ACTA IURIDICA RESOVIENSIA Nr 3(38)/2022

ISSN 2720-0574 DOI: 10.15584/actaires.2022.3.1

Marcin Burdzik

Uniwersytet Śląski w Katowicach
ORCID: 0000-0001-6607-6663

TAJEMNICA MEDYCZNA I PRAWO DO PRYWATNOŚCI W DOBIE E-ZDROWIA – UWAGI W KONTEKŚCIE SYSTEMU INFORMACJI MEDYCZNEJ

Wprowadzenie

Każdy pacjent ma prawo do zachowania w tajemnicy informacji z nim związanych, a uzyskanych w związku z wykonywaniem zawodu medycznego (art. 13 u.p.p.[1]). Informacje te objęte są tajemnicą medyczną[2] i podlegają ochronie przed nieuprawnionym dostępem do ich treści, co stanowi egzemplifikację konstytucyjnego prawa do prywatności jednostki (art. 47 Konstytucji RP). Korelatem dyskutowanego uprawnienia jest wynikający z art. 14 ust. 1 u.p.p. generalny obowiązek zachowania tajemnicy medycznej[3] przez osoby wykonujące zawody medyczne oraz należyta ochrona dokumentacji medycznej, która stanowi materialny nośnik informacji objętych wyżej wymienioną tajemnicą[4] (art. 23 ust. 2 u.p.p.). Zastrzeżenie to dotyczy dokumentacji medycznej *in genere*, tj. zarówno dokumentacji prowadzonej w formie tradycyjnej (papierowej), jak i w formie elektronicznej oraz elektronicznej dokumentacji medycznej, o której mowa w ustawie

[1] Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. 2022, poz. 1876 ze zm.).

[2] R. Kubiak, *Tajemnica medyczna*, Warszawa 2015, s. 26.

[3] W pewnym uproszczeniu można przyjąć, że tajemnica medyczna stanowi obowiązek zachowania w poufności informacji uzyskanych od pacjenta w związku z wykonywaniem zawodu medycznego. Obowiązek ten ciąży na wszystkich osobach wykonujących zawody medyczne i wynika z art. 14 u.p.p. oraz właściwych przepisów korporacyjnych regulujących zasady wykonywania poszczególnych zawodów medycznych (zob. np. art. 40 ust. 1 ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty, Dz.U. 2022, poz. 1731, dalej: u.z.l.; art. 17 ustawy z dnia 15 lipca 2011 r. o zawodach pielęgniarki i położnej, Dz.U. 2022, poz. 2702). W zakresie szczegółowych rozważań na temat zakresu znaczeniowego pojęcia *tajemnica medyczna* zob. np. R. Kubiak, *Tajemnica medyczna*, s. 26–38; M. Burdzik, *Lekarz w procesie karnym jako gwarant tajemnicy lekarskiej*, Warszawa 2021, s. 65–69.

[4] M. Burdzik, *Lekarz w procesie*…, s. 242.

z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia[5]. Dostęp do tych treści przez podmioty inne niż pacjent powinien mieć każdorazowo charakter ekstraordynaryjny i ściśle ograniczony, a także uzasadniony.

Obecnie dane zawarte w dokumentacji medycznej pacjenta są wykorzystywane do współtworzenia baz danych obsługiwanych za pomocą centralnych systemów teleinformatycznych, takich jak System Informacji Medycznej (SIM). Tego rodzaju rozwiązania niewątpliwe usprawniają przebieg procesu diagnostyczno-terapeutycznego, zapewniając szybki przepływ informacji o stanie zdrowia danej osoby pomiędzy podmiotami udzielającymi świadczeń zdrowotnych. Co jest szczególnie istotne w dobie dynamicznie rozwijającego się e-zdrowia[6].

Warto jednak zauważyć, że ustawodawca przewidział bardzo szeroki i zróżnicowany katalog podmiotów posiadających dostęp do SIM, do którego należą chociażby jednostki samorządu terytorialnego (art. 12 ust. 3–8 u.s.i.). Jednocześnie szczegółowy zakres raportowanych tam danych określany jest za pomocą aktów rangi podstawowej. *De lege lata* informacje dotyczące stanu zdrowia pacjenta są przekazywane do SIM bez wymogu uzyskania zgody tego ostatniego, a nawet gdy pacjent wyraźnie sprzeciwi się ich przekazaniu.

Zachodzi zatem pytanie, czy takie rozwiązania nie czynią z tajemnicy medycznej konstrukcji o charakterze iluzorycznym, a co za tym idzie – czy prawodawca nadal gwarantuje jednostce możliwość rzeczywistej realizacji prawa do prywatności w zakresie danych dotyczących jej stanu zdrowia. Dotyczy to zwłaszcza uprawnienia do zachowania tego rodzaju informacji w stanie wolnym od ingerencji osób trzecich, tj. decydowania o katalogu podmiotów posiadających dostęp do takich danych. Rozstrzygnięcie powyższych dylematów pozostaje zasadniczym celem niniejszego opracowania[7].

Tajemnica medyczna a prawo do prywatności

Z uwagi na intymny, nierzadko subiektywnie wstydliwy charakter informacji przekazywanych przez pacjenta osobom wykonującym zawody medyczne

[5] Dz.U. 2022, poz. 1555 ze zm. (dalej: u.s.i.).

[6] E-zdrowie stanowi wspólną domenę sektorów ochrony zdrowia i nowoczesnych technologii teleinformatycznych, w których technologie ICT służą poprawie dostępności, efektywności i jakości usług sektora ochrony zdrowia. M. Czerwińska, *Specyfika zachowań e-pacjentów w Internecie*, „Roczniki Kolegium Analiz Ekonomicznych" 2015, nr 38, 2015, s. 345. Technologie ICT wykorzystywane są zarówno do udzielania świadczeń zdrowotnych, jak i realizacji praw pacjenta, takich jak prawo do informacji czy prawo dostępu do dokumentacji medycznej. J. Król-Całkowska, *E-dokumentacja medyczna i telemedycyna. Aspekty prawne*, Warszawa 2021, s. 20.

[7] Z uwagi na ograniczone ramy opracowania kwestie dotyczące przetwarzania danych o stanie zdrowia w kontekście RODO oraz ustawy o ochronie danych osobowych nie będą szerzej eksplorowane (z wyjątkiem niezbędnych odesłań). W tym zakresie zob. np. *Ochrona danych medycznych. RODO w ochronie zdrowia*, red. M. Jackowski, Warszawa 2018.

tajemnica medyczna stanowi *conditio sine qua non* efektywnego procesu diagnozy i leczenia. Tylko w warunkach pełnej poufności możliwe jest ujawnienie wszystkich relewantnych wiadomości dotyczących stanu zdrowia pacjenta (np. okoliczności, w jakich doszło do zakażenia daną chorobą). Założenie to odnosi się do każdej gałęzi medycyny.

