

Anna Rej-Kietla (1), Sandra Kryska (2)

1. Wyższa Szkoła Planowania Strategicznego w Dąbrowie Górniczej
2. Śląski Uniwersytet Medyczny w Katowicach

## OCHRONA DANYCH OSOBOWYCH PACJENTA W ŚWIETLE OBOWIĄZUJĄCYCH PRZEPISÓW PRAWA

adres korespondencyjny:  
Anna Rej-Kietla, ul. Kościelna 6, 41-303 Dąbrowa Górnicza  
e-mail: aniarej@interia.pl

### Streszczenie

Ochrona danych osobowych wynika przede wszystkim z Konstytucji Rzeczypospolitej Polskiej, zawierającej zapis o prawie do prywatności. Normy dotyczące tego zagadnienia odnajdziemy także w prawie cywilnym i karnym, a pewne elementy w prawie administracyjnym.

Jedną z form przetwarzania danych osobowych jest prowadzenie dokumentacji medycznej. Może być prowadzona w formie papierowej lub elektronicznej.

Zasadniczym warunkiem dopuszczającym przetwarzanie tego typu informacji jest zgoda osoby, której one dotyczą. Szczególny charakter danych wrażliwych polega na tym, że zgoda, aby była skuteczna musi zostać wyrażona w formie pisemnej. Należy mieć jednak na uwadze, że jeśli przetwarzanie danych jest niezbędne do zrealizowania danego uprawnienia bądź jest wymogiem prawa, zgoda osoby, której dane dotyczą nie będzie wymagana.

Informacje o stanie zdrowia zawarte w dokumentacji medycznej są danymi poufnymi. Lekarze i pozostały personel medyczny muszą dołożyć wszelkich starań, aby dane te były chronione i nie dostały się w posiadanie osób nieupoważnionych. Osoby, które ujawniają informacje np. o stanie zdrowia pacjenta podlegają sankcjom karnym.

Słowa kluczowe: dane osobowe, dane medyczne, ochrona

## Wprowadzenie

Polski ustawodawca chroni dane pacjentów w wielu obszarach. Ochrona danych osobowych wynika przede wszystkim z Konstytucji Rzeczypospolitej Polskiej, gdzie wyraźnie wspomniano o prawie do prywatności. Inne normy dotyczące tego zagadnienia odnajdziemy także w prawie cywilnym i karnym, a pewne elementy w prawie administracyjnym.

W rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne [1].

Pierwsze uregulowania dotyczące danych osobowych znajdziemy w ustawie o ochronie danych osobowych z 1970 roku, uchwalonej w Hesji. Akt ten był początkiem dalszych uregulowań między innymi w takich krajach jak Dania, Norwegia, Francja czy Luksemburg, a później w Austria czy Wielka Brytania [2].

W literaturze wyróżnia się dwa rodzaje danych osobowych tzw. zwykłe dane i dane wrażliwe czy sensytywne.

Prawo do ochrony danych medycznych jest prawem każdego pacjenta. Dyrektywa nr 95/46/CE dotycząca danych wrażliwych, reguluje zagadnienia związane z przetwarzaniem danych do celów medycyny prewencyjnej, diagnostyki medycznej, świadczeń medycznych. Porusza także kwestie związane z wyrażeniem zgody podmiotu uprawnionego na przetwarzanie informacji o stanie zdrowia lub, jeśli podmiot jest fizycznie bądź prawnie niezdolny do udzielenia zgody, przekazania uprawnień w tym względzie innej osobie [3].

Ustawa o ochronie danych osobowych (Dz.U. z 2015 poz. 2135) nie definiuje pojęcia danych sensytywnych. Można jednak w art. 27 Ustawy znaleźć informacje, które dane podlegają szczególnej ochronie.

Zabrania się przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym [1].

