VIA MEDICA

Varia

Biuletyn Polskiego
Towarzystwa Onkologicznego
NOWOTWORY
2019, tom 4, nr 5–6, 247–251

ISSN 2543–5248
www.nowotwory.edu.pl

# Ochrona danych osobowych w indywidualnej praktyce lekarskiej – na co zwracać uwagę

Hanna Rubaszewska

*BSJP Brockhuis Jurczak Prusak Sroka Nilsson, Poznań*

W artykule przedstawiono istotne elementy związane z wdrażaniem zasad ochrony danych osobowych w placówkach medycznych. W listopadzie 2019 roku Najwyższa Izba Kontroli opublikowała wyniki kontroli w placówkach tego typu i zaleciła Prezesowi Urzędu Ochrony Danych Osobowych przeprowadzanie systemowych kontroli przestrzegania zasad ochrony danych osobowych w jednostkach z sektora ochrony zdrowia. Oznacza to, że zagadnienia odpowiedniego wdrożenia zasad ochrony danych osobowych w placówkach medycznych pozostają cały czas aktualne.

Biuletyn PTO NOWOTWORY 2019; 4, 5–6: 247–251

**Słowa kluczowe:** ochrona danych osobowych, zasady przetwarzania danych osobowych pacjentów, ocena ryzyka naruszenia danych osobowych, roszczenia pacjentów

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE – zwane w dalszej części niniejszego artykułu RODO – w jednolitym brzmieniu weszło w życie 25 maja 2018 roku we wszystkich krajach Unii Europejskiej. Polska ustawa o ochronie danych osobowych z 10 maja 2018 roku (Dz.U. 2018, poz. 1000) zaczęła obowiązywać także 25 maja 2018 roku.

Po roku obowiązywania obu aktów prawnych (21 lutego 2019 roku) – ustawą z o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE – zmieniono pakiet ustaw branżowych, dostosowujących przepisy prawa krajowego do w/w rozporządzenia, w tym między innymi ustawę z 5 grudnia 1996 o zawodzie lekarza i lekarza dentysty (Dz.U. z 2019, poz. 537 z późn. zm.) oraz ustawę z 15 kwietnia 2011 roku o działalności leczniczej (Dz.U. 2018, poz. 2190 z późn. zm.).

Warto pamiętać, że RODO ma pierwszeństwo przed przepisami krajowymi, z zastrzeżeniem, że jeżeli przepisy branżowe (krajowe) przewidują „dalej idącą ochronę", to wówczas te przepisy mają pierwszeństwo przed RODO.

Dodatkowo do Urzędu Ochrony Danych Osobowych (UODO), zgodnie z art. 40 RODO, zostały złożone dwa kodeksy branżowe, tzw. kodeksy postępowania dla sektora ochrony zdrowia, celem ujednolicenia zasad przetwarzania danych osobowych w placówkach medycznych. Zatwierdzenie tych kodeksów postępowania oznacza, że są one dla UODO wiążące i traktowane jako obligatoryjne.

Należy od razu zaznaczyć, że jedną z istotnych zasad ochrony danych osobowych jest tzw. zasada proporcjonalności, zgodnie z którą – w myśl motywu 4 RODO – **prawo do ochrony danych osobowych nie jest prawem bezwzględnym; należy go postrzegać w kontekście jego funkcji społecznej i wyważyć względem innych praw podstawowych**, tj. w myśl zasady proporcjonalności.

Oznacza to, że ochrona żywotnych interesów pacjenta ma pierwszeństwo przed realizacją prawa do ochrony jego danych osobowych – czyli ratowanie zdrowia pacjenta jest ważniejsze od przestrzegania zasad ochrony danych osobowych.

## Najważniejsze obowiązki placówek medycznych

### Podstawy przetwarzania danych osobowych

Definicja „danych dotyczących zdrowia", określona w art. 4 pkt. 15 RODO, jest zgodna z definicją WHO: „zdrowie to dobrostan fizyczny i psychiczny organizmu". W świetle komentowanej regulacji dane, które dotyczą zdrowia, ujawniają informacje o stanie zdrowia człowieka, w tym dane o jego przeszłym, obecnym i przyszłym stanie fizycznym i psychicznym, dane o nałogach czy uzależnieniach, a także informacje o korzystaniu z opieki zdrowotnej. Co istotne, zgodnie z motywem 35 RODO dane dotyczące zdrowia to wszystkie informacje, które są zbierane podczas rejestracji do usług opieki zdrowotnej lub podczas świadczenia usług opieki zdrowotnej.

