Fides, Ratio et Patria. Studia Toruńskie 19/2023
ISSN 2392-1463; e-ISSN 2956-3267
s. 139-152

https://doi.org/10.56583/frp.2550

Iwona Nowakowska[*]

Akademia Kultury Społecznej i Medialnej w Toruniu
https://orcid.org/0009-0006-3109-9439

Joanna Zdanowska[**]

Uniwersytet Zielonogórski
https://orcid.org/0000-0001-7921-8974

Obowiązek zachowania tajemnicy medycznej w dobie rozwoju nowoczesnych technologii

Streszczenie

Widoczny w ostatnim czasie rozwój technologii spowodował, że w obszarze ochrony zdrowia zaczęto na szeroką skalę wykorzystywać narzędzia informatyczne dające możliwość przetwarzania danych medycznych oraz komunikowania się na odległość. To z kolei ujawniło zagrożenia dla gwarancji zachowania tajemnicy medycznej.

Głównym celem pracy była próbą wskazania współczesnych zagrożeń dla dochowania tajemnicy medycznej wynikających z zastosowania w medycynie nowych technologii. W pierwszej kolejności należy postulować wprowadzenie definicji zawodu medycznego oraz sformułowania katalogu zawodów medycznych, co pozwoli na wyeliminowanie wątpliwości kto jest zobowiązany do dochowania poufności danych objętych tajemnicą medyczną. Nadto należy dookreślić zasady zachowania poufności przez osoby mające dostęp do danych medycznych pacjenta, a nie wykonujących czynności medycznych. Konieczne jest też zapewnienie szerszej ochrony danych o stanie

[*] Iwona Nowakowska – doktor nauk o zdrowiu, inżynier, adiunkt Wydziału Nauk Medycznych i Nauk o Zdrowiu Akademii Kultury Społecznej i Medialnej w Toruniu.

[**] Joanna Zdanowska – doktor nauk o zdrowiu, magister prawa i politologii, adiunkt w Katedrze Prawa Pracy i Postępowania Cywilnego w Instytucie Nauk Prawnych Uniwersytetu Zielonogórskiego.

zdrowia pozyskiwanych w ramach używanych aplikacji mobilnych oraz podniesienie świadomości pracowników placówek medycznych o skali zagrożenia cyberatakami.

Słowa kluczowe: *tajemnica medyczna, zagrożenie, pacjent, dane osobowe*

THE OBLIGATION TO KEEP THE VACCINE SECRET IN THE ERA OF TECHNOLOGICAL DEVELOPMENT

Abstract

Recently, the development of technology has resulted in the widespread use of IT tools in the field of health care that enable the processing of medical data and remote communication. This, in turn, revealed threats to the guarantee of medical confidentiality.

The main aim of the work was an attempt to indicate contemporary threats to maintaining medical confidentiality resulting from the use of new technologies in medicine. First of all, it is necessary to propose the introduction of a definition of the medical profession and the formulation of a catalog of medical professions, which will eliminate doubts as to who is obliged to maintain the confidentiality of data subject to medical secrecy. Moreover, the rules of confidentiality of persons having access to the patient's medical data, but not those performing medical activities, should be specified. It is also necessary to ensure broader protection of health data obtained as part of the mobile applications used and to raise the awareness of employees of medical facilities about the scale of the threat of cyberattacks.

Keywords: *medical confidentiality, threat, patient, personal data*

~ • ~

Wprowadzenie

Osoby udzielające świadczeń zdrowotnych są zobowiązane do zachowania w tajemnicy informacji związanych z pacjentem, uzyskanych w związku z wykonywaniem zawodu. Powinność ta została skonkretyzowana już w przysiędze Hipokratesa[1].

Zasadność wprowadzenia obowiązku tajemnicy jest szeroko argumentowana w doktrynie. Informacje dotyczące stanu zdrowia jednostki należą do sfery prywatności[2], która stanowi jedną z najważniejszych wartości chronionych w de-

[1] Zob. J. Gula, *Hipokrates a przerywanie ciąży,* w: *W imieniu dziecka poczętego*, red. J. W. Gałkowski, J. Gula, Rzym-Lublin 1991, s. 197.

[2] Wyrok Trybunału Konstytucyjnego z dnia 19 maja 1998 r., U 5/97, OTK 1998, nr 4, poz. 46.

mokratycznych państwach. Na gruncie polskim prawo do prywatności stanowi gwarancję konstytucyjną[3]. Trybunał Konstytucyjny uznał, że prywatność należy rozumieć jako prawo do życia własnym życiem, układanym według własnej woli z ograniczeniem do niezbędnego minimum wszelkiej ingerencji zewnętrznej. Odnosi się to między innymi do życia osobistego, w tym zdrowia jednostki[4].

Prywatność jest dobrem osobistym[5] i korzysta z ochrony prawa cywilnego[6]. Prawo do prywatności należy traktować jako uprawnienie każdej osoby do samodzielnego i wyłącznego decydowania o tym, w jakim zakresie chce zachować swą anonimowość, a jakie informacje o niej mogą być udostępniane osobom trzecim[7]. Jak słusznie zauważa Rafał Kubiak jest więc korelatem prawa do zachowania tajemnicy obejmującym również dane medyczne[8].