Przetwarzanie danych wrażliwych, co do zasady jest zabronione, poza sytuacjami wyjątkowymi wskazanymi w ustępie 2 ustawy:

- 1) osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, chyba że chodzi o usunięcie dotyczących jej danych;
- 2) przepis szczególnie innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony;

- 3) przetwarzanie takich danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora;
- 4) jest to niezbędne do wykonania statutowych zadań kościołów i innych związków wyznaniowych, stowarzyszeń, fundacji lub innych niezarobkowych organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, pod warunkiem, że przetwarzanie danych dotyczy wyłącznie członków tych organizacji lub instytucji albo osób utrzymujących z nimi stałe kontakty w związku z ich działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych;
- 5) przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem;
- 6) przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie;
- 7) przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych;
- 8) przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą;
- 9) jest niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego; publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone;
- 10) przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym. [1].

W obowiązującym aktualnie stanie prawnym zakazane jest przetwarzanie zarówno informacji odnoszących się bezpośrednio do stanu zdrowia człowieka, jak i informacji, z których przeciętny odbiorca może w prosty sposób wywieść takie dane.

Od 1 stycznia 2015 roku obowiązuje Ustawa z dnia 7 listopada 2014 o ułatwieniu prowadzenia działalności gospodarczej, przyjęta w ramach tzw. IV pakietu deregulacyjnego, która wprowadziła pewne zmiany w ustawie z dnia 29 sierpnia 1997 roku o ochronie danych osobowych. Najważniejsze z nich dotyczą kwestii związanych z administratorem bezpieczeństwa informacji oraz jego organizacji pracy.

Administratorem danych jest organ, jednostka organizacyjna, podmiot lub osoba, decydujące o celach i środkach przetwarzania danych osobowych. Lekarze prowadzący prywatne praktyki i podmioty lecznicze jako administratorzy danych również są zobowiązani do stosowania przepisów tej ustawy. Art. 36a ustawy o ochronie danych osobowych stanowi, że administrator danych może powołać administratora bezpieczeństwa informacji (ABI), lub sam wykonywać jego zadania (art. 36b). Do zadań ABI należy sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie sprawozdań w tym zakresie dla administratora danych, opracowanie i aktualizacja dokumentacji (dbanie, aby dokumentacja była kompletna, zgodna z aktualnymi przepisami prawa) [1].

Personalalia pacjenta (imię i nazwisko, data urodzenia, płeć, numer PESEL, adres zamieszkania, a w przypadku, gdy pacjentem jest osoba małoletnia, całkowicie ubezwłasnowolniona lub niezdolna do świadomego wyrażenia zgody – nazwisko i imię/imiona przedstawiciela ustawowego oraz adres jego miejsca zamieszkania), a także informacje medyczne dotyczące jego stanu zdrowia i udzielonych świadczeń zdrowotnych zawarte w dokumentacji medycznej podlegają ochronie.

Ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta z 2008 roku również reguluje kwestie związane z danymi osobowymi; w art. 13 czytamy tam, że 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 [4].

Należy tu także wspomnieć o takich aktach normatywnych jak ustawa o zawodach lekarza i lekarza dentystry czy ustawa o zawodach pielęgniarki i położnej, w których to odnajdziemy kolejne regulacje dotyczące tajemnicy lekarskiej i pielęgniarskiej o danych medycznych i osobowych związanych z pacjentem.

Warunkiem, który dopuszcza przetwarzanie danych osobowych jest zgoda osoby, której dane dotyczą. Szczególny charakter danych wrażliwych polega na tym, że zgoda musi zostać wyrażona w formie pisemnej, w przeciwnym razie zgoda ta jest nieskuteczna. Forma ta nie ma zastosowania w przypadku usuwania tego typu informacji [5,6].

