

Ewa KAWIAK-JAWOR

Magister socjologii, asystent w Katedrze Zdrowia Publicznego
Wydziału Nauk o Zdrowiu Uniwersytetu Medycznego w Lublinie

Monika KACZORUK

Magister zdrowia publicznego, asystent w Katedrze Zdrowia Publicznego
Wydziału Nauk o Zdrowiu Uniwersytetu Medycznego w Lublinie

Paulina KACZOR-SZKODNY

Magister zdrowia publicznego, Zakład Biostatystyki, Demografii i Epidemiologii,
Instytut Medycyny Wsi w Lublinie;

doktorantka w Katedrze Zdrowia Publicznego, Uniwersytet Medyczny w Lublinie

Ewa DUDZIŃSKA

Dr n. med., asystent w Katedrze Zdrowia Publicznego
Wydziału Nauk o Zdrowiu Uniwersytetu Medycznego w Lublinie

Bezpieczeństwo danych medycznych w kontekście wdrożenia elektronicznej dokumentacji medycznej

I. Dokumentacja medyczna w formie elektronicznej

Wdrożenie założeń Strategii E-zdrowie Polska 2009–2015 jest kierunkiem nieuniknionych zmian w obszarze ochrony zdrowia. Jednym z jej kluczowych założeń jest wprowadzenie elektronicznego obiegu dokumentacji medycznej. Główne kierunki tych zmian wyznacza ustawa z dnia 28 kwietnia 2011 r. *o systemie informacji w ochronie zdrowia*¹. Wprowadza ona obowiązek prowadzenia dokumentacji medycznej w wersji elektronicznej od 1 stycznia 2019 roku. Realizacja tych założeń, mimo iż termin ten był już wielokrotnie prolongowany, stoi pod znakiem zapytania. Jednym z najbardziej istotnych wyzwań, jakie stoją przed podmiotami leczniczymi jest zapewnienie bezpieczeństwa danych w obiegu elektronicznym.

Właściwe dokumentowanie wszystkich istotnych informacji w indywidualnej dokumentacji medycznej pacjenta, związanych z jego leczeniem, jest obowiązkiem wynikającym z przepisów ustawy z dnia 6.11.2008 r. *o prawach pacjenta i Rzeczniku Praw Pacjenta*². W rozdziale 7 ustawy określono prawo pacjenta do dokumentacji medycznej. Ustawa nakłada na podmioty udzielające świadczeń zdrowotnych obowiązek prowadzenia dokumentacji medycznej, jej przechowywania i udostępniania pacjentom oraz ich przedstawicielom, lekarzom i pielęgniarkom dla celów medycznych oraz innym instytucjom wymienionym w ustawie. W art. 26 wspomnianej ustawy określono dokładnie jakie podmioty mogą mieć dostęp do dokumentacji medycznej. W rozdziale 7 zawarto

¹ Ustawa z 28.04.2011 r. *o systemie informacji w ochronie zdrowia*, t.j. Dz. U. 2016, poz. 1535, 1579, 2020, z 2017 r. poz. 599.

² Ustawa z 6.11.2008 r. *o prawach pacjenta i Rzeczniku Praw Pacjenta*, t.j. Dz. U. 2009, Nr 52, poz. 417, 2018.

również delegację ustawową do wydania rozporządzenia w sprawie dokumentacji medycznej dla Ministra Zdrowia oraz ministrów posiadających resortową służbę zdrowia.

Zgodnie z obowiązującymi przepisami prawa, dokumentację medyczną można prowadzić w formie elektronicznej i tradycyjnej papierowej³. Po 31 grudnia 2018 r. dokumentacja medyczna powinna być prowadzona już jedynie w postaci elektronicznej. Od 2020 roku obowiązkowo zafunkcjonuje elektroniczna recepta, a od 2021 e-skierowanie. Zgodnie z założeniem ustawy, taka forma prowadzenia dokumentacji ma zapewnić szybszy i bardziej kompleksowy dostęp do potrzebnych informacji zarówno personelowi medycznemu, jak i samemu pacjentowi⁴.