Ochrona tajemnicy medycznej nie jest możliwa bez równoległej i właściwej ochrony dokumentacji medycznej, w której informacje pozyskane od pacjenta w związku z udzielaniem mu świadczeń zdrowotnych są następnie umieszczane[8]. Pojęcie *dokumentacja medyczna* obejmuje swoim zakresem całokształt dokumentów wytwarzanych przez podmiot udzielający świadczeń zdrowotnych w związku z ich udzielaniem. Szczegółowe zasady prowadzenia dokumentacji, w tym jej udostępniania i przechowywania, określają art. 24–30a u.p.p. oraz właściwe akty wykonawcze[9]. Dokumentacja ta obejmuje zarówno dokumentację indywidualną (dotyczącą poszczególnych pacjentów), jak i dokumentację zbiorczą, dotyczącą ogółu (lub grupy) pacjentów korzystających ze świadczeń zdrowotnych w tym podmiocie (§ 2 Rozp.DM). W obecnym stanie prawnym zasadniczą formą prowadzenia omawianej dokumentacji jest forma elektroniczna (§ 1 ust. 1 Rozp.DM). Forma papierowa jest dopuszczalna wyłącznie, gdy warunki organizacyjno-techniczne uniemożliwiają prowadzenie dokumentacji w postaci elektronicznej lub przepis rozporządzenia tak stanowi (§ 1 ust. 2 Rozp.DM). Niedopuszczalne jest przy tym równoczesne prowadzenie dokumentacji w obu wymienionych formach[10].

Od dokumentacji prowadzonej w formie elektronicznej, o której mowa powyżej, należy odróżnić elektroniczną dokumentacje medyczną (EDM). Chociaż nazwy te są bardzo zbliżone, a w języku powszechnym często stosowane za-

[8] Zgodnie z § 4 ust. 1 rozporządzenia Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. 2022, poz. 1304; dalej Rozp.DM) wpisów w dokumentacji medycznej dokonuje się niezwłocznie po udzieleniu świadczenia zdrowotnego z zapewnieniem niezaprzeczalności i integralności danych, a w dokumentacji w postaci papierowej – w sposób czytelny i w porządku chronologicznym. Wpisy i zmiany wpisów opatruje się oznaczeniem osoby, która ich dokonała (§ 4 ust. 2 Rozp.DM) oraz podpisuje zależnie od formy tej dokumentacji (§ 4 ust. 3–5).

[9] Obecnie materię tę regulują: Rozp.DM, a także rozporządzenie Ministra Obrony Narodowej z dnia 6 sierpnia 2021 r. w sprawie rodzajów, zakresu i wzorów oraz sposobu przetwarzania dokumentacji medycznej w podmiotach leczniczych utworzonych przez Ministra Obrony Narodowej (Dz.U. 2021, poz. 1825) oraz rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów oraz sposobu przetwarzania dokumentacji medycznej w podmiotach leczniczych utworzonych przez ministra właściwego do spraw wewnętrznych (Dz.U. 2022, poz. 1957).

[10] Rozwiązanie to ma zapobiegać powielaniu dokumentacji medycznej, a w efekcie przechowywaniu zdublowanych danych o pacjencie w dwóch formach. M.E. Kowalska, S. Jakubowski, A. Romaszewski, *Pacjent i jego dane – część 1 – prawo do danych o stanie zdrowia w aspekcie wdrażania planowanych rozwiązań dokumentacji medycznej w postaci elektronicznej i RODO*, „Zeszyt Naukowy Zarządzania i Bankowości w Krakowie" 2019, nr 53, s. 26.

miennie, to w płaszczyźnie normatywnej posiadają inny zakres znaczeniowy. Pojęcie EDM zostało zdefiniowane na gruncie art. 2 pkt 6 u.s.i. Zgodnie z treścią przywołanego przepisu elektroniczną dokumentację medyczną stanowią wyłącznie enumeratywnie wyliczone dokumenty, tj.:

- e-recepty,
- e-skierowania[11],
- e-zlecenia[12],
- Karty Szczepień,

oraz elementy wskazane w Rozp.EDM[13] wydanym na podstawie art. 13a u.s.i., tj.:

- karty informacyjne z leczenia szpitalnego,
- wyniki badań laboratoryjnych wraz z ich opisem,
- opis innych badań diagnostycznych,
- informacje przekazywane pacjentowi w razie odmowy przyjęcia do szpitala[14],
- informacje dla lekarza kierującego świadczeniobiorcę do poradni specjalistycznej lub leczenia szpitalnego[15],

wytworzone w postaci elektronicznej w standardzie HL7CDA[16] oraz opatrzone jednym ze wskazanych w wyżej wymienionym przepisie podpisów elektronicznych[17]. EDM zawsze dotyczy więc konkretnego pacjenta i wytwarzana jest pierwotnie w postaci elektronicznej. Obowiązek prowadzenia EDM przez podmioty lecznicze został wprowadzony z 1 stycznia 2019 r.[18] Natomiast 1 lipca 2021 r.

[11] Skierowania określone w rozporządzeniu Ministra Zdrowia z dnia 15 kwietnia 2019 r. w sprawie skierowań wystawianych w postaci elektronicznej w Systemie Informacji Medycznej (Dz.U. 2022, poz. 1417).

[12] Zlecenia na zaopatrzenie i zlecenia naprawy, o których mowa w art. 38 ust. 4a ustawy z dnia 12 maja 2011 r. o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych (Dz.U. 2022, poz. 2555).

[13] Rozporządzenie Ministra Zdrowia z dnia 8 maja 2018 r. w sprawie rodzajów elektronicznej dokumentacji medycznej (Dz.U. 2021, poz. 1153), dalej: Rozp.EDM.

[14] Informacje o rozpoznaniu choroby, problemu zdrowotnego lub urazu, wynikach przeprowadzonych badań, przyczynie odmowy przyjęcia do szpitala, udzielonych świadczeniach zdrowotnych oraz ewentualnych zaleceniach.

[15] Informacje o rozpoznaniu, sposobie leczenia, rokowaniu, ordynowanych lekach, środkach spożywczych specjalnego przeznaczenia żywieniowego i wyrobach medycznych, w tym okresie ich stosowania i sposobie dawkowania, oraz wyznaczonych wizytach kontrolnych.

[16] Zob. Ministerstwo Zdrowia, *Odpowiedź na pisma NRL dot. obowiązku wymiany elektronicznej dokumentacji medycznej (EDM) z 19 maja 2021 r.*, DIeZ.541.264.2021.MD, https://nil.org.pl/uploaded_files/art_1 621576369_210520-mz-nrl-wymianaedm-odp.pdf (25.03.2022), s. 5.