W związku z tym powstała wątpliwość, czy dane zbierane podczas rejestracji, np. numer telefonu czy adres e-mail pacjenta, należą do danych, które można przetwarzać bez jego zgody, jako niezbędny element wykonywania świadczenia usług opieki zdrowotnej. Odpowiedź na to pytanie jest twierdząca, tzn. również te dane można przetwarzać bez zgody pacjenta, ponieważ jest to niezbędne do zrealizowania obowiązku lub uprawnienia wynikającego z przepisu prawa, np. pacjent musi być poinformowany o zmianie wizyty czy niezwłocznie o wyniku badania.

Projekty kodeksów branżowych złożonych w Urzędzie Ochrony Danych Osobowych zasadnie wyróżniły elementy świadczenia usług opieki zdrowotnej, które nie wymagają zgody pacjenta na przetwarzanie jego danych osobowych.

1. Zgodnie z art. 6 ust. 1 lit. C i D RODO, w zw. z art. 9 ust. 2 lit. H RODO, przetwarzanie danych osobowych dotyczących stanu zdrowia znajduje oparcie w przepisach krajowego prawa medycznego [1–4]. Oznacza to, że przetwarzanie danych osobowych pacjenta w celach zdrowotnych – związanych ze świadczeniem opieki zdrowotnej, ale i profilaktyki zdrowotnej, diagnozy medycznej, zapewnienia opieki społecznej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej, medycyny pracy, oceny zdolności pracownika do pracy – nie wymaga jego zgody.
   Odnośnie:
   a) profilaktyki zdrowotnej – w tym zakresie mieszczą się: zaproszenia na badania przesiewowe, zaproszenia na wykonanie szczepień, przekazywanie materiałów edukacyjnych, przekazywanie informacji o wydarzeniach prozdrowotnych, wykonywanie wizyt patronażowych, badań bilansowych i testów przesiewowych – profilaktyka zdrowotna jest wówczas niezbędna, jeżeli jest uzasadniona stanem zdrowia pacjenta lub czynnikami ryzyka, lub rokowaniami co do niego zawartymi w dokumentacji medycznej, albo jeżeli wynika to z przepisów prawa [5];
   b) diagnozy medycznej i leczenia – w tym zakresie mieszczą się: przetwarzanie danych osobowych pacjenta w związku z procesem udzielania świadczeń zdrowotnych (diagnostycznych i leczniczych), w tym prowadzenie dokumentacji medycznej (na podstawie art. 3 ust.1 ustawy o działalności leczniczej oraz art. 24 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta).
2. Przetwarzanie danych osobowych pacjenta bez jego zgody – w tym zakresie także mieszczą się sytuacje związane z dochodzeniem roszczeń (na podstawie art. 6 ust.1 lit. F RODO).
3. Przetwarzanie danych osobowych pacjenta za jego zgodą – m.in. w celach marketingowych, w związku z badaniami klinicznymi.

### Obowiązek informacyjny

Każda placówka medyczna musi spełniać obowiązek informacyjny. Podstawą jest tu art. 13 RODO, tzw. klauzula informacyjna. Oznacza to, że w każdej placówce medycznej, w miejscu widocznym, powinna znajdować się klauzula zawierająca co najmniej:

- nazwę placówki medycznej i jej dane kontaktowe,
- dane inspektora ochrony danych, jeżeli został powołany,
- informację o celu przetwarzania i kategorię odbiorców,
- informację o prawie dostępu do danych, ich poprawiania, dobrowolności podania, cofnięciu zgody,
- podstawę prawną przetwarzania danych,
- prawne uzasadnienie interesu administratora, jeżeli na tej podstawie odbywa się przetwarzanie,
- informację o zamiarze przekazania danych do państwa trzeciego (jeżeli dotyczy),
- informację o okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe – informacje o kryteriach ustalenia tego okresu,
- profilowaniu, zautomatyzowanym podejmowaniu decyzji,
- informację o prawie wniesienia skargi do Urzędu Ochrony Danych Osobowych,
- informację, czy podanie danych osobowych jest wymogiem ustawowym, umownym lub warunkiem zawarcia umowy oraz informację o konsekwencji niepodania takich danych,
- informację o prawach osoby, której dane dotyczą.

Pacjent nie musi pisemnie potwierdzać, że zapoznał się z tą klauzulą. Wystarczy, że placówka medyczna zadba, by klauzula informacyjna była dostępna i by pacjent bez trudu mógł się z nią zapoznać.