Nowelizacja ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia dokonuje zmian w zakresie definicji elektronicznej dokumentacji medycznej. Z art. 2 pkt 6 wynika, że EDM zdefiniowana jest jako dokumenty umożliwiające usługobiorcy uzyskanie od usługodawcy świadczenia opieki zdrowotnej określonego rodzaju. Całość dokumentacji ma być gromadzona na Elektronicznej Platformie Gromadzenia, Analizy i Udostępniania Zasobów Cyfrowych o Zdarzeniach Medycznych P1.

Zgodnie z § 80 rozporządzenia Ministra Zdrowia w sprawie prowadzenia dokumentacji medycznej, „dokumentacja może być prowadzona w postaci elektronicznej, pod warunkiem prowadzenia jej w systemie teleinformatycznym zapewniającym: właściwe zabezpieczenie danych przed uszkodzeniem lub utratą oraz zabezpieczenie integralności danych poprzez ochronę przed nieuprawnionym dostępem. Jednocześnie istotne dla właściwego zabezpieczenia potrzeb zdrowotnych jest umożliwienie stałego dostępu do danych dla osób uprawnionych. Dostęp ten może zostać zapewniony pod warunkiem właściwej identyfikacji osoby dokonującej wpisu oraz osoby udzielającej świadczeń zdrowotnych. Realizację tego założenia zapewni dokumentowanie dokonywanych przez te osoby zmian w dokumentacji medycznej oraz metadanych. Kolejną z istotnych funkcjonalności systemu teleinformatycznego jest możliwość udostępnienia dokumentacji medycznej lub innych danych i zestawień w formie plików XML lub PDF. Umożliwia to sprawne raportowanie, prowadzenie statystyk w tym badań naukowych. Funkcja ta zapewnia również możliwość dostępu do dokumentacji medycznej w wybranych zakresach dla samego pacjenta. Prawo pacjenta do uzyskania dostępu do własnej dokumentacji zabezpiecza również możliwość wydruku danych przetwarzanych w systemie teleinformatycznym.

II. Osoby upoważnione do przetwarzania danych z dokumentacji

Zgodnie z art. 24 ust. 2 u.p.p osoby wykonujące zawód medyczny, czynności pomocnicze przy udzielaniu świadczeń zdrowotnych, a także czynności związane z utrzymaniem systemu teleinformatycznego, na podstawie upoważnienia administratora danych, są uprawnione do przetwarzania danych zawartych w dokumentacji medycznej. W zależności od funkcji pełnionej przez osoby uprawnione ustawa wskazuje również na cele w jakich może dochodzić do przetwarzania zawartych w systemie danych. Osoby upoważnione są również zobowiązane do zachowania tajemnicy informacji zwią-

³ Rozporządzenie Ministra Zdrowia z 21.12.2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania, Dz. U. 2010, Nr 252, poz. 1697.

⁴ Ustawa z 28.04. 2011 r. o systemie informacji w ochronie zdrowia (t.j. Dz. U. 2016, poz. 1535, 1579, 2020.)

zanych z pacjentem uzyskanych w związku z wykonywaniem pracy. Tajemnica ta pozostaje w mocy również po śmierci pacjenta.

W toku kontroli NIK badano indywidualną dokumentację medyczną pod względem jej tworzenia i prowadzenia zgodnego z obowiązującymi przepisami. Stwierdzono, że tylko 26,5% badanej dokumentacji (458 kart spośród 1730) prowadzonej było prawidłowo, tzn. spełniało wszystkie wymagania określone przepisami, a 49,4% badanej dokumentacji (854 karty) zawierało do pięciu uchybień różnego rodzaju. Natomiast 24,1% badanej dokumentacji (418 kart) prowadzonej było nieprawidłowo, tzn. w każdej z kart stwierdzono więcej niż pięć uchybień różnego rodzaju⁵.