Ochronę tajemnicy gwarantują również przepisy prawa karnego, w szczególności art. 266 par. 1 Kodeksu karnego[9]. Penalizację naruszenia prawa do prywatności w kontekście przetwarzania danych osobowych przewidziano w ustawie o ochronie danych osobowych[10].

Pomimo istnienia ogólnych unormowań prawnych kwestia tajemnicy medycznej wymagała uszczegółowienia. Z uwagi na jej znaczenie, szczególnie w kontekście zagwarantowania autonomii pacjenta i poszanowania jego prywatności, które stanowią podstawę zaufania do przedstawicieli profesji medycznych, należało wyznaczyć zakres informacji objętych tajemnicą, krąg osób uprawnionych do uzyskania informacji, przypadki legalizujące ujawnienie tajemnicy bez zgody pacjenta oraz sankcje za bezpodstawne ich przekazanie. Powyższe regulacje zostały ujęte w przepisach rangi ustawowej oraz normach deontologicznych.

Obowiązek zachowania w tajemnicy informacji o pacjencie uzyskanych przez osoby w związku z wykonywaniem zawodu medycznego, a w szczególności

[3] Zob. szerzej R. Kubiak, L. Kubicki red., *System prawa medycznego*, t. 1, *Pojęcie, źródła i zakres prawa medycznego*, Warszawa 2018, s. 120-129.

[4] Wyrok Trybunału Konstytucyjnego z dnia 11 października 2011 r., K 16/10, OTK-A 2011, nr 8, poz. 80.

[5] Ustawa z dnia 23.04.1964 r. - Kodeks cywilny, tekst jednolity: Dz. U. z 2019 r. poz. 1145 z późn. zm., art. 23.

[6] Zob. wyrok Sądu Najwyższego z 13 czerwca 1980 r., IV CR 182/80, OSNC 1981, nr 2-3, poz. 30, wyrok Sądu Najwyższego z 26 maja 2017 r., I CSK 557/16, OSNC 2018, nr 3, poz. 33. Na temat prawa do prywatności zob. szerzej: K.W. Kubiński, *Ochrona życia prywatnego człowieka*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 1993, z. 1, s. 61 -72.

[7] Wyrok Sądu Apelacyjnego w Poznaniu z dnia 10 stycznia 2008 r., I ACa 1048/07, niepublikowane.

[8] R. Kubiak, *Tajemnica medyczna*, Warszawa 2015, s. 11.

[9] Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny, tekst jednolity: Dz.U. z 2019 r. poz. 1950 z późn. zm. (dalej K.k.), zob.: A. Zoll, *Ochrona prywatności w prawie karnym*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2000, z. 1, s. 226.

[10] Zob. art. 107 par. 1 i 2 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, tekst jednolity: Dz.U. z 2019 r. poz. 1781.

udzielaniem świadczeń zdrowotnych został zagwarantowany w rozdziale 4 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta[11]. Odpowiednio w ustawach zawodowych nałożono na przedstawicieli zawodów medycznych obowiązek przestrzegania tajemnicy oraz skonkretyzowano jego zasady. Najszerszą regulację zawiera ustawa o zawodzie lekarza i lekarza dentysty[12]. W art. 40 wskazano zakres przedmiotowy i podmiotowy tajemnicy medycznej oraz przypadki wyłączenia obowiązku jej dochowania. Podobne regulacje znajdują zastosowanie do innych grup zawodowych pracowników medycznych – w tym pielęgniarek, położnych, fizjoterapeutów, diagnostów laboratoryjnych oraz ratowników medycznych, co wskazuje na ich uniwersalny charakter.

Szybki rozwój nauki i technologii widoczny w ostatnich latach spowodował, że również w obszarze ochrony zdrowia zaczęto na szeroką skalę wykorzystywać narzędzia informatyczne dające możliwość przetwarzania danych medycznych oraz komunikowania się na odległość. Choć sam trend jest bez wątpienia słuszny i konieczny to należy wziąć pod uwagę, iż rodzi nowe niebezpieczeństwa dla zachowania poufności danych medycznych. Zagwarantowanie tajemnicy jest konieczne nie tylko dla budowania zaufania w relacjach pacjent – lekarz, pacjent – placówka ochrony zdrowia, ale również z uwagi na wymiar komercyjny. Jak słusznie zauważa K. Konopka uzyskanie danych o stanie zdrowia pozwala na profilowane ich wykorzystanie, głównie w sieci internetowej w postaci wyświetlanych reklam czy pozycjonowania stron. Informacje mogą być także wykorzystane przez ubezpieczycieli czy potencjalnych pracodawców[13]. Mogą stanowić też podłoże czynu zabronionego.

Celem pracy jest analiza obecnie obowiązujących regulacji prawnych gwarantujących zachowanie poufności danych objętych tajemnicą medyczną oraz próbą wskazania współczesnych wielopłaszczyznowych zagrożeń mogących utrudniać lub uniemożliwiać dochowanie tajemnicy medycznej wynikających z zastosowania w medycynie nowych technologii.