### Upoważnienia

Do przetwarzania danych mogą być dopuszczone wyłącznie osoby, które:

- mają upoważnienie nadane przez lekarza prowadzącego indywidulaną praktykę lub zarząd w spółkach osobowych i kapitałowych i
- przetwarzają dane zawsze **na podstawie polecenia lekarza czy zarządu**.

Zgodnie z art. 107 ustawy o ochronie danych osobowych **„kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony – podlega grzywie, karze ograniczenia wolności albo pozbawienia wolności do dwóch lat".**

Należy zwrócić szczególną uwagę na to, aby każda osoba, która ma dostęp do danych osobowych, miała upoważnienie ze wskazaniem jego zakresu. Przy czym inny zakres należy wskazać dla lekarza – np. prawo dokonywania wpisów, inny dla rejestratorek – prawo do przeglądania, kopiowania, a jeszcze inny dla prezesa placówki, który nie jest lekarzem – np. prawo do przeglądania danych zbiorczych.

Trzeba też pamiętać, że w placówce medycznej dane osobowe mogą przetwarzać tylko osoby przeszkolone i takie, które mają odpowiednie upoważnienie.

## Realizacja praw pacjenta

Każda placówka medyczna powinna także mieć regulamin realizacji praw pacjenta opracowany w oparciu o przepisy o ochronie danych osobowych. Urząd Ochrony Danych Osobowych zwraca na to szczególną uwagę podczas swoich kontroli. Taki regulamin określa zasady realizacji wniosków pacjentów dotyczących ich danych osobowych.

1. Zgodnie z art. 15 RODO **każdy pacjent ma prawo dostępu do swoich danych osobowych.**
   Nowelizacja art. 28 ust. 2 a) ustawy z 6 listopada 2008 roku o prawach pacjenta i Rzeczniku Praw Pacjenta (dalej ustawa o pp) dotyczy opłat za udostępnianie kopii dokumentacji medycznej i rozstrzyga spór o odpłatność za wydanie pierwszej kopii dokumentacji medycznej. Do niedawna kontrowersje wzbudzała relacja art. 15 ust. 3 RODO do w/w art. 28 ust.1 ustawy o pp w poprzednim brzmieniu. Z jednej strony RODO w art. 15 ust. 3 wskazuje na nieodpłatność pierwszej kopii danych osobowych, a z drugiej strony zgodnie z art. 28 ust.1 poprzedniej wersji ustawy o pp przysługiwało placówce medycznej prawo do pobierania opłaty za kopię dokumentacji medycznej. Rzecznik Praw Pacjenta uznał, że każda pierwsza kopia dokumentacji medycznej powinna być bezpłatna, natomiast Urząd Ochrony Danych Osobowych rozróżnił prawo do otrzymania kopii danych osobowych (nie musi być ona w formie dokumentacji medycznej) oraz prawo do otrzymania kopii dokumentacji medycznej.

   **Obecnie, po nowelizacji, opłaty za udostępnienie dokumentacji medycznej nie pobiera się:**

   a) od pacjenta/przedstawiciela ustawowego po raz pierwszy w żądanym zakresie i w sposób, o którym mowa w art. 27 ust.1 pkt. 2 i 5 ustawy o pp (przez sporządzenie wyciągu, odpisu, kopii, wydruku lub zapisania na informatycznym nośniku danych) i w ust. 3 (przez sporządzenie kopii w formie skanu);
   b) w związku z postępowaniem przed wojewódzką komisją ds. orzekania o zdarzeniach medycznych.
2. Zgodnie z art. 16 RODO **każdy pacjent ma prawo do sprostowania danych (które są nieprawidłowe)** – takie żądanie zawsze należy zrealizować.
3. Zgodnie z art. 17 RODO **każdy pacjent ma prawo do usunięcia danych i prawo do bycia zapomnianym**. W przesłanym do Urzędu Ochrony Danych Osobowych projekcie kodeksu branżowego słusznie uznano, że pacjentowi, który będzie domagał się usunięcia jego danych osobowych, należy odmówić realizacji tego prawa. Zgodnie z przepisami prawa, w tym zgodnie z art. 29 ust.1 ustawy o pp, każda placówka medyczna ma obowiązek przechowywać dokumentację medyczną przez lat 20, licząc od końca roku kalendarzowego, w którym dokonano ostatniego wpisu oraz w pozostałych przypadkach wskazanych w tym przepisie, czyli odpowiednio: 5 lat – dla skierowań na badania lub zleceń lekarza, 2 lata – dla wystawionych skierowań, 22 lata – dla dokumentacji medycznej dziecka, które nie ukończyło 2 lat, 30 lat – w razie zgonu pacjenta lub uszkodzenia jego ciała czy zatrucia.