Prowadzenie dokumentacji medycznej w sposób elektroniczny niewątpliwie przyczyni się do ograniczenia liczby błędów zawartych w danych dotyczących procesu diagnozy i leczenia. Wykorzystanie technologii informacyjno-komunikacyjnych wymusi większą czytelność i kompletność zawartych w EDM danych.

III. Elektroniczny rekord pacjenta

Elektroniczny rekord pacjenta (ERP) jest terminem, który ma bardzo szerokie znaczenie. W literaturze międzynarodowej istnieje wiele pojęć o zbliżonym znaczeniu: *EHR* – *electronic health record*, *EPR* – *electronic patient record*, *EMR* – *electronic medical record*, *CPR* – *computerised patient rekord*. Ogromna różnorodność systemów i rozwiązań technologicznych wpływa na zakres i precyzyjną definicję pojęcia. Elektroniczny Rekord Pacjenta może być rozumiany, jako zbiór pewnych danych pacjenta, które są zgromadzone w określonym miejscu. Różnice w definicji wynikają z precyzyjnego określenia, które dane należy gromadzić, kto może odczytywać i edytować dane oraz w którym miejscu dane są gromadzone. W szerszym znaczeniu ERP jest definiowany, jako system informatyczny, system zarządzania danymi, który umożliwia zbieranie i korzystanie z danych dotyczących pacjentów⁶.

Budowa systemu elektronicznej wymiany danych medycznych trwa od lat 90. ubiegłego wieku. W tym czasie dokonały się zasadnicze przekształcenia zarówno w obszarze uwarunkowań prawnych, jak i społecznych. Nowo budowany system musi sprostać oczekiwaniom wielu interesariuszy systemu. Jednakże niezależnie od cech specyficznych dla poszczególnych stron priorytetem zawsze było i jest bezpieczeństwo danych.

Obecnie kluczowym aktem prawnym regulującym cały proces informatyzacji jest ustawa z dnia 28 kwietnia 2011 roku *o systemie informacji w ochronie zdrowia*, która weszła w życie 1 stycznia 2012 roku. Umożliwia ona wprowadzenie Systemu Informacji Medycznej (SIM), dzięki któremu lekarze w całej Polsce otrzymają dostęp do informacji o udzielanych i planowanych świadczeniach zdrowotnych.

Pierwotnie tekst ustawy definiował elektroniczną dokumentację medyczną, odwołując się do rozporządzenia w sprawie rodzajów, zakresu i wzorów dokumentacji medycz-

⁵ T. J. Marcinkowski, T. Kaczmarek, A. Herfort, R. Szozda, Cz. Żaba, *Rola i znaczenie dokumentacji medycznej w orzecznictwie ubezpieczeniowym oraz w postępowaniu sądowym*, „Orzecznictwo Lekarskie” 2011, nr 8, s. 73–78.

⁶ E. Buczak-Stec, K. Lemanowicz, M. Mazurek, *E-zdrowie – wyzwanie dla systemu ochrony zdrowia*, „Przegląd Epidemiologiczny” 2011, nr 65(1), s. 107–114.

nej oraz sposobu jej przetwarzania, w którym w zasadzie każdy zbiór danych medycznych traktowany jest formalnie jako dokument medyczny. Doprowadzało to do szeregu wątpliwości natury prawnej oraz problemów technicznych. W wyniku nowelizacji ustawy dokonano doprecyzowania definicji elektronicznej dokumentacji medycznej w polskim prawie. Obecnie katalog elektronicznej dokumentacji medycznej został wyznaczony przez wskazanie konkretnych rodzajów dokumentów, które podlegać będą obowiązkowi ich wytworzenia w postaci elektronicznej oraz opatrzenia kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP. Dokumenty medyczne podlegające obowiązkowi ich wytworzenia w postaci elektronicznej zostaną wskazane w nowym rozporządzeniu w sprawie rodzajów elektronicznej dokumentacji medycznej, które zostanie wydane na podstawie zmienionego art. 13 ustawy z dnia 28 kwietnia 2011 roku *o systemie informacji w ochronie zdrowia*.