[17] Kwalifikowanym podpisem elektronicznym, podpisem zaufanym, podpisem osobistym albo z wykorzystaniem sposobu potwierdzania pochodzenia oraz integralności danych dostępnego w systemie teleinformatycznym udostępnionym bezpłatnie przez Zakład Ubezpieczeń Społecznych.

[18] Zgodnie z art. 56 ust. 1 u.s.i. dokumentacja medyczna określona w rozporządzeniu Ministra Zdrowia z dnia 8 maja 2018 r. w sprawie rodzajów elektronicznej dokumentacji medycznej mogła być prowadzona w postaci papierowej do 31 grudnia 2018 r.

wszedł w życie obowiązek wymiany danych zawartych EDM za pośrednictwem Systemu Informacji Medycznej (art. 56 ust. 4 u.s.i.). Nie ulega zatem wątpliwości, że EDM ma stanowić podstawowy nośnik danych i informacji na temat stanu zdrowia pacjentów[19], które można będzie sprawnie przekazywać za pomocą dedykowanych systemów teleinformatycznych pomiędzy jednostkami systemu ochrony zdrowia w celu poprawy jakości i dostępności świadczonych usług.

Właściwa ochrona informacji objętych tajemnicą medyczną, w tym ochrona dokumentacji medycznej, to immamentne narzędzia realizacji konstytucyjnego prawa jednostki do prywatności[20] w każdej sytuacji, w której ta jednostka staje się pacjentem. Informacje związane ze stanem zdrowia wchodzą bowiem w obszar „życia prywatnego" każdego człowieka i jako takie podlegają ochronie na gruncie art. 47 Konstytucji RP[21] oraz aktów prawa międzynarodowego[22]. Warto podkreślić, że w każdym przypadku prawo do prywatności powinno gwarantować jednostce swego rodzaju „stan niezależności" uprawniający ją do autonomicznego decydowania o zakresie informacji na temat własnej osoby, które mogą zostać ujawnione innym podmiotom[23].

System Informacji Medycznej – zakres przetwarzanych danych

SIM jest systemem teleinformatycznym, który służy przetwarzaniu danych dotyczących udzielonych, udzielanych i planowanych świadczeń opieki zdrowotnej. Dane te są udostępniane przez systemy teleinformatyczne usługodawców[24] (art. 10 ust. 1 u.s.i.) oraz pozyskiwane z właściwych dziedzinowych systemów teleinformatycznych (art. 10 ust. 3–6b u.s.i.). Ustawa przewiduje bardzo szeroki zakres danych przetwarzanych w ramach SIM, który obejmuje obecnie:

[19] K. Biczysko-Pudełko, *Prawne aspekty wykorzystania technologii cloud computing w sektorze opieki zdrowotnej*, „Prawo Mediów Elektronicznych" 2020, nr 3, s. 15.

[20] M. Jabłońska, *Tajemnica medyczna a prawo osoby bliskiej pacjenta do informacji medycznej – przyczynek do dyskusji*, „Białostockie Studia Prawnicze" 2020, nr 2(25), s. 277.

[21] Wyrok TK z dnia 11 października 2011 r., sygn. K 16/10, Lex nr 992832.

[22] Prawo do prywatności zostało zagwarantowane także w art. 8 ust. 1 Europejskiej Konwencji Praw Człowieka, art. 7 ust. 1 Karty Praw Podstawowych Unii Europejskiej czy art. 17 ust. 1 Międzynarodowego Paktu Praw Obywatelskich i Politycznych.

[23] Tak słusznie: A. Mednis, *Prawo do prywatności a interes publiczny*, Kraków 2006, s. 68.

[24] Usługodawcami są podmioty wykonujące działalność leczniczą w rozumieniu przepisów o działalności leczniczej (zob. szerzej: P. Lenio, *Publicznoprawne źródła finansowania ochrony zdrowia*, Warszawa 2018, Lex/el., rozdz. 4.1.2), osoby fizyczne posiadające fachowe uprawnienia do udzielania świadczeń zdrowotnych, które udzielają ich w ramach wykonywanej działalności gospodarczej, podmioty realizujące czynności z zakresu zaopatrzenia w wyroby medyczne oraz podmioty udzielające opieki farmaceutycznej – art. 2 pkt 15 u.s.i. w zw. z art. 5 pkt 41 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz.U. 2022, poz. 2561), dalej: u.ś.o.z.

- dane osobowe[25] i jednostkowe dane medyczne o usługobiorcach[26],
- imiona i nazwiska oraz numery PESEL przedstawicieli ustawowych, opiekunów prawnych, pełnomocników oraz opiekunów faktycznych usługobiorców w rozumieniu u.p.p.,
- dane o usługodawcach, pracownikach medycznych i podmiotach, o których mowa w art. 31b ust. 1 u.s.i. (tzw. asystentach medycznych),
- dane o płatnikach, tj. podmiotach finansujących lub współfinansujący udzielenie świadczenia opieki zdrowotnej,
- dane dotyczące udzielonych świadczeń opieki zdrowotnej finansowanych lub współfinansowanych ze środków publicznych oraz kwoty środków publicznych wydatkowanych na sfinansowanie tych świadczeń,
- dane umożliwiające wymianę dokumentów elektronicznych pomiędzy usługodawcami oraz usługodawcami a płatnikami,
- dane dotyczące produktów leczniczych.

Ponadto zgodnie z art. 11 ust. 3 u.s.i. każdy usługodawca ma obowiązek przekazywania do SIM danych zdarzenia medycznego (tj. danych na temat udzielonego świadczenia zdrowotnego[27]). Celem tego rozwiązania jest umożliwienie innym usługodawcom pobrania danych osobowych lub jednostkowych danych medycznych pacjenta zawartych zarówno w EDM, jak i w dokumentacji medycznej, o której mowa w u.p.p. (tj. dokumentacji medycznej prowadzonej w formie elektronicznej zgodnie z wymogami Rozp.DM), w zakresie niezbędnym do prowadzenia diagnostyki lub zapewnienia ciągłości leczenia[28].