W pracy wykorzystano metodę dogmatyczną, stąd oparto się na analizie aktualnych przepisów prawa, a nadto dokonano analizy doktryny odnoszącej się do istoty instytucji tajemnicy medycznej, ochrony danych o stanie zdrowia i obecnych zagrożeń wynikających z zastosowania nowych technologii.

[11] Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, tekst jednolity: Dz.U. z 2019 r. poz. 1127 (dalej: u.p.p.).

[12] Ustawa z dnia 5 grudnia 1996 r. o zawodzie lekarza i lekarza dentysty, tekst jednolity: Dz.U. z 2020 r. poz. 514 (dalej: u.z.l.).

[13] K. Konopka, *Ochrona tajemnicy medycznej w e-zdrowiu*, „Białostockie Studia Prawnicze" 2020, vol. 25, nr 2, s. 248.

Pojęcie oraz zakres podmiotowy, przedmiotowy i temporalny tajemnicy medycznej

Tajemnica medyczna jest powinnością nakładającą konieczność zachowania poufności wszystkich informacji dotyczących pacjenta uzyskanych w związku z leczeniem.

Zakres podmiotowy i przedmiotowy ochrony tajemnicy medycznej został wskazany wprost w art. 13 u.p.p., zgodnie z brzmieniem którego „pacjent ma prawo do zachowania w tajemnicy przez osoby wykonujące zawód medyczny, w tym udzielające mu świadczeń zdrowotnych, informacji z nim związanych, a uzyskanych w związku z wykonywaniem zawodu medycznego".

Krąg podmiotów, na których ciąży obowiązek zachowania w tajemnicy informacji o pacjencie został określony szeroko jako wszystkie osoby wykonujące zawód medyczny. Należy zauważyć, że ustawodawca nie zdefiniował pojęcia zawodu medycznego, a jedynie osobę wykonującą zawód medyczny. Legalna definicja takiej osoby została zawarta w art. 2 ust. 1 pkt. 2 ustawy o działalności leczniczej[14]. Do podmiotów tych zalicza się osoby uprawnione na podstawie odrębnych przepisów do udzielania świadczeń zdrowotnych oraz osoby legitymujące się nabyciem fachowych kwalifikacji do udzielania świadczeń zdrowotnych w określonym zakresie lub w określonej dziedzinie medycyny.

W przypadku pierwszej grupy nie budzi wątpliwości, że obowiązek konfidencji obejmuje przedstawicieli tych profesji medycznych, których zasady wykonywania zawodu zostały określone ustawowo. Przykładowo w odniesieniu do lekarzy podstawą prawną jest art. 40 ustawy o zawodzie lekarza i lekarza dentysty. Zgodnie z brzmieniem ust. 1 powinność ta została nałożona na wszystkich lekarzy niezależnie od specjalizacji, miejsca oraz formy wykonywania zawodu. Podobnie obowiązek konfidencji został sformułowany w odniesieniu do m.in. pielęgniarek i położnych, fizjoterapeutów, diagnostów laboratoryjnych, farmaceutów oraz ratowników medycznych.

Obowiązkiem dochowania tajemnicy medycznej zostały również objęte osoby legitymujące się nabyciem fachowych kwalifikacji do udzielania świadczeń zdrowotnych w określonym zakresie lub w określonej dziedzinie medycyny. Należy przez to rozumieć inne niż wyżej wymienione osoby, które w sposób stały i fachowy oraz w celach zarobkowych wykonują zawód związany z medycyną i posiadają do tego odpowiednie kwalifikacje. Jak słusznie wskazuje Rafał Kubiak w praktyce ustalenia w tym zakresie należy dokonywać in casu[15].

[14] Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej, tekst jednolity: Dz.U. z 2020 r. poz. 295.

[15] R. Kubiak, *Prawo medyczne*, Warszawa 2017, s. 219.

W kręgu podmiotów objętych obowiązkiem konfidencji znajdują się również osoby, które na mocy art. 22 ust. 3 u.p.p. uczestniczą przy udzielaniu świadczeń zdrowotnych. Natomiast odmiennie kształtuje się sytuacja osób, które mają dostęp do danych sensytywnych zawartych w dokumentacji medycznej z uwagi na wykonywaną działalność administracyjną lub techniczną jak również osoby uczące się zawodu (studenci). Wobec nich obowiązek konfidencji może być wyprowadzony jedynie z przepisów ogólnych[16]. Należy zdawać sobie jednak sprawę już dziś, że wraz z rozwojem nowoczesnych technologii osób zaangażowanych w szeroko rozumiany proces udzielania świadczeń zdrowotnych będzie coraz więcej. Technologię wykorzystuje się bowiem na kilku obszarach, w tym do kontaktu z pacjentem, udzielania świadczeń zdrowotnych oraz do prowadzenia konkretnych czynności medycznych przy użyciu nowoczesnej aparatury i sprzętu medycznego. W celu sprawnego funkcjonowania wyżej wymienionych zakresów konieczna będzie pomoc i nadzór specjalistów z innych branż niż medyczna. To z kolei będzie się wiązało z koniecznością lub możliwością dostępu tych osób do danych medycznych pacjenta.