W projekcie wymienia się trzy rodzaje elektronicznej dokumentacji medycznej:

- 1) informację o rozpoznaniu choroby, problemu zdrowotnego lub urazu, wynikach przeprowadzonych badań, przyczynie odmowy przyjęcia do szpitala, udzielonych świadczeniach zdrowotnych oraz ewentualnych zaleceniach – w przypadku odmowy przyjęcia pacjenta do szpitala, o której mowa w § 28 ust. 2 rozporządzenia Ministra Zdrowia z dnia 9 listopada 2015 r. *w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania*, Dz. U. poz. 2069;
- 2) informację dla lekarza kierującego świadczeniobiorcą, o której mowa w § 12 ust. 4 załącznika do rozporządzenia Ministra Zdrowia z dnia 8 września 2015 r. *w sprawie ogólnych warunków umów o udzielanie świadczeń opieki zdrowotnej*, Dz. U. 2016, poz. 1146;
- 3) kartę informacyjną z leczenia szpitalnego, o której mowa w § 2 ust. 4 pkt 5 rozporządzenia Ministra Zdrowia z dnia 9 listopada 2015 r. *w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania*.

W przyszłości katalog ten ma być sukcesywnie rozbudowywany, aż do momentu uzyskania pełnej informatyzacji usługodawców działających w systemie informacji.

IV. Zabezpieczenie danych

Dokumentacja medyczna stanowi szczególnie zestaw danych, które z uwagi na swój szczególny charakter winny być w sposób kompleksowy chronione przed nieuprawnionym dostępem i przetwarzaniem. Regulacje prawne dotyczące zabezpieczenia danych zawartych w dokumentacji medycznej reguluje wiele aktów prawnych w tym: ustawa z 27 sierpnia 2004 r. *o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych*⁷, ustawa z 29 sierpnia 1997 r. *o ochronie danych osobowych*⁸, rozporządzenie Ministra Zdrowia z dnia 9 listopada 2015 r. *w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania*.

Według art. 2 ustawy z dnia 28.04.2011 r. *o systemie informacji w ochronie zdrowia*, jednostkowe dane medyczne definiowane są jako dane osobowe gromadzone

⁷ Ustawa z 27.08.2004 r. *o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych*, t.j.: Dz. U. 2016, poz. 1793.

⁸ Ustawa z 29.08.1997 r. *o ochronie danych osobowych*, t.j.: Dz. U. 2016, poz. 922).

i przetwarzane w celu realizacji szeroko rozumianych świadczeń zdrowotnych. Każda dokumentacja medyczna stanowi dane osobowe i z tego tytułu regulowane są sposoby jej gromadzenia i przetwarzania. Już w opinii Grupy Roboczej ds. Ochrony Danych Komisji Europejskiej, wszelkie dane zawarte w dokumentacji medycznej należy traktować, jako „dane osobowe szczególnie chronione”⁹.

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, które od 25 maja 2018 zastąpi dyrektywę 95/46/We stwierdza, iż szczególnej ochronie podlegają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej, w tym o korzystaniu z usług opieki zdrowotnej, ujawniające informacje o stanie jej zdrowia.

Podmioty wykonujące działalność leczniczą zobowiązane są do zapewnienia odpowiedniego poziomu bezpieczeństwa danych medycznych¹⁰. Regulacje prawne dotyczące mechanizmów zabezpieczenia danych medycznych zawarte są w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku¹¹ w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Rozporządzenie definiuje trzy poziomy bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym, w zależności od kategorii przetwarzanych danych. Dane medyczne przetwarzane w systemie informatycznym podmiotu leczniczego należy zaliczyć do trzeciego wysokiego poziomu bezpieczeństwa stosowanego w sytuacji, kiedy w systemie informatycznym są przetwarzane wrażliwe dane osobowe, a sam system ma połączenie z publiczną siecią informatyczną. Aby zapewnić ochronę danych na właściwym poziomie należy między innymi dokonać zabezpieczenia budynków i pomieszczeń, w których przetwarzane są dane, stosować zabezpieczenia kontroli dostępu oraz mechanizmy tworzenia kopii zapasowych.