Ustawodawca określił ogólny katalog danych identyfikujących zdarzenie medyczne, jakie należy przekazać do SIM (art. 11 ust. 4 u.s.i.), stanowiąc jednocześnie, że szczegółowy zakres danych, sposób oraz termin ich przekazania będzie określany w aktach wykonawczych wydawanych w oparciu o delegację ustawową z art. 11 ust. 4a u.s.i. Obecnie kwestie te reguluje rozporządzenie Ministra Zdrowia z dnia 26 czerwca 2020 r.[29] Zgodnie z tym ostatnim do SIM należy

[25] W tym m.in.: imię (imiona), nazwisko, nazwisko rodowe, płeć, obywatelstwo, wykształcenie, numer PESEL, serię i numer dowodu osobistego lub paszportu oraz datę ważności tych dokumentów, datę urodzenia, adres miejsca zamieszkania (w przypadku braku – adres miejsca pobytu), adres do korespondencji, adres zameldowania, numer telefonu kontaktowego, NIP.

[26] Usługobiorcą jest osoba fizyczna korzystająca lub uprawniona do korzystania ze świadczeń opieki zdrowotnej w rozumieniu u.ś.o.z. W pewnym uproszczeniu można więc przyjąć, że usługobiorca jest pacjentem w rozumieniu powszechnie przyjętym, toteż na gruncie niniejszego opracowania pojęcia te jako tożsame będą stosowne zamiennie. Zob. szerzej na temat wykładni pojęcia *pacjent* np. M. Burdzik, *Lekarz w procesie*…, s. 86–93.

[27] Każde działanie służące profilaktyce, zachowaniu, ratowaniu, przywracaniu lub poprawie zdrowia oraz inne działanie medyczne wynikające z procesu leczenia lub przepisów odrębnych regulujących zasady ich udzielania (art. 5 pkt 4 u.ś.o.z.).

[28] Dane te są też udostępniane Narodowemu Funduszowi Zdrowia w celu rozliczania świadczeń opieki zdrowotnej.

[29] Rozporządzenie w sprawie szczegółowego zakresu danych zdarzenia medycznego przetwarzanego w systemie informacji oraz sposobu i terminów przekazywania tych danych do Systemu Informacji Medycznej (Dz.U. 2020, poz. 1253), dalej: Rozp.SIM.

raportować m.in. informacje na temat stawianych pacjentowi rozpoznań (głównych i współistniejących)[30] będących przyczyną udzielenia danego świadczenia (§ 2 ust. 1 pkt 3 lit. e Rozp.SIM) czy dane pozwalające zidentyfikować dokumentację medyczną prowadzoną w postaci elektronicznej[31].

W ramach wymiany EDM do SIM przekazywana jest obligatoryjnie także karta informacyjna z leczenia szpitalnego pacjenta[32] (art. 11 ust. 2 u.s.i. w zw. z § 1 pkt 3 Rozp.EDM). Co prawda Rozp.EDM nie określa jej elementów obowiązkowych, niemniej kwestię tę reguluje Rozp.DM, zgodnie z którym karta informacyjna powinna zawierać m.in.: informacje dotyczące stanu zdrowia (lub stanu funkcjonowania) pacjenta oraz procesu diagnostycznego, leczniczego, pielęgnacyjnego lub rehabilitacji, a także wspomniane już rozpoznania chorobowe (§ 21 ust. 4 Rozp.DM). Omawiany dokument stanowi więc ważne i kompleksowe źródło informacji na temat przeprowadzonego procesu diagnostyczno-terapeutycznego, w tym jego efektów i dalszych rokowań, przebiegu samej hospitalizacji czy stanu pacjenta zarówno w momencie przyjęcia do szpitala, jak i w chwili wypisu. Należy pamiętać, że w pewnych sytuacjach informacje, które zostały zamieszczone w karcie informacyjnej, z uwagi na ich medyczną relewantność mogą mieć dla pacjenta charakter krępujący (subiektywnie wstydliwy)[33]. Obawy związane z obecnością tych danych w SIM mogą prowadzić do oporu przed ich ujawnieniem osobie udzielającej świadczeń zdrowotnych. Skutkiem takiej postawy będzie więc ograniczenie wiedzy na temat pacjenta rzutujące negatywnie na proces diagnozy i leczenia.

Zgoda pacjenta na dostęp do danych zawartych w SIM

Ustawa o systemie informacji w ochronie zdrowia przyznaje pacjentowi pewne uprawnienia, które pozwalają mu w określonym zakresie limitować krąg podmiotów posiadających dostęp do danych na temat jego stanu zdrowia prze-

[30] Według obowiązującej w Polsce Międzynarodowej Statystycznej Klasyfikacji Chorób i Problemów Zdrowotnych Rewizja Dziesiąta (ICD-10). Dla porządku wskazać należy, że od 1 stycznia 2022 r. formalnie obowiązuje kolejna wersja tej klasyfikacji (tj. ICD-11). Proces transformacji nie został jeszcze przeprowadzony, toteż polski system ochrony zdrowia w praktyce nadal posługuje się klasyfikacją ICD-10.

[31] M.in. jej identyfikator nadany w systemie usługodawcy, datę wytworzenia, tryb udostępnienia czy adres repozytorium, w którym jest przechowywana (§ 2 ust. 1 pkt 6 Rozp.SIM).

[32] W języku powszechnym kartę informacyjną określa się często mianem „karty wypisowej" lub „wypisu". Zob. np. https://sjp.pwn.pl/sjp/wypis;2540156.html (28.03.2022).

[33] Np. w karcie informacyjnej z leczenia w szpitalu psychiatrycznym mogą się znaleźć informacje o poprzedzającej hospitalizację próbie samobójczej, zachowaniach agresywnych podejmowanych pod wpływem doznań psychotycznych czy utracie zahamowań społecznych (w tym seksualnych) w przebiegu epizodu maniakalnego. Na ten temat zob. np. P. Gałecki, A. Szulc, *Psychiatria*, Wrocław 2018, s. 191 i n.

twarzanych za pośrednictwem SIM. Zasadnicze znaczenie w tej materii mają rozwiązania przewidziane w art. 35 ust. 1 i 1a u.s.i. Zgodnie z nimi pełen dostęp do danych przetwarzanych w SIM niezależnie od zgody pacjenta przysługuje:

- lekarzowi, pielęgniarce oraz położnej, którzy udzielają świadczeń z zakresu podstawowej opieki zdrowotnej[34] (art. 35 ust. 1 pkt 3 u.s.i.),
- pracownikowi medycznemu, który wytworzył EDM pacjenta lub wykonuje zawód u usługodawcy, u którego EDM została wytworzona, jeżeli jest to niezbędne do prowadzenia diagnostyki lub zapewnienia ciągłości leczenia (art. 35 ust. 1 pkt 1 i 2 u.s.i.).