Zakres przedmiotowy konfidencji został określony szeroko. Obejmuje on nie tylko dane dotyczące stanu zdrowia pacjenta, ale także wszystkie inne informacje, o których pozyskał wiedzę personel medyczny. Natomiast bez znaczenia pozostaje czy informacje zostały powzięte w sposób zamierzony czy przypadkowo, w sposób legalny czy z naruszeniem przepisów prawa, czy pacjent przekazał je osobiście czy zrobiła to za niego osoba trzecia[17] oraz czy lekarz zdobył je zgodnie z wolą pacjenta czy wbrew jego woli[18]. Nadto nieistotne jest czy pacjent ma świadomość posiadanej o nich wiedzy przez personel medyczny, a także czy w ogóle dane te zna, albo ich istnienia się domyśla[19]. Należy zaznaczyć, że tajemnicą objęte są również informacje, których nadawcą jest pacjent, a dotyczą one osób trzecich. Mogą to być zarówno osoby bliskie jak i postronne. Zdaniem Marka Safjana dla ustalenia, które informacje podlegają utajnieniu należy zastosować kryterium „zdrowego rozsądku". Jednocześnie wskazuje, że sferę ochrony wyznacza „nie tyle zawartość informacji, ale poufny charakter relacji, w których zostały uzyskane"[20]. Powyższe wpisuje się w podgląd prezentowany w literaturze, w myśl którego rozpowszechnianie danych o pacjencie w sposób zanonimizowany (uniemożliwiający identyfikację pacjenta) nie będzie stanowiło naruszenia tajemnicy medycznej[21].

[16] R. Kubiak, *Tajemnica*, s. 31.

[17] A. Bronowska-Garncarz, J. Garncarz, *Tajemnica zawodowa w medycynie*, „Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury", 2019, z. 4, s. 27.

[18] A. Huk, *Tajemnica zawodowa lekarza w polskim procesie karnym*, Warszawa 2006, s. 256.

[19] J. Sobczak, *Tajemnica lekarska,* „Medyczna Wokanda", 2016, nr 8, s. 62.

[20] M. Safjan, *Problemy prawne tajemnicy lekarskiej*, „Kwartalnik Prawa Prywatnego", 1995, nr 1, s. 11-12.

[21] Zob. M. Boratyńska, P. Konieczniak, *Prawa pacjenta*, Warszawa 2001, s. 338; R. Kubiak, *Prawo …..*, s. 221-222.

Obowiązek zachowania tajemnicy medycznej powstaje z chwilą powzięcia przez osoby wykonujące zawód medyczny informacji o pacjencie i wiąże również po jego śmierci, co wynika wprost z art. 14 ust. 3 u.p.p. Tak szeroko ujęty zakres temporalny obowiązku, stanowi, zdaniem niektórych autorów, przejaw poszanowania praw przysługujących pacjentowi za życia[22].

Obowiązek konfidencji nie jest absolutny. W art. 14 ust. 2 u.p.p. ustawodawca przewidział jego wyłączenia. Nadto dopuścił możliwość wyrażenia zgody na ujawnienie tajemnicy po śmierci pacjenta przez osobę bliską. Jednakże zwolnienia tego nie będzie można zastosować, gdy inna osoba bliska lub sam pacjent za życia wyrażą na to sprzeciw.

Dopuszczalność przetwarzania i ochrona danych o stanie zdrowia

Zasady dotyczące ochrony danych osobowych w Polsce określa ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych[23] oraz 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 (RODO)[24].

Artykuł 9 ust. 1 RODO wprowadza katalog danych osobowych, których przetwarzanie jest zabronione. Są to tzw. dane sensytywne, które wymagają szczególnej ochrony, z uwagi na to, że kontekst ich przetwarzania może powodować poważne ryzyko dla podstawowych praw i wolności. Wśród danych tych wymienia się dane dotyczących zdrowia osoby, które definiuje się jako dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia (art. 4 pkt 15 RODO). Jednocześnie w motywie 35 RODO wskazano, że do danych osobowych dotyczących zdrowia należy zaliczyć wszystkie dane o stanie zdrowia osoby, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą. Są to informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas

[22] P. Karlik, *Tajemnica zawodowa lekarza w procesie karnym w świetle ostatnich zmian*, „Medyczna Wokanda" 2016, nr 8, s. 75-76; I. Bernatek-Zaguła, *Pacjent–konsument czy podopieczny?,* „Acta Uniwersitatis Wratislaviensis. Przegląd Prawa i Administracji" 2004, t. LX, s. 135-136.

[23] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, tekst jednolity: Dz. U. z 2019 r., poz. 1781.

[24] Rozporządzenia 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. U. UE. L. z 2016 r., nr 119 (dalej: RODO).