Zgoda na przetwarzanie danych osobowych jest uznawana za oświadczenie woli, zatem należy się odwołać do Kodeksu cywilnego (art.78), w którym ustawodawca wyjaśnia, że do zachowania pisemnej formy czynności prawnej wystarczy złożenie własnoręcznego podpisu na dokumencie, który obejmuje oświadczenie woli. Oznacza to, że nie jest wymagane, aby całe oświadczenie woli zostało sporządzone własnoręcznie, jego treść może zostać wydrukowana np. na formularzu. Wymagany jest tu jednak własnoręczny podpis osoby upoważnionej [7,8].

Jednak jeśli przetwarzanie danych staje się niezbędne do zrealizowania danego uprawnienia bądź jest wymogiem prawa, wówczas zgoda osoby, której dane dotyczą nie jest wymagana.

### **Znaczenie dokumentacji medycznej**

Jedną z form przetwarzania danych osobowych jest prowadzenie dokumentacji medycznej. Może być prowadzona w formie papierowej lub elektronicznej. Udostępnianie dokumentacji może nastąpić przez wgląd w podmiocie leczniczym, sporządzenie odpisów lub kopii, a także wydanie oryginału z zastrzeżeniem zwrotu po jej wykorzystaniu.

Może mieć ona dwojaki charakter: zewnętrzny, który obejmuje dokumenty przeznaczone na użytek pacjenta, takie jak na przykład. Skierowanie, oraz wewnętrzny – sporządzony na potrzeby jednostki ochrony zdrowia.

Odmowa wydania dokumentacji wymaga formy pisemnej oraz podania przyczyn. Należy mieć na uwadze, że może być udostępniona tylko podmiotom i organom uprawnionym na podstawie odrębnych przepisów, tym m.in. Zakładowi Ubezpieczeń Społecznych, Narodowemu Funduszowi Zdrowia czy Głównemu Urzędowi Statystycznemu [9].

Poza tym, że ma ważne znaczenie w procesie diagnozowania i leczenia pacjenta, jest także istotnym środkiem dowodowym. Na gruncie prawa cywilnego dokumentacja medyczna jako środek dowodowy ma szczególne znaczenie, głównie w postępowaniach dotyczących odpowiedzialności deliktowej oraz odpowiedzialności kontraktowej.

Dokumentacja ta często jest wykorzystywana także w postępowaniu karnym, w postępowaniu z zakresu prawa pracy i ubezpieczeń społecznych oraz w postępowaniu w przedmiocie odpowiedzialności zawodowej personelu medycznego [9,10].

Konieczność prowadzenia dokumentacji medycznej można wywieść z prawa pacjenta do uzyskania informacji o swoim stanie zdrowia, zapisanego w Ustawie o prawach pacjenta i Rzeczniku Praw Pacjenta [11].

Konsekwencje utraty dokumentacji medycznej na gruncie ustawy o ochronie danych osobowych są natury prawnokarnej. Wszelkie sankcje ponosić będzie osoba odpowiedzialna za zabezpieczenie dokumentacji, a więc administrator danych.

Dokumentacja medyczna może być prowadzona również w formie elektronicznej. Tą kwestię reguluje ustawa z dnia 28 kwietnia 2011 roku o systemie informacji w ochronie zdrowia. Należy zwrócić uwagę, iż 23 lipca 2014 roku, Prezydent RP podpisał nowelizację tej ustawy. Umożliwia ona prowadzenie dokumentacji w postaci papierowej lub elektronicznej do 31 lipca 2017 roku. Po tym terminie obowiązywać będzie tylko dokumentacja medyczna w postaci elek-

tronicznej. Kolejnym krokiem w celu podniesienia jakości usług medycznych będzie wykorzystanie nowych technologii informatycznych w wyniku stworzenia infrastruktury technicznej i informatycznej, która pozwoli na wprowadzenie specjalistycznych e-usług z zakresu telemedycyny.