Dodatkowo w sytuacji zagrożenia życia pacjenta dostęp ten przysługuje każdemu pracownikowi medycznemu, niezależnie od charakteru czy trybu udzielanych świadczeń zdrowotnych (art. 35 ust. 1 pkt 4 u.s.i). Dostęp do jednostkowych danych medycznych został przyznany również podmiotom finansującym lub współfinansującym udzielenie świadczenia opieki zdrowotnej pod warunkiem, że udostępnienie tych danych jest związane z wykonywaniem zadań określonych w art. 11 ust. 1 oraz art. 12 ust. 1 pkt 1–4, 6 i 8 u.ś.o.z. W takim przypadku nieudzielenie zgody przez pacjenta pozostaje prawnie irrelewantne (art. 35 ust. 4 u.s.i.).

W innych niż opisane powyżej przypadkach zgodnie z art. 35 ust. 1a u.s.i. udostępnienie danych z SIM wymaga każdorazowo zgody pacjenta lub jego przedstawiciela ustawowego. Wyrażenie zgody następuje za pośrednictwem Internetowego Konta Pacjenta (art. 7a ust.1 pkt 3 u.s.i.). Oznacza to m.in., że dostępu do danych zawartych w SIM nie otrzymują *ex lege* lekarze specjaliści oraz inne podmioty, które udzielają świadczeń specjalistycznych[35], także w zakresie leczenia szpitalnego. Wyrażając zgodę, pacjent określa zakres czasowy i przedmiotowy, w jakim dane dotyczące jego stanu zdrowia zostaną udostępnione (art. 35 ust. 1a zd. 2 u.s.i.). Zgoda ta może zostać cofnięta w każdym czasie (*arg. ex* art. 7a ust. 1 pkt 3 u.s.i.).

Zagrożenia związane z Systemem Informacji Medycznej w kontekście prawa do prywatności pacjenta

Stosowanie nowoczesnych technologii teleinformatycznych w sektorze ochrony zdrowia jest zjawiskiem niewątpliwie korzystnym, zwłaszcza z punktu widzenia poprawy dostępności i jakości świadczonych usług (w tym przepływu informacji)[36].

[34] W rozumieniu art. 2 ustawy z dnia 27 października 2017 r. o podstawowej opiece zdrowotnej (Dz.U. 2022, poz. 2527).

[35] Świadczeniem specjalistycznym jest każde świadczenie opieki zdrowotnej we wszystkich dziedzinach medycyny z wyłączeniem świadczeń udzielanych w zakresie podstawowej opieki zdrowotnej (art. 5 pkt 36 u.ś.o.z.).

[36] Stanowiska dotyczące korzystnych aspektów rozwoju technologii teleinformatycznych w sektorze ochrony zdrowia w zakresie dotyczącym cyfryzacji danych były niejednokrotnie prezentowane w doktrynie. Zob. np. D.M. Szymczyk, A. Horoch, *Implementacja elektronicznej do-*

Nie można jednak pomijać potencjalnych zagrożeń związanych z procesem powszechnej cyfryzacji informacji objętych tajemnicą medyczną i transferu tychże do ogólnokrajowych baz danych. Co prawda ustawodawca przewidział liczne wymogi, jakie muszą być spełnione przez systemy teleinformatyczne[37], w których przetwarzane są dane o stanie zdrowia pacjentów. Niemniej nawet przy zastosowaniu najwyższych standardów bezpieczeństwa nie da się całkowicie wyeliminować ryzyka związanego z przetwarzaniem tych danych w tzw. cyberprzestrzeni[38]. Dotyczy to zwłaszcza prób uzyskania nieautoryzowanego dostępu do ich treści czy następczego ujawnienia (upublicznienia) tak pozyskanych informacji[39]. Z uwagi na wysoką sensytywność danych medycznych mogę one zostać wykorzystane również do naruszenia dóbr osobistych (art. 23 k.c.), zniesławienia czy znieważenia (art. 212 i 216 k.k.) osoby, której dotyczą[40], a także popełnienia innych czynów zabronionych na jej szkodę[41]. Powyższe zastrzeżenia nie kwestionują ogólnej zasadności dalszego rozwoju systemów teleinformatycznych w sektorze ochrony zdrowia, kładą jedynie nacisk na priorytet ochrony przetwarzanych tam danych.

Należy jednak pamiętać, że dyskutowane rozwiązania pozbawiają pacjenta tej części prawa do prywatności, która pozwala na decydowanie o zachowaniu w poufności informacji na temat własnego stanu zdrowia. Konieczne jest zatem istnienie odpowiednich regulacji prawnych, które ograniczą stopień ingerencji w omawianą tu sferę prywatności do niezbędnego minimum – zarówno w aspekcie

kumentacji medycznej. Część 2 – korzyści dla uczestników systemu ochrony zdrowia, „Medycyna Ogólna i Nauki o Zdrowiu" 2013, nr 3(19), s. 325; A. Klich, *Wybrane zagadnienia prawne elektronicznej dokumentacji medycznej*, „Ekonomiczne Problemy Usług" 2017, nr 1, s. 354–355.

[37] Zob. np. art. 8 ust. 1, art. 8b, art. 9a czy art. 37 i n. u.s.i., a także wymogi dotyczące systemów teleinformatycznych, w których prowadzona jest dokumentacja medyczna usługodawców (§ 1 ust. 5–6 Rozp.DM). Na poziomie prawa unijnego kwestię tę reguluje m.in. tzw. dyrektywa NIS, tj. dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii. Jej implementacja do polskiego porządku prawnego została dokonana poprzez wprowadzenie ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2020, poz. 1369). Zgodnie z art. 41 pkt 5 tejże organem właściwym do spraw cyberbezpieczeństwa dla sektora ochrony zdrowia jest minister właściwy ds. zdrowia.

[38] Tak słusznie: K. Konopka, *Ochrona tajemnicy medycznej w e-zdrowiu*, „Białostockie Studia Prawnicze" 2020, nr 2, s. 251.

[39] Oczywiście ryzyko to występuje też w przypadku dokumentacji medycznej prowadzonej w formie tradycyjnej (papierowej). Niemniej w tej sytuacji nieuprawniona ingerencja wymaga osobistej „styczności" z dokumentacją, tj. przebywania w miejscu, w którym jest ona przechowywana. Natomiast próby uzyskania dostępu do dokumentacji elektronicznej mogą być przeprowadzane zasadniczo z dowolnego miejsca na świecie, a także z wielu miejsc jednocześnie.

[40] Dane te mogą być wykorzystywane również w celach marketingowych (np. w procesie profilowania, oferowania produktów dedykowanych), a także przez podmioty świadczące usługi ubezpieczeniowe czy potencjalnych pracodawców. K. Konopka, *Ochrona tajemnicy*…, s. 248.

[41] Np. poprzez wykorzystanie newralgicznych informacji o stanie zdrowia jednostki w celu wymuszenia jej określonego zachowania – działania, zaniechania bądź znoszenia (art. 191 § 1 k.k.).

przedmiotowym (zakres raportowanych danych), jak i podmiotowym (zakres podmiotów posiadających dostęp do tych danych)[42]. Niektóre regulacje u.s.i. wydają się nie spełniać powyższego postulatu.