   Oznacza to, że wszystkie dane osobowe zawarte w dokumentacji medycznej nie mogą zostać usunięte przed upływem wymienionych okresów.

   Jeżeli dane osobowe pacjenta są przetwarzane na podstawie jego zgody (np. przetwarzane w celach marketingowych (por. pkt. 3 Podstawy przetwarzania danych osobowych nin. opracowania), to wówczas takie żądanie należy zrealizować.
4. Zgodnie z art. 20 RODO **każdy pacjent ma prawo do przenoszenia danych**. Placówka medyczna nie może zrealizować tego prawa wobec danych osobowych przetwarzanych w dokumentacji medycznej. Prawo to należy zrealizować tylko wobec tych operacji, które są przetwarzane w sposób zautomatyzowany i w oparciu o zgodę pacjenta lub w oparciu o umowę, której pacjent jest stroną.

   Placówka medyczna ma obowiązek przekazać dane w ustrukturyzowanym formacie, umożliwiającym odczyt komputerowy (PDF).

## Szacowanie ryzyka

Każda placówka medyczna, zgodnie z art. 32 RODO, ma obowiązek dokonania oszacowania ryzyka. Jest to najważniejszy element wdrażania RODO w placówce medycznej, gdyż całe rozporządzenie opiera się na ocenie ryzyka.

Ocena ryzyka polega na usystematyzowaniu znajdujących się w każdej placówce medycznej aktywów, takich jak:

- **aktywa informacyjne:** zbiory danych osobowych, dokumentacja (materiały szkoleniowe, procedury eksploatacyjne, plany utrzymania ciągłości działania, informacje zarchiwizowane),
- **aktywa fizyczne:** sprzęt komputerowy, informacyjny, nośniki, pomieszczenia, zabezpieczenia budynku,
- **aktywa oprogramowania:** aplikacyjne, systemowe, narzędziowe,

- **aktywa usług:** usługi infrastruktury technicznej (ogrzewanie, oświetlenie, klimatyzacja, zasilanie, ochrona),
- **czynnik ludzki:** świadomość, umiejętności, wiedza, szkolenia, doświadczenie, zastępowalność.

Następnie należy przyjąć model oszacowania ryzyka, który uwzględnia katalog zabezpieczeń, zagrożeń, ocenę prawdopodobieństwa wystąpienia zagrożenia i ocenę powagi ryzyka.

Przy ocenie ryzyka dokonuje się analizy wszystkich czynników, nie tylko informatycznych.

Trzeba jednak zwrócić uwagę, że RODO nie wskazuje konkretnych sposobów zabezpieczeń (poza przykładową pseudonimizacją oraz szyfrowaniem danych) koniecznych do wdrożenia procedur. Zgodnie z art. 32 RODO każda placówka medyczna powinna w ramach oceny ryzyka uwzględniać takie sposoby i metody, które zapewnią stopień bezpieczeństwa danych osobowych odpowiadający oszacowanemu ryzyku.

Nie ma więc ogólnych wzorców, które byłyby dopasowane do każdej placówki medycznej. Dla przykładu: w każdej placówce medycznej jest inna liczba zatrudnionych osób, liczba komputerów, laptopów, rozwiązań organizacyjnych, podmiotów, z którymi dana placówka medyczna współpracuje, zabezpieczeń, rozwiązań informatycznych. Dlatego wymagane jest kompleksowe podejście do oceny ryzyka i z takiej oceny powinien powstać dokument, który ocenia Urząd Ochrony Danych Osobowych podczas ewentualnej kontroli.

## Naruszenie danych osobowych

Naruszenie danych osobowych to przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Należy zwrócić uwagę, że wysłanie omyłkowo maila z danymi osobowymi do osoby, która nie powinna być adresatem wiadomości, jest naruszeniem danych osobowych – to tzw. incydent. Podobnie zagubienie recepty, ujawnienie danych pacjenta czy historii choroby osobie nieuprawnionej.

Zgodnie z art. 33 RODO w przypadku naruszenia danych osobowych, placówka medyczna bez zbędnej zwłoki – nie później niż w ciągu 72 godzin po stwierdzeniu naruszenia – musi zgłosić to organowi nadzorczemu (chyba, że jest mało prawdopodobne, aby naruszenie danych skutkowało ryzykiem naruszenia praw i wolności osób fizycznych). Termin 72 godzin jest bardzo restrykcyjny – za opóźnienie zgłoszenia grożą kary.