świadczenia jej usług opieki zdrowotnej, numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych, informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych oraz wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą, niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne in vitro[25]. Ze wskazanego wyżej objaśnienia expressis verbis wynika, że dane medyczne, zwłaszcza zawarte w dokumentacji medycznej, posiadają status danych szczególnie chronionych[26]. Ich przetwarzania jest dopuszczalne jedynie za zgodą osoby, której dane maja być przetwarzane oraz w sytuacjach wskazanych w art. 9 ust. 2 lit. h rozporządzenia czyli gdy jest to niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem określonych warunków i zabezpieczeń. Dane te mogą być przetwarzane wyłącznie przez pracownika lub inną osobę podlegającego obowiązkowi zachowania tajemnicy zawodowej na mocy przepisów prawa. Nadto w oparciu o art. 9 ust. 4 państwa członkowskie mogą zachować lub wprowadzić dalsze warunki, w tym ograniczenia w odniesieniu do przetwarzania danych dotyczących zdrowia.

Powinność zachowania tajemnicy medycznej oraz dopuszczenie przetwarzania danych o stanie zdrowia pod pewnymi warunkami jest ze sobą związane na gruncie faktycznym[27]. Wymaga ono jednak zapewnienia odpowiedniego wielopłaszczyznowego zabezpieczenia przetwarzanych danych. W innym przypadku mogłoby to prowadzić do naruszenia prawa pacjenta do konfidencji oraz osłabiać poczucie bezpieczeństwa pacjenta jakie daje zapewnienie poufności.

Gwarancją odpowiedniego zabezpieczenia danych o stanie zdrowia jest nie tylko ustawowe ograniczenie ich przetwarzania, ale również stosowanie przez podmioty udzielające świadczeń zdrowotnych odpowiednich zabezpieczeń technicznych i organizacyjnych. Konieczna jest więc bieżąca ocena ryzyka za-

[25] Motyw 35, https://gdpr-text.com/pl/read/recital-35/. [dostęp: 2.11.2023].

[26] R. Kubiak, *Karnoprawna ochrona danych medycznych*, „Białostockie Studia Prawnicze" 2020, vol. 25, nr 2, s. 110.

[27] P. Durbajło, A. Piskorz-Ryń, *Problemy cyberbezpieczeństwa w telemedycynie*, w: *Telemedycyna i e-Zdrowie. Prawo i informatyka*, red. I. Lipowicz, G. Szpor, M. Świerczyński, Warszawa 2019, s. 285-286.

grożeń oraz opracowanie, wdrożenie i przestrzeganie procedur przetwarzania i zabezpieczania danych. Nadto zastosowanie i bieżące kontrolowanie środków bezpieczeństwa dostosowanych do zagrożeń, bazujących na aktualnym stanie wiedzy. Niezbędne jest też stałe aktualizowanie używanego oprogramowania i kontrolowanie funkcjonowania organizacyjnych i techniczno-informatycznych sposobów zabezpieczenia, a także okresowe dokonywanie oceny ich skuteczności. Wziąć pod uwagę należy także konieczność przechowywania dokumentacji medycznej w długim okresie czasu. Tym samym placówki ochrony zdrowia powinny zaplanować przenoszenie dokumentacji medycznej na informatyczne nośniki danych oraz do nowych formatów danych, jeśli wymaga tego zapewnienie ciągłości dostępu do przetwarzanej dokumentacji[28], a także właściwie zabezpieczyć pomieszczenia, w których znajduje się infrastruktura sieciowa lub serwerowa.

W ostatnim kontekście należy zwrócić uwagę na zakres podmiotowy dostępu do danych o stanie zdrowia przetwarzanych w systemie informatycznym[29] lub w Systemie Informacji Medycznej (SIM)[30]. Zgodnie z art. 35 ust. 1 ustawy o systemie informacji w ochronie zdrowia dostęp taki posiadają pracownicy medyczni, którzy wytworzyli elektroniczną dokumentację medyczną zawierającą dane osobowe lub jednostkowe dane medyczne pacjenta; pozostali pracownicy medyczni, którzy wykonują zawód w podmiocie, w którym została wytworzona elektroniczna dokumentacja medyczna, jeżeli jest to niezbędne do prowadzenia diagnostyki lub zapewnienia ciągłości leczenia; lekarze, pielęgniarki lub położne udzielający świadczeń opieki zdrowotnej w ramach umowy o udzielanie świadczeń opieki zdrowotnej z zakresu podstawowej opieki zdrowotnej oraz każdy pracownik medyczny w sytuacji zagrożenia życia pacjenta[31]. W innych przypadkach udostępnianie danych medycznych może nastąpić wyłącznie za zgodą pacjenta. Ustawodawca przewidział jednak szereg wyjątków w tym zakresie określonych w art. 12 ust. 3 – 8 u.s.i.o.z. Warto zauważyć, że szeroki katalog odstępstw jak i określenie podmiotów uprawnionych do dostępu do danych o stanie zdrowia w różnych aktach prawnych osłabia gwarancję zapewnienia poufności

[28] Par. 1 ust. 5 Rozporządzenia Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania, tekst jednolity: Dz. U. z 2022 r., poz. 1304.

[29] System teleinformatyczny to system teleinformatyczny w rozumieniu art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne – art. 2 pkt 13 u.s.i.o.z.

[30] System Informacji Medycznej (SIM) jest systemem teleinformatycznym służącym przetwarzaniu danych dotyczących udzielonych, udzielanych i planowanych świadczeń opieki zdrowotnej udostępnianych przez systemy teleinformatyczne usługodawców – art. 10 ust. 1 u.s.i.o.z.