W pierwszej kolejności zastrzeżenia budzi rozwiązanie przyjęte na gruncie art. 11 ust. 4a u.s.i., które uprawnia ministra właściwego ds. zdrowia do decydowania o zakresie danych raportowanych do SIM w drodze aktu rangi podustawowej. Takie rozwiązanie sprawia, że minister w formie *de facto* jednoosobowej decyzji może dowolnie zmodyfikować katalog tych danych, np. znacznie go rozszerzając[43]. Jak wspomniano, ustawodawca co prawda określił pewne ramy tego katalogu, tworząc ogólny wykaz danych raportowanych do SIM (art. 11 ust. 4 u.s.i.), który rozporządzenie ma jedynie precyzować. Rozwiązanie to nie niweluje jednak ryzyka wspomnianej arbitralności z dwóch powodów. Po pierwsze, danymi na temat zdarzenia medycznego przetwarzanymi w SIM są także „inne dane pozwalające na identyfikację zdarzenia medycznego" (art. 11 ust. 4 pkt 7), co sprawia, że katalog ten ma charakter otwarty. Po drugie, pozostałe kategorie danych identyfikujących zdarzenie medyczne (pkt 1–6) również zostały określone w sposób bardzo ogólny, co stwarza potencjalną możliwość ich szerokiej interpretacji z zastosowaniem wykładni rozszerzającej.

Biorąc pod uwagę charakter informacji o stanie zdrowia, które przetwarzane są w ramach SIM, oraz wymogi wynikające z RODO czy konstytucyjnej zasady proporcjonalności (art. 31 ust. 3 Konstytucji RP), przyjąć należy, że określenie tego katalogu powinno bezwzględnie pozostać domeną ustawodawcy. Nie jest to

[42] Zastrzeżenie to pozostaje w pełni uzasadnione w świetle konstytucyjnej zasady proporcjonalności (art. 31 ust. 3 Konstytucji RP) oraz wynikającego z niej zakazu nadmiernej ingerencji w podstawowe prawa i wolności obywatelskie. L. Garlicki, *Polskie prawo konstytucyjne*, Warszawa 2014, s. 103.

[43] Tytułem przykładu warto wskazać na rozporządzenie Ministra Zdrowia z dnia 3 czerwca 2022 r. zmieniające rozporządzenie w sprawie szczegółowego zakresu danych zdarzenia medycznego przetwarzanego w systemie informacji oraz sposobu i terminów przekazywania tych danych do Systemu Informacji Medycznej (Dz.U. 2022, poz. 1296). Na podstawie tego rozporządzenia obecnie do SIM należy raportować również informacje o ciąży pacjentki czy informacje o wyrobach medycznych zaimplantowanych u pacjenta, o ile usługodawca uzyska je w związku z udzielaniem świadczenia zdrowotnego lub realizacją istotnej procedury medycznej. Warto zaznaczyć, że powyższe rozwiązania wzbudziły spore obawy społeczne już na etapie konsultacji społecznych, zwłaszcza w świetle zaostrzenia prawa aborcyjnego w następstwie wydania wyroku TK z dnia 22 października 2020 r. (sygn. K 1/20, Lex nr 3071397). Obecność danych o ciąży w SIM może okazać się przydana jedynie w sytuacjach, w których pacjentka nie potrafi przekazać informacji o ciąży samodzielnie (np. jest nieprzytomna). W pozostałym zakresie brak jest wyraźnego uzasadnienia dla zamieszczania w systemie tej kategorii danych. Tym bardziej że pytanie o ewentualną ciążę w przypadku badania pacjentki w wieku rozrodczym należy do standardowych elementów lekarskiej anamnezy, niezależnie od specjalizacji. W razie wątpliwości w wyżej wymienionym zakresie możliwe jest zresztą przeprowadzenie odpowiednich badań laboratoryjnych, np. pomiaru stężenia ludzkiej gonadotropiny kosmówkowej (β-HCG) w surowicy, w celu wykluczenia lub potwierdzenia ciąży.

bowiem sprawa czysto techniczna, a kwestia związana z nieodwracalną ingerencją w prawo do prywatności jednostki. Należy przy tym ponownie podkreślić, że decyzja o przekazaniu określonej informacji do SIM jest równoznaczna z utratą prawa zachowania jej w poufności, tj. w stanie wolnym od ingerencji innych podmiotów, przez osobę, której informacja ta bezpośrednio dotyczy.

W dalszej kolejności należy zwrócić uwagę na generalny brak możliwości wyrażenia przez pacjenta skutecznego sprzeciwu wobec transmisji danych dotyczących jego stanu zdrowia do SIM. Obecnie każdy usługodawca (podmiot udzielający świadczeń zdrowotnych) ma generalny obowiązek przekazywania do SIM danych na temat udzielonego świadczenia zdrowotnego (art. 11 ust. 3 u.s.i.). Obowiązek dotyczy zarówno podmiotów udzielających świadczeń w ramach umowy z Narodowym Funduszem Zdrowia, jak i jednostek świadczących usługi prywatne. *De lege lata* transfer danych do SIM nie wymaga zgody pacjenta, gdyż takiego wymogu nie przewiduje analizowany art. 11 ust. 3 u.s.i. ani pozostałe przepisy tej ustawy. Usługodawca ma więc bezwzględny obowiązek przekazania danych o udzielonym świadczeniu zdrowotnym do SIM, nawet jeżeli pacjent jednoznacznie sprzeciwi się ich przekazaniu do tego systemu. Zgodnie z art. 35 ust. 1a u.s.i. pacjent może co prawda nie wyrazić zgody na następcze udostępnienie tych danych określonym podmiotom[44], ale uprawnienie to pozostaje bez wpływu na sam proces transmisji danych do SIM.

Wprowadzenie ogólnego wymogu uzyskania zgody pacjenta na każdorazowe przekazanie danych o udzielonych mu świadczeniach zdrowotnych do SIM nie wydaje się jednak rozwiązaniem właściwym. Taki wymóg mógłby nazbyt ograniczyć rozwój systemów teleinformatycznych, a w pewnym zakresie całkowicie go uniemożliwić. Należy natomiast rozważyć wprowadzenie do ustawy o systemie informacji w ochronie zdrowia instytucji sprzeciwu wobec przekazania do SIM pewnych „szczególnie wrażliwych" kategorii danych. Takie rozwiązanie może być uzasadnione w odniesieniu do informacji o dalece intymnym, a nierzadko wstydliwym charakterze, np. danych związanych ze świadczeniami zdrowotnymi z zakresu seksuologii czy ochrony zdrowia psychicznego (zwłaszcza wobec nadal obecnej w społeczeństwie tendencji do stygmatyzacji osób cierpiących na zaburzenia psychiczne[45]). Instytucja sprzeciwu stanowiłaby rzeczywiste narzędzie ochrony prywatności pacjenta. Sprzeciw pozwalałby bowiem na podjęcie autonomicznej decyzji o zachowaniu wspomnianych kategorii informacji w stanie całkowicie wolnym od ingerencji podmiotów zewnętrznych, tj. utrzymaniu ich poza systemem SIM.

