przepisy par. 10–12 określają m.in. warunki organizacyjno-techniczne przetwarzania, udostępniania, autoryzacji oraz zabezpieczenia elektronicznej dokumentacji medycznej przed utratą. Bezpieczeństwo wymiany danych w tym systemie jest także gwarantowane implementacją wymogów zawartych w normie PN-EN 13606-4 (na podstawie par. 9 pkt 2 tego rozporządzenia.) oraz prowadzeniem SZBI z uwzględnieniem wytycznych normy ISO 27799 (zgodnie z par. 9 ust. 2 pkt 3). Analogicznie uregulowano wymagania bezpieczeństwa w akcie wykonawczym

[22] K. Świtała, *Prawnoadministracyjne aspekty problematyki bezpieczeństwa informacji w podmiotach publicznych*, „Przegląd Prawa Publicznego" 2013, nr 10, s. 24–27.

dotyczącym funkcjonowania systemów teleinformatycznych P1 i P2 obsługujących system informacji w ochronie zdrowia[23].

7. Ochrona danych medycznych w przepisach regulujących tajemnice zawodów medycznych

W przepisach prawa regulujących funkcjonowanie systemu ochrony zdrowia ustanowiono szereg ograniczeń jawności przetwarzanych w nim informacji. Najważniejszymi i najstarszymi instytucjami prawnymi tego rodzaju są tajemnice zawodów medycznych[24]. Bez wątpienia „zachowanie w tajemnicy informacji związanych z pacjentem jest ważne z punktu widzenia poszanowania jego prywatności i intymności, a także utrzymania zaufania do osób wykonujących medyczne profesje. Instytucja ta, zapewniając ochronę wspomnianych wartości, jest jedną z najważniejszych gwarancji należytego ukształtowania relacji pomiędzy osobą wykonującą zawód medyczny a pacjentem, opartej na wzajemnym zaufaniu oraz poszanowaniu autonomii i podmiotowości"[25]. Zgodnie z art. 13 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta pacjent ma prawo do zachowania w tajemnicy przez osoby wykonujące zawód medyczny informacji z nim związanych, a uzyskanych w związku z wykonywaniem tego zawodu. W przypadku większości aktów prawnych regulujących zasady wykonywania poszczególnych profesji medycznych odnajdziemy przepisy szczególne (*lex specialis*) ustanawiające i chroniące tajemnice zawodowe:

- lekarza i lekarza dentysty – art. 40 ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (Dz. U. z 1997 r. Nr 28, poz. 152);
- pielęgniarki i położnej – art. 17 ustawy z dnia 15 lipca 2011 r. o zawodach pielęgniarki i położnej (Dz. U. z 2011 r. Nr 174, poz. 1039);
- felczera – art. 7 ustawy z dnia 20 lipca 1950 r. o zawodzie felczera (Dz. U. z 1950 r. Nr 36, poz. 336);

---

[23] Rozporządzenie Ministra Zdrowia z dnia 14 sierpnia 2013 r. w sprawie opisu, minimalnej funkcjonalności oraz warunków organizacyjno-technicznych funkcjonowania Platformy Udostępniania On-Line Usług i Zasobów Cyfrowych Rejestrów Medycznych oraz Elektronicznej Platformy Gromadzenia, Analizy i Udostępnienia Zasobów Cyfrowych o Zdarzeniach Medycznych (Dz. U. z 2013 r. poz. 1001).

[24] M. Safjan, *Prawo i medycyna. Ochrona praw jednostki a dylematy współczesnej medycyny*, Instytut Wymiaru Sprawiedliwości, Warszawa 1998, s. 106–107.

[25] K. Świtała, *Tajemnice zawodów medycznych – podstawowa charakterystyka*, „Monitor Prawniczy" 2014, nr 11, s. 603.