Centrum Systemów Informatycznych w Ochronie Zdrowia w 2017 r. wydało rekomendacje w zakresie bezpieczeństwa oraz rozwiązań technologicznych stosowanych podczas przetwarzania dokumentacji medycznej w postaci elektronicznej. W dokumencie prezentowane są wiarygodne rozwiązania z zakresu zabezpieczenia procesu przetwarzania danych medycznych. CSIOZ wskazuje na istotne zagrożenia związane z bezpieczeństwem funkcjonowania poszczególnych rozwiązań architektury informatycznej opartych na modelu klasycznym, outsourcingu oraz chmurze obliczeniowej¹².

Systemy teleinformatyczne używane przez podmioty lecznicze, funkcjonują w oparciu o normy uwzględniające cechy istotne z punktu widzenia ich zastosowa-

⁹ Grupa robocza ds. ochrony danych powołana na mocy art. 29, Dokument Roboczy w Sprawie Przetwarzania Danych Osobowych Dotyczących Zdrowia w Elektronicznej Dokumentacji Zdrowotnej (EHR), 00323/07/PL WP 131, 2007.

¹⁰ M. Łokaj, M. Narolski, *Komentarz praktyczny. Należyte prowadzenie elektronicznej dokumentacji medycznej pacjenta*, Lex-El 2017.

¹¹ Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 29.04.2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, Dz. U. 2004, Nr 100, poz. 1024.

¹² *Rekomendacje Centrum Systemów Informatycznych w Ochronie Zdrowia w zakresie bezpieczeństwa oraz rozwiązań technologicznych stosowanych podczas przetwarzania dokumentacji medycznej w postaci elektronicznej*, Warszawa 2017.

nia. Przede wszystkim muszą zapewnić możliwie pełną niezawodność działania oraz wydajność. Niezwykle istotna jest również możliwość dostosowania systemów do indywidualnych zakresów potrzeb w podmiotach leczniczych, co skutecznie może zapewnić skalowalność oraz modułowość systemu. Skuteczna implementacja systemu informatycznego zapewnia również bezpieczeństwo danych w systemie na każdym jej etapie. Zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury¹³. Na każdym etapie wdrażania systemu (projektowanie, wdrażanie, eksploatawanie, monitorowanie, przeglądanie, utrzymanie) niebywale istotne jest zarządzanie bezpieczeństwem danych, z uwzględnieniem Polskich Norm: PN-ISO/IEC 20000-1 i PN-ISO/IEC 20000-2.

V. Autoryzacja danych w systemie elektronicznej dokumentacji medycznej

W celu zapewnienia bezpieczeństwa i wiarygodności danych wprowadzanych do elektronicznej dokumentacji medycznej, osoba wprowadzająca dane do dokumentacji medycznej, musi w odpowiedni sposób autoryzować wpis. Zgodnie z obowiązującymi regulacjami prawnymi pracownik medyczny od 1 stycznia 2019 r. będzie musiał używać jednego z dwóch rodzajów autoryzacji wpisu do elektronicznej dokumentacji medycznej: Kwalifikowanego podpisu elektronicznego weryfikowanego przy pomocy ważnego certyfikatu lub Podpisu potwierdzonego profilem zaufanym ePUAP w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne¹⁴.

Kwalifikowany podpis elektroniczny zastąpił pojęcie bezpiecznego podpisu elektronicznego w rozumieniu ustawy z dnia 18 września 2001 r. *o podpisie elektronicznym*, która przestała obowiązywać. Został ustanowiony w celu skutecznego i bezpiecznego określenia tożsamości podmiotów, którzy uczestniczą w elektronicznym obrocie prawnym. Profil zaufany w przeciwieństwie do podpisu elektronicznego jest bezpłatną możliwością uwierzytelnienia osoby w systemach e-administracji¹⁵.