[44] Pacjent może nie wyrazić zgody na udostępnienie danych osobowych i jednostkowych danych medycznych podmiotom innym niż wymienione w art. 35 ust. 1 u.s.i.

[45] Zob. np. M. Babicki, K. Kotowicz, P. Piotrowski i in., *Obszary stygmatyzacji i dyskryminacji osób chorujących psychicznie wśród respondentów internetowych w Polsce*, „Psychiatria Polska" 2018, nr 52(1), s. 93 i n.

Jednocześnie podmiot, który pierwotnie nie wyraził sprzeciwu wobec przekazania dyskutowanych danych do SIM, powinien posiadać przysługujące mu w każdym czasie uprawnienie do żądania ich usunięcia z tego systemu. Aby proponowane rozwiązania nie przekreśliły założeń rozwoju systemów teleinformatycznych wspierających sektor ochrony zdrowia, należałoby precyzyjnie określić przesłanki i zakres ich zastosowania w przepisach u.s.i.

Pewne wątpliwości budzi również rozwiązanie przyjęte na gruncie art. 12 ust. 8 u.s.i. Zgodnie z przywołanym przepisem jednostkom samorządu terytorialnego przysługuje dostęp do danych przetwarzanych w SIM w zakresie zadań wykonywanych przez te podmioty w obszarze zdrowia publicznego[46]. Po pierwsze, ustawodawca przyznał jednostkom samorządu terytorialnego dostęp do danych przetwarzanych w SIM *in genere*, nie zaś, jak ma to miejsce w przypadku wojewodów, do danych zbiorczych (art. 12 ust. 5 u.s.i.). Oznacza to, że jednostce samorządu terytorialnego na podstawie analizowanego tu przepisu przysługuje dostęp zarówno do danych zbiorczych, jak i jednostkowych danych medycznych poszczególnych usługobiorców. Warto przypomnieć, że dostępu do tych danych nie posiadają *ex lege* chociażby lekarze udzielający specjalistycznych świadczeń zdrowotnych (*arg. ex* art. 35 ust. 1a u.s.i), którzy w przeciwieństwie do pracowników jednostek samorządu terytorialnego związani są obowiązkiem zachowania tajemnicy lekarskiej (art. 40 ust. 1 u.z.l.).

Po drugie, zakres zadań jednostek samorządu terytorialnego warunkujący ich dostęp do SIM również został określony w sposób bardzo ogólny (wykonywanie zadań w zakresie zdrowia publicznego). Taka konstrukcja literalna nie pozwala na precyzyjne ustalenie okoliczności, w jakich dostęp ten powinien przysługiwać ani jakie dane obejmować. Konieczność ochrony prawa do prywatności pacjenta prowadzi do wniosku, iż kwestie te powinny zostać jednoznacznie sprecyzowane na poziomie ustawowym, ostatecznie w drodze aktów wykonawczych.

Podsumowanie

Wykorzystywanie nowoczesnych technologii teleinformatycznych w sektorze ochrony zdrowia jest zjawiskiem niewątpliwie korzystnym. Proces ten przyczynia się do poprawy jakości i dostępności usług zdrowotnych. Należy jednak pamiętać, iż dane dotyczące stanu zdrowia jednostki stanowią sferę jej życia prywatnego i jako takie nadal podlegają ochronie w ramach gwarantowanego konstytucyjnie i konwencyjnie prawa do prywatności. Urzeczywistnieniu tego prawa służy obowiązek zachowania tajemnicy medycznej przez osoby wykonujące zawody medyczne oraz właściwa protekcja dokumentacji medycznej.

[46] Zadania te określają właściwe przepisy regulujące zadania samorządu terytorialnego.

Chociaż ustawodawca przewiduje szereg wymogów dla systemów teleinformatycznych, takich jak SIM, w których przetwarzane są dane medyczne, to niektóre rozwiązania normatywne budzą pewne wątpliwości w kontekście nadmiernej ingerencji w prawo do prywatności pacjenta. Nie można też całkowicie zlikwidować ryzyka nieautoryzowanego dostępu do ich treści i ujawnienia tak pozyskanych informacji ze szkodą dla osoby, której dane te bezpośrednio dotyczą.

W obecnym stanie prawnym dane o stanie zdrowia pacjenta oraz udzielonych mu świadczeniach zdrowotnych przekazywane są obligatoryjnie do SIM bez wymogu uzyskania jego zgody w tym zakresie (art. 11 ust. 3 u.s.i.). Przepisy u.s.i. nie przewidują również instytucji sprzeciwu wobec takiego przekazania. Całkowite pozbawienie pacjenta autonomii decyzyjnej istotnie ogranicza jego prawo do prywatności w zakresie wyżej wymienionych danych i czyni z tajemnicy medycznej instytucję o charakterze częściowo iluzorycznym. Informacje przekazane osobie wykonującej zawód medyczny z zamiarem zachowania ich w stanie wolnym od ingerencji osób trzecich zostają bowiem przekazane przez tę osobę do SIM z uwagi na ciążący na niej obowiązek ustawowy, nawet gdy pacjent wyraźnie sprzeciwia się takiemu przekazaniu.

Poważne wątpliwości budzi też rozwiązanie uprawniające ministra właściwego ds. zdrowia do określania szczegółowego katalogu danych raportowanych do SIM w drodze rozporządzenia (art. 11 ust. 4a u.s.i). Ustawowe ramy tego katalogu zostały określone w sposób nazbyt ogólny, co sprawia, że ma on charakter potencjalnie otwarty, a jego poszczególne elementy mogą być interpretowane w sposób rozszerzający. Wątpliwości dotyczą także zakresu uprawnień dostępowych przyznanych jednostkom samorządu terytorialnego (art. 12 ust. 8 u.s.i.).