[31] Art. 35 ust. 1 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, tekst jednolity: Dz. U. 2022, poz. 1555 (dalej: u.s.i.o.z.).

przetwarzanych danych[32]. Co więcej problem budzi również niekonsekwentne stosowanie przez polskiego ustawodawcę pojęcia danych medycznych. W myśl standardów europejskich dane medyczne to szczególny typ danych osobowych. Są to te dane, które dotyczą zdrowia. Na gruncie polskim ustawodawca albo nie posługuje się tym pojęciem w ogóle, co ma miejsce w przypadku ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, która zawiera przepisy określające sposób prowadzenia dokumentacji medycznej, albo wprowadza pojęcie jednostkowych danych medycznych jak w przypadku ustawy o systemie informacji w ochronie zdrowia. Taki brak jednolitości terminologicznej może powodować problemy interpretacyjne i wymaga przy stosowaniu pojęcia danych medycznych ich dookreślenia w miarę możliwości[33].

Tajemnica medyczna a technologia mHealth

W ostatnich latach zauważalny jest szybki rozwój obszaru mHealth (mobile health) czyli usług świadczonych za pomocą aplikacji instalowanych na urządzeniach mobilnych. Są to zarówno aplikacje tworzone przez samodzielnych deweloperów jak i placówki medyczne (autorskie aplikacje np. dla pacjentów laboratorium, przychodni itp). Aplikacje działają na urządzenia mobilnych takich jak m.in. telefon, smartwatch.

Technologia mHealth służy do zbierania licznych danych, przykładowo o wskaźnikach zdrowotnych, takich jak poziom ciśnienia krwi, masa ciała, ilość wykonanych kroków czy aktywność fizyczna. Jest więc nie tylko narzędziem pozwalającym na monitorowanie zdrowego trybu życia, ale również może wspomagać proces udzielania świadczeń zdrowotnych poprzez dostarczanie informacji o stanie zdrowia. To z kolei może się przyczyniać do rozpoznania i leczenia licznych schorzeń.

Potencjał mHealth został zauważony w Polsce już kilka lat temu nie tylko przez podmioty prywatne, ale również podmioty publiczne. W 2017 roku Narodowy Fundusz Zdrowia wprowadził dwie aplikacje na telefon: CanCell Cancer oceniającą ryzyko zachorowania na najczęściej występujące nowotwory oraz SweetPregna, wspomagającą samokontrolę, prawidłowe odżywianie, aktywność fizyczną oraz kontrolę glikemii kobiet ciężarnych, u których zdiagnozowano cukrzycę ciążową. Rok później uruchomiono aplikację mojeIKP zapewniającej dostęp do funkcjonalności Internetowego Konta Pacjenta.

O ile dane zbierane podczas kontaktu przedstawiciela zawodu medycznego z pacjentem podlegają odpowiedniej ochronie prawnej o tyle dane dotyczące

[32] K. Świtała, *Pacjent jako beneficjent ograniczeń jawności elektronicznej dokumentacji medycznej*, Warszawa 2018, s. 88-89.

[33] M. Jagielski, *Pojęcie danych medycznych i zasady ich ochrony*, w: *Ochrona danych osobowych medycznych*, K. Anders, E. Bielak-Jomaa, M. Jagielski, i in., Warszawa 2018, s. 3-7.

zdrowia zbierane przez deweloperów aplikacji mobilnych takimi regulacjami nie są objęte. W takim przypadku przetwarzanie danych odbywa się na podstawie zgody wyrażonej przez użytkownika aplikacji. W obecnym stanie prawnym widoczna jest więc niekonsekwencja. Dane uzyskane przez osoby wykonujące zawody medyczne i uczestniczące w procesie leczenia podlegają znacznie bardziej rygorystycznym regulacjom niż dane o stanie zdrowia pobierane przez inne podmioty.

Zakończenie

Choć nowoczesne technologie mają zastosowanie w sektorze ochrony zdrowia od stosunkowo niedawna to bezsprzecznie zwiększają efektywność procesów leczenia i wyznaczają kierunek dalszego jego rozwoju. Niemniej należy w pierwszej kolejności kierować się ogólną zasadą dobra pacjenta. W tym celu należy obecnie identyfikować nie tylko zalety ekonomiczne i społeczne jakie niesie za sobą zastosowanie technologii, ale również wskazywać nowe zagrożenia dla pacjentów i procesów leczenia[34].

Należy więc postulować wprowadzenie przez ustawodawcę definicji zawodu medycznego oraz sformułowania katalogu zawodów medycznych[35]. Pozwoliłoby to na wyeliminowanie wątpliwości co do tego kto jest zobowiązany do dochowania poufności danych objętych tajemnicą medyczną. Również pojęcie danych medycznych wymaga doprecyzowania. Brak bowiem jednolitości terminologicznej może powodować problemy interpretacyjne i potrzebę każdorazowego doprecyzowania tych danych.