- diagnosty laboratoryjnego – art. 29 ustawy z dnia 27 lipca 2001 r. o diagnostyce laboratoryjnej (Dz. U. z 2001 r. Nr 100, poz. 1083);
- farmaceuty – art. 21 pkt 2 ustawy z dnia 19 kwietnia 1991 r. o izbach aptekarskich (Dz. U. z 1991 r. Nr 41, poz. 179);
- fizjoterapeuty – art. 9 pkt 3 ustawy z dnia 25 września 2015 r. o zawodzie fizjoterapeuty (Dz. U. z 2015 r. poz. 1994);
- ratownika medycznego – art. 11 ust. 9 pkt 3 ustawy z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym (Dz. U. z 2013 r. poz. 757 j.t.);
- psychologa – art. 14 ust. 1 ustawy z dnia 8 czerwca 2001 r. o zawodzie psychologa i samorządzie zawodowym psychologów (Dz. U. z 2001 r. Nr 73, poz. 763).

W przypadku zawodów medycznych niemających uregulowanej w przepisach prawa własnej instytucji tajemnicy zawodowej stosujemy wprost normy ogólne z ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.

Poza tajemnicami zawodów medycznych w ustawodawstwie należącym do sektora ochrony zdrowia uregulowano wiele rodzajów, wyodrębnionych zarówno podmiotowo, jak i przedmiotowo, innych tajemnic prawnie chronionych, np. tajemnicę:

- psychiatryczną – art. 50 ust. 1 ustawy z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego (Dz. U. z 1994 r. Nr 111, poz. 535);
- przeszczepów – art. 19 ust. 1 ustawy z dnia 1 lipca 2005 r. o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów (Dz. U. z 2005 r. Nr 169, poz. 1411);
- dawcy krwi – art. 13 ustawy z dnia 22 sierpnia 1997 r. o publicznej służbie krwi (Dz. U. z 1997 r. Nr 106, poz. 681);
- Służby Medycyny Pracy – art. 11 ust. 3 z dnia 27 czerwca 1997 r. o służbie medycyny pracy (Dz. U. z 1997 r. Nr 96, poz. 593);
- osób wykonujących czynności związane z planowaniem rodziny, ochroną płodu ludzkiego i przerywaniem ciąży – art. 4c ust. 1 ustawy z dnia 7 stycznia 1993 r. o planowaniu rodziny, ochronie płodu ludzkiego i warunkach dopuszczalności przerywania ciąży (Dz. U. z 1993 r. Nr 17, poz. 78);
- znaków identyfikacyjnych pacjentów szpitali – art. 36 ust. 5 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz. U. z 2011 r. Nr 112, poz. 654);
- badań klinicznych – art. 37b ust. 2 pkt 3 ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne (Dz. U. z 2001 r. Nr 126, poz. 1381);
- danych zawartych w elektronicznej dokumentacji medycznej – art. 24 ust. 3 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2009 r. Nr 52, poz. 417).

Przepisy te nie zawierają jednak szczególnych wymagań dotyczących zabezpieczania informacji objętych omówionymi powyżej tajemnicami. W takiej sytuacji stosujemy w tym zakresie przedstawione wcześniej przepisy dotyczące ochrony danych osobowych[26] i dokumentacji medycznej[27].

8. Ochrona danych medycznych a normy techniczne z zakresu informatyzacji ochrony zdrowia

Poza przepisami prawa problematykę bezpieczeństwa danych medycznych regulują także normy techniczne ustanowione przez Polski Komitet Normalizacyjny[28]. Do tej grupy należą następujące standardy:

- **PN-EN ISO 10781:2015-11** – model funkcjonalny systemu elektronicznej dokumentacji zdrowotnej HL7, wersja 2; system przetwarzający elektroniczną dokumentację medyczną powinien spełniać wymagania opisane w niniejszej normie; w jej treści określono model funkcjonalny systemu elektronicznej dokumentacji zdrowotnej zgodnego ze standardami HL7; w modelu tym podano listę referencyjną wyodrębnionych z perspektywy użytkownika funkcji, które mogą występować w systemie elektronicznej dokumentacji zdrowotnej (EHR-S); katalog funkcjonalności w zakresie bezpieczeństwa obejmuje następujące elementy: uwierzytelnianie podmiotu, autoryzacja podmiotu, kontrola dostępu dla podmiotu, zarządzanie dostępem pacjenta, niezaprzeczalność, bezpieczna wymiana danych, poświadczanie informacji, zabezpieczenie prywatności i poufności danych pacjenta;
- **PN-EN ISO 27799:2010** – informatyka w ochronie zdrowia – zarządzanie bezpieczeństwem informacji w ochronie zdrowia z wykorzystaniem ISO/IEC 27002; w normie tej określono wskazówki dotyczące wsparcia interpretacji i stosowania w sektorze ochrony zdrowia standardu ISO 27002; określono zbiór szczegółowych praktycznych wytycznych i narzędzi kontrolnych w zakresie zarządzania bezpieczeństwem informacji w ochronie zdrowia;
- **PN-EN 13606-4:2009** – informatyka w ochronie zdrowia – przesyłanie elektronicznej dokumentacji zdrowotnej – część 4: bezpieczeństwo danych;