Obecnie w Polsce obowiązują bezpośrednio regulacje prawa Unii Europejskiej dotyczące podpisu elektronicznego zawarte w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 910/2014 z 23 lipca 2014 r. *w sprawie identyfikacji elektronicznej i usług zaufania publicznego w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE z 23.07.2014 r.* – rozporządzenie eIDAS, a ponadto ustawa *o usługach zaufania i identyfikacji elektronicznej* z 5.09.2016 r.¹⁶

¹³ A. Romaszewski, W. Trąbka, *Wymagania i standardy związane z przetwarzaniem danych medycznych*, Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie, 2014, s. 71–80.

¹⁴ M. Paszkowska, *Dokumentacja medyczna w świetle zmian przepisów*, „Medium. Gazeta Dolnośląskiej Izby Lekarskiej” 2016, <http://medium.dilnet.wroc.pl/index.php/luty-2016/910-2016-02-03-08-29-03>, 29 grudnia 2016; Rozporządzenie Parlamentu Europejskiego i Rady *w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do e-transakcji na rynku wewnętrznym*, NR 910/2014, Dz. U. Parlamentu Europejskiego L 257/73.

¹⁵ M. Paszkowska, *Dokumentacja Medyczna...*

¹⁶ M. Paszkowska, *Dokumentacja Medyczna...*

Kolejną istotną kwestią w aspekcie prowadzenia dokumentacji medycznej w wersji elektronicznej jest możliwość złożenia podpisu przez pacjenta. Pomimo wprowadzenia formy elektronicznej dokumentacji medycznej korzystanie z formy papierowej, z uwagi na zapewnienie bezpieczeństwa zdrowotnego, będzie konieczne w przypadku zgody na zabiegi o podwyższonym ryzyku medycznym dla pacjenta np. zabieg operacyjny. Dokument taki powinien zostać wydrukowany, opatrzony podpisem odręcznym, a następnie zeskanowany. Po odwzorowaniu cyfrowym i wprowadzeniu do systemu teleinformatycznego dokument powinien zostać zniszczony przez osobę upoważnioną. W niektórych przypadkach warto zachować kopie w formie papierowej dla celów dowodowych. Może stać się to użyteczne w przypadku konieczności przeprowadzenia dowodu z opinii biegłego z zakresu pisma ręcznego na okoliczność własnoręczności podpisu pacjenta.

VI. Zagrożenia bezpieczeństwa danych elektronicznych

Wśród opinii publicznej pojawia się szereg obaw o bezpieczeństwo danych elektronicznych w systemie. Powołując się na wyniki II edycji badania ankietowego, dotyczącego stopnia informatyzacji podmiotów wykonujących działalność leczniczą, przeprowadzone przez CSIOZ autorzy artykułów medialnych stawiają tezę o braku zabezpieczenia danych medycznych w systemach informatycznych w przypadku nawet co dziesiątej badanej jednostki¹⁷. Podmioty zapytane o stosowanie metod autoryzacji elektronicznych dokumentów medycznych w rozumieniu ustawy o SIOZ w zdecydowanej większości wskazywały na uwierzytelnienie użytkownika jedynie w lokalnym systemie informatycznym. CSIOZ w opublikowanym na swojej stronie oświadczeniu przedstawia tę sytuację, jako wystarczającą do właściwego zabezpieczenia danych i zgodną z obowiązującymi regulacjami prawnymi¹⁸. Do podpisywania elektronicznej dokumentacji medycznej pracownik medyczny może użyć kwalifikowanego podpisu elektronicznego lub podpisu potwierdzonego profilem zaufanym ePUAP. Jednostkowe dane medyczne, dopóki nie powstanie z nich dokument medyczny (EDM), nie muszą być potwierdzone powyższymi podpisami.