### **Dostęp osób upoważnionych oraz innych podmiotów do dokumentacji medycznej**

Podmiot udzielający świadczeń zdrowotnych udostępnia dokumentację medyczną przede wszystkim pacjentowi, ale również przedstawicielowi ustawowemu pacjenta, a także osobie przez niego wyznaczonej. Po śmierci pacjenta wgląd do jego dokumentacji ma tylko osoba, upoważniona przez pacjenta za życia [12].

Uważa się, że w przypadku osoby poczętej, lecz jeszcze nienarodzonej, informacje dotyczące *nasciturusa* stają się danymi osobowymi pod warunkiem, że urodzi się ona żywa. Wtedy też dane te chronione są od momentu jego poczęcia. W sytuacji, gdy osoba poczęta nie urodziła się żywa wszelkie dane i informacje jej dotyczące, uważa się, że danymi osobowymi nie są. Oczywiście, nie oznacza to, że informacje te w ogóle nie będą chronione. Będą one mimo wszystko chronione, gdyż są danymi osobowymi matki [13].

Podmiotami i organami, które w myśl ustawy o prawach pacjenta (art. 26 ust. 3), z urzędu mają prawo wglądu do dokumentacji są:

- 1) podmioty udzielający świadczeń zdrowotnych, jeżeli dokumentacja ta jest niezbędna do zapewnienia ciągłości świadczeń zdrowotnych;
- 2) organy władzy publicznej, Narodowy Fundusz Zdrowia, organy samorządu zawodów medycznych oraz konsultanci krajowi i wojewódzcy, w zakresie niezbędnym do wykonywania przez te podmioty ich zadań, w szczególności kontroli i nadzoru;
- 3) podmioty, o których mowa w art. 119 ust. 1 i 2 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej, w zakresie niezbędnym do przeprowadzenia kontroli na zlecenie ministra właściwego do spraw zdrowia;
- 4) minister właściwy do spraw zdrowia, sądy, w tym sądy dyscyplinarne, prokuratorzy, lekarze sądowi i rzecznicy odpowiedzialności zawodowej, w związku z prowadzonym postępowaniem;
- 5) uprawnione na mocy odrębnych ustaw organy i instytucje, jeżeli badanie zostało przeprowadzone na ich wniosek;
- 6) organy rentowe oraz zespoły do spraw orzekania o niepełnosprawności, w związku z prowadzonym przez nie postępowaniem;
- 7) podmioty prowadzące rejestry usług medycznych, w zakresie niezbędnym do prowadzenia rejestrów;
- 8) zakłady ubezpieczeń, za zgodą pacjenta;

- 9) lekarz, pielęgniarka lub położna, w związku z prowadzeniem procedury oceniającej podmiot udzielający świadczeń zdrowotnych na podstawie przepisów o akredytacji w ochronie zdrowia, w zakresie niezbędnym do jej przeprowadzenia;
- 10) wojewódzka komisja do spraw orzekania o zdarzeniach medycznych, o której mowa w art. 67e ust. 1, w zakresie prowadzonego postępowania;
- 11) spadkobiercy w zakresie prowadzonego postępowania przed wojewódzką komisją do spraw orzekania o zdarzeniach medycznych, o której mowa w art. 67e ust. 1;
- 12) osoby wykonujące czynności kontrolne na podstawie art. 39 ust. 1 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. Nr 113, poz. 657 i Nr 174, poz. 1039), w zakresie niezbędnym do ich przeprowadzenia;
- 13) dokumentacja medyczna może być udostępniona także szkole wyższej lub instytutowi badawczemu do wykorzystania w celach naukowych, bez ujawniania nazwiska i innych danych umożliwiających identyfikację osoby, której dokumentacja dotyczy.

### **Odpowiedzialność karna**

Warto zwrócić uwagę na kwestie związane z odpowiedzialnością karną w wymienionych niżej sytuacjach:

#### Przetwarzanie danych przez nieuprawnionego

Przetwarzanie danych osobowych przez osobę, która nie jest do tego uprawniona podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Jeżeli ujawnienie danych dotyczy tzw. danych wrażliwych sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.