## Roszczenia cywilne pacjentów związane z naruszeniem ich danych osobowych

Zgodnie z art. 82 RODO i art. 92 ustawy o ochronie danych osobowych wprowadzono prawo do wystąpienia z nowym roszczeniem cywilnym – żądaniem zaniechania naruszania danych osobowych lub/i podjęcia działań niezbędnych do usunięcia jego skutków. Dochodzenie tych roszczeń w trybie cywilnym następuje przed właściwym sądem okręgowym.

Według RODO każdy pacjent ma prawo do pełnej rekompensaty szkody, tj. zarówno szkody materialnej, jak i niematerialnej – poniesionej na skutek naruszenia jego danych osobowych.

Na chwilę obecną nie ma jeszcze orzecznictwa w tym zakresie, dlatego nie wiadomo, jak sądy będą oceniały takie roszczenia.

## Najczęstsze błędy

Kontrole Urzędu Ochrony Danych Osobowych (UODO) wcześniej Generalnego Inspektora Ochrony Danych Osobowych (GIODO) wskazywały na najczęstsze naruszenia ochrony danych osobowych, jakie popełniają placówki medyczne. Te najczęstsze błędy to:

- wywoływanie pacjentów „po nazwisku" – zgodnie z wytycznymi UODO wywoływanie pacjenta może nastąpić poprzez: podanie imienia oraz godziny wizyty lub/i numeru gabinetu, identyfikację po nadanym numerze czy numeracji elektronicznej,
- udzielanie informacji o stanie zdrowia przez telefon – brak mechanizmów weryfikacji tożsamości pacjenta,
- obieg recept – brak upoważnienia dla rejestratorek, błędny proces przekazywania, przechowywania recept – recepty są ogólnie dostępne,
- brak prowadzenia rejestru udostępniania historii chorób,
- brak prowadzenia rejestru wydawania historii chorób,
- brak ewidencji osób upoważnionych do przetwarzania danych osobowych (ewidencja jako odrębny dokument),
- umieszczanie danych osobowych na szpitalnych łóżkach,
- nieprawidłowe upoważnienia do przetwarzania danych (np. dla salowych i sanitariuszy),
- przechowywanie dokumentacji medycznej w ogólnie dostępnych szafach,
- brak odpowiednich zabezpieczeń informatycznych dla dokumentacji w postaci elektronicznej.

## Podsumowanie

Placówki medyczne – z uwagi na przetwarzanie danych szczególnych kategorii – mają obowiązek wdrożenia i przestrzegania przepisów o ochronie danych osobowych. Jednocześnie duży nacisk należy położyć na szkolenia personelu, które także są obowiązkiem każdego pracodawcy (placówki medycznej) i elementem wdrażania RODO.

Wobec możliwych kar oraz roszczeń pacjentów jest to niezbędne. Przy tym trzeba pamiętać, że ubezpieczenie lekarzy od odpowiedzialności cywilnej nie obejmuje roszczeń z tytułu naruszenia danych osobowych oraz przepisów o ochronie danych osobowych.

Po ostatniej kontroli NIK i stwierdzeniu poważnych naruszeń zasad ochrony danych osobowych w placówkach me-

dycznych, należy uznać, że nadal dane osobowe pacjentów nie są odpowiednio chronione.

**Konflikt interesów:** nie zgłoszono

**Hanna Rubaszewska**
*BSJP Brockhuis Jurczak Prusak Sroka Nilsson*
*ul. Iłłakowiczówny 11*
*60-789 Poznań*
*e-mail: hanna.rubaszewska@bsjp.pl*

*Received and accepted: 5 Nov 2019*

## Piśmiennictwo

1. Ustawa z dnia 15.04.2011 o działalności leczniczej (Dz.U. z 2018, poz. 2190 z późn. zm.).
2. Ustawa z dnia 06.11.2008 o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. z 2016, poz. 186 z późn. zm.).
3. Ustawa z dnia 05.12.1996 o zawodach lekarza i lekarza dentysty (Dz.U z 2019, poz. 537 z późn. zm.).
4. Rozporządzenie Ministra Zdrowia z dnia 09.11.2015 w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. 2015, poz. 2069 z późn. zm.)
5. Ustawa o szczepieniach ochronnych, przepisy regulujące zasady prowadzenia profilaktyki chorób w ramach POZ lub realizacji Narodowych Programów do Walki z Chorobami Nowotworowymi.