[26] R. Kubiak, *Tajemnica medyczna*, C.H. Beck, Warszawa 2015, s. 31.
[27] Ibidem, s. 18.
[28] K. Nyczaj, P. Piecuch, *Elektroniczna dokumentacja medyczna. Wdrożenie i prowadzenie w placówce medycznej*, Wiedza i Praktyka, Warszawa 2013, s. 95.

w dokumencie tym opisano metodologię określania uprawnień niezbędnych do uzyskania dostępu do danych EHR; metodologia ta stanowi część ogólnej architektury przesyłania danych EHR.

Jak już wcześniej wspominano, niektóre przepisy szczegółowe regulujące funkcjonowanie modułów systemu informacji w ochronie zdrowia i zasady prowadzenia elektronicznej dokumentacji medycznej zobowiązują administratorów danych do stosowania wymagań i wytycznych uregulowanych w wymienionych normach technicznych.

9. Inne standardy związane z problematyką bezpieczeństwa danych medycznych

Poza omówionymi wcześniej wymaganiami prawnymi i normami technicznymi z zakresu bezpieczeństwa danych medycznych w ostatnich latach wydano wiele aktów należących do kategorii prawa miękkiego (ang. *soft law*), dotyczących holistycznego podejścia do problematyki bezpieczeństwa usług publicznych (także w obszarze ochrony zdrowia) i powiązanych z nimi zbiorów danych. Dokumenty takie są przejawem tendencji do regulowania zagadnień charakteryzujących się dużą dynamiką zmian i występujących na pograniczu zakresu działania systemu prawa, procesów zarządczych i technologii informacyjno-komunikacyjnych za pomocą elastycznych instrumentów prawa miękkiego. Pozwalają one rozszerzyć oddziaływanie podmiotów publicznych na obszary, gdzie zastosowanie skutecznych mechanizmów tradycyjnego prawa stanowionego jest ograniczone[29]. Przykładem może być tu dokument odnoszący się do pryncypiów architektury korporacyjnej podmiotów publicznych[30], zawierający pryncypium generalne dotyczące zapewniania przez cały okres cyklu życia bezpieczeństwa danych przetwarzanych w związku ze świadczeniem elektronicznych usług publicznych (GEN3). Podobną zasadę sformułowano wcześniej

[29] B. Fischer, *Transgraniczność prawa administracyjnego na przykładzie regulacji przekazywania danych osobowych z Polski do państw trzecich*, Wolters Kluwer, Warszawa 2010, s. 288–289.

[30] *Pryncypia architektury korporacyjnej podmiotów publicznych*, Warszawa 2015, https://mc.gov.pl/files/pryncypia_pryncypia_architektury_korporacyjnej_podmiotow_publicznych_w._1.0.pdf (data odczytu: 01.08.2015).

w dokumentach strategicznych z tego zakresu w USA (2007 r.) i Danii (2003 r.)[31]. Warto dodać, że analiza treści obowiązującego *Programu zintegrowanej informatyzacji państwa*[32] potwierdza potrzebę stworzenia w Polsce odpowiednich warunków do funkcjonowania efektywnej i bezpiecznej e-administracji, pozwalającej na skuteczne świadczenie usług publicznych. W lutym 2016 r. Ministerstwo Cyfryzacji sformułowało nowe założenia strategii cyberbezpieczeństwa dla Rzeczypospolitej Polskiej[33].