#### Udostępnianie danych osobom, które nie są do tego uprawnione:

Administrowaniem zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

#### Przechowywanie danych w sposób nieprawidłowy

Kto administrując zbiorem danych przechowuje w zbiorze dane osobowe niezgodnie z celem utworzenia zbioru, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

### Udostępnianie danych osobom nieuprawnionym

Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

### Niezgłoszenie danych do rejestru

Niezgłoszenie przez osoby do tego obowiązane zbioru danych do rejestru, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

### Naruszenie obowiązku zabezpieczenia danych

Administrator danych, który choćby nieumyślnie naruszy obowiązek zabezpieczenia ich przed zabraniami przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

### Niezgłoszenie danych do rejestru

Kto będąc do tego obowiązany nie zgłasza do rejestracji zbioru danych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

## **Podsumowanie**

Informacje o stanie zdrowia, które zawarte są w dokumentacji medycznej są danymi poufnymi. Lekarze i personel medyczny muszą dołożyć wszelkich starań, aby dane te były odpowiednio chronione i nie dostały się w posiadanie osób nieupoważnionych. Osoby, które ujawniają dane np. o stanie zdrowia pacjenta podlegają sankcjom karnym.

## **Bibliografia**

1. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2015 r. poz. 2135).
2. Goździewicz G., Szablowska M. (red.) *Prawna ochrona danych osobowych na tle europejskich standardów*. Dom Organizatora, Toruń 2000.
3. Jacek A, Szwed K, Ożóg K, Porada S. *Aspekt ochrony danych osobowych pacjentów w świetle obowiązujących regulacji prawnych w Polsce oraz Unii Europejskiej*. *Hygeia Public Health*. 2013; 48(1): 46–50.
4. Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. 2012, poz. 159).
5. Strzesak E. *Jak udostępnić dokumentację medyczną*. *Magazyn Pielęgniarki i Położnej*. 2002; 12: 34–35.



6. Jackowski M. *Ochrona danych medycznych*. Dom Wyd. ABC. Warszawa, 2002.
7. Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny, Dz.U. 1964 Nr 16 poz. 93.
8. Barta J., Fajgielski P., Markiewicz R. *Ochrona danych osobowych. Komentarz, LEX 2011*.
9. Materna N. *E-dokumentacja medyczna, a ochrona danych osobowych*. Biuletyn Stowarzyszenia Absolwentów i Przyjaciół Wydziału Prawa Katolickiego Uniwersytetu Lubelskiego. 2014; 11.
10. Kordel K. *Prowadzenie dokumentacji medycznej – implikacje dowodowe*. Prawo i Medycyna. 2006; 3: 100–110.
11. Jendry M. (red.) *Ochrona danych medycznych w 2015 r.* Wyd. Wiedza i Praktyka, Warszawa 2015; 7–13.
12. Wroński K, Bocian R, Cywiński J, Dziki A. *Prawne konsekwencje związane z ujawnieniem dokumentacji medycznej osobom nieuprawnionym*. Kardiochirurgia i Torakochirurgia Polska. 2008; 5(4): 463–465.
13. Rzymowski J. *Ochrona osobowych danych medycznych*. Alergia. 2012; 1: 21–23.

## **Legal regulations concerning the protection of patients' personal data**

### **Abstract**

Protection of personal data is primarily due to the Polish Constitution, which mentions the right to privacy. Civil, criminal, and some elements of administrative law offer more on this subject.

The keeping of medical records in paper or electronic form is one form of processing personal data.

The main condition which allows the processing of this type of information is the consent of the data subject. The specific nature of sensitive data is the reason that consent must be expressed in writing, otherwise the agreement is ineffective.

Health information contained in medical records is confidential data. Doctors and medical staff must ensure that the data is protected against unauthorized access. Those who reveal information about your health are subject to criminal penalties.

Key words: personal data, medical data, protection