Istotne wydaje się również rozszerzenie katalogu osób zobowiązanych do zachowania tajemnicy medycznej. W dobie rozwoju nowoczesnych technologii postulat ten znajduje uzasadnienie z uwagi na konieczność zaangażowania w proces udzielania świadczeń zdrowotnych również osób nie wykonujących zawodów medycznych, a niezbędnych do prawidłowego funkcjonowania systemu teleinformatycznego, w którym przetwarzania jest dokumentacja medyczna czy też prowadzenia konkretnych czynności medycznych przy użyciu nowoczesnej aparatury i sprzętu medycznego. Obecnie osoby takie nie są objęte obowiązkiem konfidencji poza regulacjami wynikającymi z przepisów prawa pracy lub postanowieniami umownymi. Należy więc postulować wprowadzenie przez ustawodawcę definicji zawodu medycznego oraz sformułowania katalogu zawodów

[34] K. Świtała, s. 1.

[35] 26 marca 2024 roku wejdzie w życie ustawa z dnia 17 sierpnia 2023 roku o niektórych zawodach medycznych. Nie stanowi ona jednak pełnego katalogu zawodów medycznych, a jedynie wprowadza regulacje dotyczące wykonywania 15 zawodów, które nie były dotychczas regulowane ustawowo.

medycznych[36]. Pozwoliłoby to na wyeliminowanie wątpliwości co do tego kto jest zobowiązany do dochowania poufności danych objętych tajemnicą medyczną. Również pojęcie danych medycznych wymaga doprecyzowania. Brak bowiem jednolitości terminologicznej może powodować problemy interpretacyjne i potrzebę każdorazowego doprecyzowania tych danych.

Istotne wydaje się również rozszerzenie katalogu osób zobowiązanych do zachowania tajemnicy medycznej. W dobie rozwoju nowoczesnych technologii postulat ten znajduje uzasadnienie z uwagi na konieczność zaangażowania w proces udzielania świadczeń zdrowotnych również osób nie wykonujących zawodów medycznych, a niezbędnych do prawidłowego funkcjonowania systemu teleinformatycznego, w którym przetwarzania jest dokumentacja medyczna czy też prowadzenia konkretnych czynności medycznych przy użyciu nowoczesnej aparatury i sprzętu medycznego. Obecnie osoby takie nie są objęte obowiązkiem konfidencji poza regulacjami wynikającymi z przepisów prawa pracy lub postanowieniami umownymi.

Zagrożenia dla bezpieczeństwa pacjenta związane z zachowaniem poufności danych dotyczących zdrowia występują w dużej mierze w obszarze technologii mHealth. Obecnie należy zrezygnować z myślenia według modelu zagwarantowania poufności danych w relacji lekarz – pacjent i rozszerzyć ją na inne płaszczyzny takie jak choćby pacjent – deweloper aplikacji. Konieczne jest więc zapewnienie szerszej ochrony danych o stanie zdrowia pozyskiwanych w ramach używanych aplikacji mobilnych.

W kontekście wyżej wymienionych zagrożeń należy zaznaczyć, iż mimo właściwego stosowania procedur bezpieczeństwa i przepisów prawa w świecie cyfrowym zawsze będzie występowało ryzyko naruszenia gwarancji bezpieczeństwa danych objętych tajemnicą medyczną. Rozwój technologii pomimo wszystkich aspektów pozytywnych spowodował też zwiększone ryzyko uzyskania dostępu do danych w wyniku działalności cyberprzestępczej[37]. Jednakże w placówkach ochrony zdrowia pozostaje niska świadomość o skali zagrożenia cyberatakami. Wynikiem tego jest często brak stosownych procedur wewnętrznych mających

[36] 26 marca 2024 roku wejdzie w życie ustawa z dnia 17 sierpnia 2023 roku o niektórych zawodach medycznych. Nie stanowi ona jednak pełnego katalogu zawodów medycznych, a jedynie wprowadza regulacje dotyczące wykonywania 15 zawodów, które nie były dotychczas regulowane ustawowo.

[37] Według Cybercrime Magazine w 2015 r. w USA zanotowano około 111 milionów cyberataków w sektorze ochrony zdrowia, które dotknęły w sumie 35% amerykańskiego społeczeństwa. W ataku na firmę zajmującą się sprzedażą ubezpieczeń zdrowotnych Anthem – doszło do jednorazowego wycieku ponad 78 milionów danych pacjentów. Według szacunków w latach 2017-2021 globalna wartość strat wynikających z działalności cyberprzestępców na świecie wyniosła 6 bilionów USD, a konieczne wydatki związane z zapewnieniem cyberbezpieczeństwa w tym okresie pochłonęły co najmniej 1 bilion USD, http://cybersecurityventures.com/cybersecurity-market-report/ [dostęp: 2.11.2023].

na celu ochronę systemów informatycznych[38]. Dlatego niezbędne wydaje się podnoszenie świadomości zagrożeń pracowników ochrony zdrowia poprzez edukację i odpowiednie regulacje wewnętrzne gwarantujące bezpieczeństwo danych dotyczących stanu zdrowia.

References

Bibliografia

Bernatek-Zaguła I., *Pacjent–konsument czy podopieczny?*, „Acta Uniwersitatis Wratislaviensis. Przegląd Prawa i Administracji" 2004, t. LX.