Jeśli chodzi o akty prawa miękkiego dotyczące bezpieczeństwa przetwarzania danych w ochronie zdrowia, to szczególną uwagę należy zwrócić na opublikowany w 2014 r. przez Centrum Systemów Informacyjnych Ochrony Zdrowia dokument zawierający wytyczne, zasady i rekomendacje dla usługodawców w zakresie budowy i stosowania systemu bezpiecznego przetwarzania elektronicznej dokumentacji medycznej[34]. Zawiera on analizę modeli architektury bezpiecznego przechowywania EHR (model klasyczny, outsourcing, *Cloud Computing*, platformy regionalne), model logiczny systemu wspierającego bezpieczne przetwarzanie EHR (cykl życia EHR, tworzenie dokumentacji w postaci elektronicznej, dodawanie wpisów do dokumentacji, struktura EHR, autoryzacja dokumentu, gromadzenie, przechowywanie, udostępnianie i archiwizacja EHR) oraz przykładowe scenariusze dotyczące bezpiecznego przetwarzania EHR. Podstawowym mankamentem tego aktu jest jego ograniczony zakres przedmiotowy – odnosi się przede wszystkim do zabezpieczania procesów przetwarzania danych w elektronicznej dokumentacji medycznej, w dużej mierze pomijając zagadnienia bezpieczeństwa usług elektronicznych e-zdrowia oraz te dotyczące wymagań i wytycznych odnośnie do SZBI dla podmiotów z sektora ochrony zdrowia.

---

[31] A. Sobczak, *Pryncypia architektury korporacyjnej*, w: *Wstęp do architektury korporacyjnej*, red. B. Szafrański, A. Sobczak, WAT, Warszawa 2009, s. 78–89.

[32] *Program zintegrowanej informatyzacji państwa*, Warszawa 2013, https://mc.gov.pl/files/pzip_ostateczny.pdf (data odczytu: 01.08.2016).

[33] *Założenia strategii cyberbezpieczeństwa dla Rzeczypospolitej Polskiej*, Warszawa 2016, https://mc.gov.pl/files/zalozenia_strategii_cyberbezpieczenstwa_v_final_z_dnia_22-02–2016.pdf (data odczytu: 01.04.2016).

[34] *Wytyczne, zasady i rekomendacje dla usługodawców w zakresie budowy i stosowania systemu bezpiecznego przetwarzania elektronicznej dokumentacji medycznej*, Warszawa 2014, http://csioz.gov.pl/file.php?s=YT8xOTc= (data odczytu: 30.10.2015).

10. Podsumowanie

Po przeanalizowaniu istniejących w Polsce regulacji prawnych w zakresie bezpieczeństwa danych medycznych można sformułować następujące wnioski i postulaty *de lege ferenda*:

- zapewnienie większej spójności przepisów prawnych dotyczących ochrony danych osobowych, tajemnic zawodów medycznych i przetwarzania dokumentacji medycznej;
- wprowadzenie kompleksowego minimalnego standardu normatywnego podstawowych wymagań odnośnie do SZBI w podmiotach publicznych należących do sektora ochrony zdrowia (na wzór par. 20 rozporządzenia w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych), uwzględniającego obowiązki w zakresie zarządzania ryzykiem i implementację paradygmatu *Privacy by Design*[35];
- wzmocnienie obowiązków związanych z przeglądami polityk bezpieczeństwa i ciągłym doskonaleniem SZBI przez cały okres cyklu życia w podmiotach publicznych należących do sektora ochrony zdrowia;
- wprowadzenie sankcji administracyjnych o charakterze pieniężnym za naruszenie zasad bezpieczeństwa danych medycznych przez podmioty publiczne należące do sektora ochrony zdrowia;
- wprowadzenie obowiązków notyfikacyjnych w związku z incydentami dotyczącymi bezpieczeństwem danych medycznych (obowiązek informacyjny wobec podmiotów danych i organów nadzorczych);
- publikowanie przez organy nadzorcze na bieżąco aktualizowanych katalogów dobrych praktyk w zakresie bezpieczeństwa danych medycznych i wytycznych dotyczących wdrażania odpowiednich zabezpieczeń w SZBI podmiotów publicznych należących do sektora ochrony zdrowia;
- zapewnienie wsparcia organizacyjnego i finansowego podmiotom publicznym należącym do sektora ochrony zdrowia w zakresie wdrażania i doskonalenia SZBI.