W chwili obecnej pojawia się wiele wyzwań związanych z prowadzeniem i zapewnieniem właściwego poziomu zabezpieczenia elektronicznej dokumentacji medycznej. Wynika to z faktu rozpoczęcia stosowania unormowań zawartych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 (RODO). Regulacje mają bowiem zastąpić wszelkie regulacje krajowe dotyczące ochrony danych osobowych osób fizycznych. Zmiany wchodzi w życie z dniem 25.05.2018 r. Nowe prawo nakłada na podmioty lecznicze obowiązek rozszerzenia dokumentacji

¹⁷ M. Janczura, K. Klinger, *Informatyzacja szpitali po polsku. Dane o naszych chorobach nie są zabezpieczane nawet hasłem*, W www.tokfm.pl, 2016, <http://www.tokfm.pl/Tokfm/7,102433,21016429,informatyzacja-szpitali-po-polsku-dane-o-naszyc-chorobach.html>, 21 stycznia 2017.

¹⁸ CSIOZ, *Wyjaśnienia do artykułu dotyczącego zabezpieczania danych medycznych pacjentów, gromadzonych w postaci elektronicznej*, 2016, <https://www.csioz.gov.pl/aktualnosci/szczegoly/wyjasnienia-do-artykulu-dotyczacego-zabezpieczania-danych-medycznych-pacjentow-gromadzonych-w-p/>, 21 stycznia 2017.

dotyczącej ochrony danych osobowych o dokumenty rejestru czynności przetwarzania. Odpowiedzialnym za zabezpieczenie informacji w jednostkach ochrony zdrowia będzie inspektor ochrony danych osobowych, którego zatrudnienie będzie obligatoryjne. Jedną z bardziej kontrowersyjnych zmian jest również wprowadzenie obowiązku informowania Urzędu Ochrony Danych Osobowych o każdym stwierdzonym naruszeniu zasad ochrony danych osobowych w ciągu 72 godzin. Regulacje RODO znacznie zwiększają również kary za wszelkie naruszenia¹⁹.

Właściwe przygotowanie podmiotów leczniczych do zbliżających się wyzwań, związanych z wprowadzeniem elektronicznej dokumentacji medycznej, e-zwolnienia, e-recepty, e-zlecenia, regulacji RODO i szeregu innych rozwiązań kształtujących wymianę informacji w systemie, powinno stać się priorytetem zarówno dla władz państwowych na wszystkich szczeblach, jak i zarządzających poszczególnymi jednostkami ochrony zdrowia.

Streszczenie

Właściwe dokumentowanie wszystkich istotnych informacji w indywidualnej dokumentacji medycznej pacjenta, związanych z jego leczeniem, jest obowiązkiem wynikającym z przepisów prawa. W celu zapewnienia bezpieczeństwa i wiarygodności danych wprowadzanych do elektronicznej dokumentacji medycznej osoba wprowadzająca do niej dane musi w odpowiedni sposób autoryzować wpis. Prowadzenie dokumentacji medycznej w postaci elektronicznej nie jest zatem nierozłącznie związane z posiadaniem przez lekarza podpisu elektronicznego w rozumieniu art. 18 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej. Autoryzacja wpisów dokonywanych przez niego w tej dokumentacji możliwa jest również przy wykorzystaniu wewnętrznych mechanizmów systemu teleinformatycznego innych niż kwalifikowany podpis elektroniczny.

Słowa kluczowe: bezpieczeństwo danych medycznych, elektroniczna dokumentacja medyczna, pacjent

Security of medical data in the context of the implementation of electronic medical records

Summary

Proper documentation of all relevant information in the patient's individual medical records related to his/her treatment is an obligation under the law. In order to ensure the safety and reliability of data entered in the electronic medical records, the person entering the data in the medical documentation must authorise the entry in an appropriate manner. Keeping medical records in an electronic form is therefore not inseparably connected with the physician having an electronic signature, as defined in Art. 18 of the Act of 5 September 2016 on trust services and electronic identification. Authorisation of entries made by the physician in this documentation is also possible using internal mechanisms of the ICT system other than a qualified electronic signature.

Key words: medical data security, electronic medical records, patient

¹⁹ M. Łokaj, *Ochrona zdrowia – co przyniesie rok 2018? Komentarz praktyczny LEX El.* (ABC, 2017).