Boratyńska M., Konieczniak P., *Prawa pacjenta*, Warszawa 2001.

Bronowska-Garncarz A., Garncarz J., *Tajemnica zawodowa w medycynie,* „Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury" 2019, z. 4.

Dane osobowe: Cyberbezpieczeństwo a sektor ochrony zdrowia, https://www.rp.pl/zadania/art29-35351-dane-osobowe-cyberbezpieczenstwo-a-sektor-ochrony-zdrowia [dostęp: 2.11.2023].

Durbajło P., Piskorz-Ryń A., *Problemy cyberbezpieczeństwa w telemedycynie*, w: *Telemedycyna i e-Zdrowie. Prawo i informatyka*, red. I. Lipowicz, G. Szpor, M. Świerczyński, Warszawa 2019, s. 285-286.

Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021, http://cybersecurityventures.com/cybersecurity-market-report/ [dostęp: 2.11.2023].

Gula J., *Hipokrates a przerywanie ciąży*, w: *W imieniu dziecka poczętego*, red. J. W. Gałkowski, J. Gula, Rzym-Lublin 1991.

Huk A., *Tajemnica zawodowa lekarza w polskim procesie karnym*, Warszawa 2006.

Jagielski M., *Pojęcie danych medycznych i zasady ich ochrony*, w: *Ochrona danych osobowych medycznych*, K. Anders, E. Bielak-Jomaa, M. Jagielski, i in., Warszawa 2018.

Karlik P., *Tajemnica zawodowa lekarza w procesie karnym w świetle ostatnich zmian*, „Medyczna Wokanda" 2016, nr 8.

Konopka K., *Ochrona tajemnicy medycznej w e-zdrowiu*, „Białostockie Studia Prawnicze" 2020, vol. 25, nr 2.

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

Kubiak R., *Prawo medyczne,* Warszawa 2017.

Kubiak R., Kubicki L. red., *System prawa medycznego*, t. 1, *Pojęcie, źródła i zakres prawa medycznego*, Warszawa 2018.

Kubiak R., *Karnoprawna ochrona danych medycznych*, „Białostockie Studia Prawnicze" 2020, vol. 25, nr 2, s. 110.

Kubiński K. W., *Ochrona życia prywatnego człowieka*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 1993, z. 1.

Safjan M., *Problemy prawne tajemnicy lekarskiej*, „Kwartalnik Prawa Prywatnego" 1995, nr 1.

Sobczak J., *Tajemnica lekarska*, „Medyczna Wokanda" 2016, nr 8.

Świtała K., *Pacjent jako beneficjent ograniczeń jawności elektronicznej dokumentacji medycznej*, Warszawa 2018.

[38] Dane osobowe: Cyberbezpieczeństwo a sektor ochrony zdrowia, https://www.rp.pl/zadania/art2935351-dane-osobowe-cyberbezpieczenstwo-a-sektor-ochrony-zdrowia [dostęp: 2.11.2023].

Zoll A., *Ochrona prywatności w prawie karnym*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2000, z. 1.

Orzecznictwo

Wyrok Trybunału Konstytucyjnego z dnia 19.05.1998 r., U 5/97, OTK 1998, nr 4 poz. 46.

Wyrok Trybunału Konstytucyjnego z dnia 11.10.2011 r., K 16/10, OTK-A 2011, nr 8, poz. 80.

Wyrok Sądu Najwyższego z 13.06.1980 r., IV CR 182/80, OSNC 1981, nr 2-3, poz. 30.

Wyrok Sądu Najwyższego z 26.05.2017 r., I CSK 557/16, OSNC 2018, nr 3, poz. 33.

Wyrok Sądu Apelacyjnego w Poznaniu z dnia 10.01.2008 r., I ACa 1048/07, niepublikowany.

Akty prawne

Motyw 35, https://gdpr-text.com/pl/read/recital-35/ [dostęp: 2.11.2023].

Rozporządzenia 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.U. UE.L. z 2016 r., nr 119.

Rozporządzenie Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania, tekst jednolity: Dz. U. z 2022 r., poz. 1304.

Ustawa z dnia 23.04.1964 r. Kodeks cywilny, tekst jednolity: Dz. U. z 2023 r. poz. 610.

Ustawa z dnia 5.12.1996 r. o zawodzie lekarza i lekarza dentysty, tekst jednolity: Dz.U. z 2020 r. poz. 514.

Ustawa z dnia 6.06.1997 r. - Kodeks karny, tekst jednolity: Dz.U. z 2022 r. poz. 1138 z późn. zm.

Ustawa z dnia 6.11.2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, tekst jednolity: Dz.U. z 2023 r. poz. 1545 .

Ustawa z dnia 15.04.2011 r. o działalności leczniczej, tekst jednolity: Dz.U. z 2020 r. poz. 295.

Ustawa z dnia 28.04.2011 r. o systemie informacji w ochronie zdrowia, tekst jednolity: Dz. U. 2022, poz. 1555.

Ustawa z dnia 10.05.2018 r. o ochronie danych osobowych, tekst jednolity: Dz.U. z 2019 r. poz. 1781.