[35] Omówienie tego zagadnienia w kontekście konstrukcji prawnych gwarancji ochrony prywatności przedstawił: W. Wiewiórowski, *Privacy by Design jako paradygmat ochrony prywatności*, w: *Internet. Prawno-informatyczne problemy sieci, portali i e-usług*, red. G. Szpor, W. Wiewiórowski, Wydawnictwo C.H. Beck, Warszawa 2012, s. 13–29.

Warto również zwrócić uwagę na fakt, że część zaprezentowanych postulatów zostanie zrealizowana przy okazji wprowadzania instrumentów prawnych związanych z reformą mechanizmów ochrony danych osobowych w UE – sankcje administracyjne o charakterze pieniężnym, obowiązki notyfikacyjne, a także podejście uwzględniające potrzebę zarządzania ryzykiem i stosowanie paradygmatu *Privacy By Design*[36]. Bez wątpienia harmonizacja prawa w tym obszarze na poziomie UE wzmocni funkcjonowanie wspólnego rynku przepływu informacji, przy jednoczesnym utrzymaniu gwarancji normatywnych realizacji praw podmiotów danych[37]. Należy pamiętać jednak o tym, że właściwe wdrożenie i poziom skuteczności nowych instrumentów prawnych będą w dużej mierze determinowane efektywną koordynacją wprowadzania nowych regulacji, spójnymi regułami kontroli tych procesów i edukacją w zakresie nowych obowiązków prowadzoną przez krajowe organy ochrony danych osobowych w państwach członkowskich UE.

Bibliografia

Barta J., Fajgielski P., Markiewicz R., *Ochrona danych osobowych. Komentarz*, Wolters Kluwer, Warszawa 2011.

Białas A., *Podstawy bezpieczeństwa systemów teleinformatycznych*, Wydawnictwo Pracowni Komputerowej Jacka Skalmierskiego, Gliwice 2002.

Byczkowski M., Zawiła-Niedźwiecki J., *Analiza ryzyka w zarządzaniu bezpieczeństwem danych osobowych. Zarządzanie ryzykiem w kontekście ochrony informacji*, „Dodatek do Monitora Prawniczego" 2014, nr 9, s. 47–48.

Di Iorio C., Carinci F., *Privacy and Health Care Information Systems: Where Is the Balance?*, w: *eHealth: Legal, Ethical and Governance Challenges*, red. C. George, D. Whitehouse, P. Duquenoy, Springer-Verlag, Berlin–Heidelberg 2013, s. 77–105.

Dokument roboczy w sprawie przetwarzania danych osobowych dotyczących zdrowia w elektronicznej dokumentacji zdrowotnej (EHR), 00323/07/PL WP 131, Bruksela 2007.

Dokumentacja medyczna, red. U. Drozdowska, Cegedim, Warszawa 2012.

[36] D. Karwala, *Nowa unijna regulacja w zakresie danych osobowych – uwagi na temat projektu rozporządzenia z dnia 25 stycznia 2012 r. – część 1*, „Czas Informacji" 2012, nr 1, s. 42–44.

[37] W. Wiewiórowski, *Nowe ramy ochrony danych osobowych w Unii Europejskiej*, „Dodatek do Monitora Prawniczego" 2012, nr 7, s. 9.

Fischer B., *Transgraniczność prawa administracyjnego na przykładzie regulacji przekazywania danych osobowych z Polski do państw trzecich*, Wolters Kluwer, Warszawa 2010.

Garlicki L., *Polskie prawo konstytucyjne*, Liber, Warszawa 2006.

Jackowski M., *Ochrona danych medycznych*, Wolters Kluwer, Warszawa 2011.

Karwala D., *Nowa unijna regulacja w zakresie danych osobowych – uwagi na temat projektu rozporządzenia z dnia 25 stycznia 2012 r. – część 1*, „Czas Informacji" 2012, nr 1, s. 38–44.

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Plan działania w dziedzinie e-zdrowia na lata 2012–2020 – Innowacyjna opieka zdrowotna w XXI wieku", COM(2012) 736.

Korczak K., *Internetowe narzędzia wspomagające opiekę zdrowotną*, Wolters Kluwer, Warszawa 2014.