Z uwagi na rangę prawa do prywatności oraz wysoką sensytywność informacji o stanie zdrowia jednostki zasadne wydaje się wprowadzenie do u.s.i. rozwiązań gwarancyjnych, które wzmocnią rzeczywistą ochronę jednostkowych danych medycznych. *De lege ferenda* zmiany powinny obejmować wprowadzenie do u.s.i. instytucji sprzeciwu wobec przekazania do SIM pewnych szczególnie wrażliwych informacji (np. dotyczących świadczeń zdrowotnych z zakresu ochrony zdrowia psychicznego). Osobie, która pierwotnie nie wyraziła sprzeciwu, powinno także przysługiwać prawo żądania usunięcia tych danych z systemu w późniejszym terminie. Aby uniknąć zbędnych nadużyć, zakres przedmiotowy, podmiotowy oraz temporalny dyskutowanej instytucji należałoby w takim przypadku precyzyjnie określić w przepisach ustawy.

Ustalenie katalogu danych raportowanych do SIM przez usługodawców powinno pozostać bezwzględną domeną ustawodawcy. Z tego względu należy zlikwidować kompetencję ministra właściwego ds. zdrowia pozwalającą mu modyfikować wyżej wymieniony katalog w drodze rozporządzenia (art. 11 ust. 4a). Każdorazowe rozszerzenie tego katalogu stanowi bowiem ingerencję w prawo do prywatności jednostki i z tego względu musi uwzględniać wymogi wynikają-

ce z art. 31 ust. 3 Konstytucji RP[47]. Zasadne wydaje się też zrewidowanie i dookreślenie zakresu uprawnień dostępowych do SIM przysługujących jednostkom samorządu terytorialnego.

Są to jedynie przykładowe propozycje zmian w dyskutowanym obszarze, które mogą stanowić asumpt do dalszej dyskusji nad przedstawionym zagadnieniem.

Bibliografia

Babicki M., Kotowicz K., Piotrowski P. i in., *Obszary stygmatyzacji i dyskryminacji osób chorujących psychicznie wśród respondentów internetowych w Polsce*, „Psychiatria Polska" 2018, nr 52(1).

Biczysko-Pudełko K., *Prawne aspekty wykorzystania technologii cloud computing w sektorze opieki zdrowotnej*, „Prawo Mediów Elektronicznych" 2020, nr 3.

Burdzik M., *Lekarz w procesie karnym jako gwarant tajemnicy lekarskiej*, Warszawa 2021.

Czerwińska M., *Specyfika zachowań e-pacjentów w Internecie*, „Roczniki Kolegium Analiz Ekonomicznych" 2015, nr 38.

Gałecki P., Szulc A., *Psychiatria*, Wrocław 2018.

Garlicki L., *Polskie prawo konstytucyjne*, Warszawa 2014.

Jabłońska M., *Tajemnica medyczna a prawo osoby bliskiej pacjenta do informacji medycznej – przyczynek do dyskusji*, „Białostockie Studia Prawnicze" 2010, nr 2.

Klich A., *Wybrane zagadnienia prawne elektronicznej dokumentacji medycznej*, „Ekonomiczne Problemy Usług" 2017, nr 1.

Konopka K., *Ochrona tajemnicy medycznej w e-zdrowiu*, „Białostockie Studia Prawnicze" 2020, nr 2.

Kowalska M.E., Jakubowski S., Romaszewski A., *Pacjent i jego dane – część 1 – prawo do danych o stanie zdrowia w aspekcie wdrażania planowanych rozwiązań dokumentacji medycznej w postaci elektronicznej i RODO*, „Zeszyt Naukowy Zarządzania i Bankowości w Krakowie" 2019, nr 53.

Król-Całkowska J., *E-dokumentacja medyczna i telemedycyna. Aspekty prawne*, Warszawa 2021.

Kubiak R., *Tajemnica medyczna*, Warszawa 2015.

Lenio P., *Publicznoprawne źródła finansowania ochrony zdrowia*, Warszawa 2018.

Łakomiec K., *Konstytucyjna ochrona prywatności. Dane dotyczące zdrowia*, Warszawa 2020.

Mednis A., *Prawo do prywatności a interes publiczny*, Kraków 2006

Ochrona danych medycznych. RODO w ochronie zdrowia, red. M. Jackowski, Warszawa 2018.

Szymczyk D.M., Horoch A., *Implementacja elektronicznej dokumentacji medycznej. Część 2 – korzyści dla uczestników systemu ochrony zdrowia*, „Medycyna Ogólna i Nauki o Zdrowiu" 2013, nr 3(19).

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

Streszczenie

Rozwój nowoczesnych technologii teleinformatycznych oraz ich wykorzystanie w sektorze ochrony zdrowia to zjawiska, które przyczyniają się do poprawy jakości i dostępności usług zdrowotnych. Przejawem tego rodzaju rozwiązań jest System Informacji Medycznej (SIM), w którym gromadzone są informacje o udzielanych świadczeniach zdrowotnych. Obecnie dane te przekazy-

[47] Tj. m.in. zasadę wyłączności ustawy dla ustanawiania ograniczeń w zakresie konstytucyjnych wolności i praw jednostki.

wane są do SIM bez konieczności uzyskania zgody pacjenta, a nawet gdy ten wyraźnie sprzeciwia się temu. Jednocześnie informacje o stanie zdrowia podlegają ochronie w ramach konstytucyjnego prawa do prywatności, które uprawnia jednostkę do zachowania ich w poufności. Ich ochronie w tym zakresie służy tajemnica medyczna oraz właściwe zabezpieczenie dokumentacji medycznej. Zachodzi zatem pytanie, czy takie rozwiązania jak SIM nie ingerują nadmiernie w prawo do prywatności, a co za tym idzie – czy nie czynią z tajemnicy medycznej instytucji o charakterze iluzorycznym. Celem artykułu jest rozstrzygnięcie powyższych dylematów.

Słowa kluczowe: prawo do prywatności, elektroniczna dokumentacja medyczna, system informacji medycznej, tajemnica medyczna, e-zdrowie

MEDICAL SECRECY AND THE RIGHT TO PRIVACY IN THE ERA OF E-HEALTH – COMMENTS IN THE CONTEXT OF THE MEDICAL INFORMATION SYSTEM

Summary

The development of modern ICT technologies and their use in the health care sector are phenomena that contribute to improving the quality and availability of health services. This type of solution is the Medical Information System (SIM), which collects information on health services provided. Currently, these data are transferred to SIM without obtaining the patient's prior consent, and even if the patient expressly opposes their transfer. At the same time, health information is protected under the constitutional right to privacy, which entitles the individual to keep this information confidential. Their protection in this respect is ensured by medical confidentiality and proper securing of medical records. Therefore, the question arises whether solutions such as SIM do not excessively interfere with the right to privacy and thus make medical secrecy an institution of an illusory nature. The article aims to resolve the above dilemmas.

Keywords: the right to privacy, electronic medical records, medical information system, medical confidentiality, e-health