Kubiak R., *Tajemnica medyczna*, Wydawnictwo C.H. Beck, Warszawa 2015.

Kuta G., *Zarządzanie ryzykiem bezpieczeństwa informacji niejawnych – obecnie i w przyszłości*, w: *Przeszłość, teraźniejszość i przyszłość ochrony informacji niejawnych w zapewnieniu bezpieczeństwa narodowego*, red. J. Sobczak, KSOIN i UŚ, Katowice 2014, s. 129–142.

Liderman K., *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Wydawnictwo Naukowe PWN, Warszawa 2009.

Nyczaj K., Piecuch P., *Elektroniczna dokumentacja medyczna. Wdrożenie i prowadzenie w placówce medycznej*, Wiedza i Praktyka, Warszawa 2013.

Polok M., *Bezpieczeństwo danych osobowych*, Wydawnictwo C.H. Beck, Warszawa 2008.

Safjan M., *Prawo i medycyna. Ochrona praw jednostki a dylematy współczesnej medycyny*, Instytut Wymiaru Sprawiedliwości, Warszawa 1998.

Sobczak A., *Pryncypia architektury korporacyjnej*, w: *Wstęp do architektury korporacyjnej*, red. B. Szafrański, A. Sobczak, WAT, Warszawa 2009, s. 78–89.

Świtała K., *Prawnoadministracyjne aspekty problematyki bezpieczeństwa informacji w podmiotach publicznych*, „Przegląd Prawa Publicznego" 2013, nr 10, s. 21–30.

Świtała K., *Tajemnice zawodów medycznych – podstawowa charakterystyka*, „Monitor Prawniczy" 2014, nr 11, s. 603–608.

Wąsik D., *Ustawa o systemie informacji w ochronie zdrowia. Komentarz*, Wolters Kluwer, Warszawa 2015.

Wiewiórowski W., *Nowe ramy ochrony danych osobowych w Unii Europejskiej*, „Dodatek do Monitora Prawniczego" 2012, nr 7, s. 2–9.

Wiewiórowski W., *Privacy by Design jako paradygmat ochrony prywatności*, w: *Internet. Prawno-informatyczne problemy sieci, portali i e-usług*, red. G. Szpor, W. Wiewiórowski, Wydawnictwo C.H. Beck, Warszawa 2012, s. 13–29.

Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych), COM(2012) 11.

Źródła sieciowe

e-Health, www.who.int/topics/ehealth/en (data odczytu: 05.07.2010).

Program zintegrowanej informatyzacji państwa, Warszawa 2013, https://mc.gov.pl/files/pzip_ostateczny.pdf (data odczytu: 01.08.2016).

Pryncypia architektury korporacyjnej podmiotów publicznych, Warszawa 2015, https://mc.gov.pl/files/pryncypia_pryncypia_architektury_korporacyjnej_podmiotow_publicznych_w._1.0.pdf (data odczytu: 01.08.2015).

Wytyczne, zasady i rekomendacje dla usługodawców w zakresie budowy i stosowania systemu bezpiecznego przetwarzania elektronicznej dokumentacji medycznej, Warszawa 2014, http://csioz.gov.pl/file.php?s=YT8xOTc= (data odczytu: 30.10.2015).

Założenia strategii cyberbezpieczeństwa dla Rzeczypospolitej Polskiej, Warszawa 2016, https://mc.gov.pl/files/zalozenia_strategii_cyberbezpieczenstwa_v_final_z_dnia_22-02–2016.pdf (data odczytu: 01.04.2016).

* * *

The legal obligations for medical data processing entities in the context of e-Health solutions in Poland

Summary

Without a doubt, one of the most important issues for the information society is the improvement of the health conditions of citizens. This can be done by using information and communication technologies to reduce costs, and to produce more effective resource consumption in the health sector. However, in this context, we should note the importance of ensuring the right balance between the functionality of e-Health services on the one hand; and reliable, legally and technically adequate guaranties for the patient's privacy, related to her or his autonomy, on the other. Without meeting these requirements it seems impossible to achieve a satisfactory level of patient confidence in the implementation of ICT in the healthcare sector.

Keywords: e-Health, EHR, personal data protection, medical data, ISMS, risk management