



FIC Szkolenia -Ignacy Chruszczyński

Naruszenia ochrony danych w podmiocie leczniczym – postępowanie, ocena ryzyka i obowiązki administratora

Online 18 listopada 2026r.

Ostatnie tygodnie pokazały, że wyciek danych nie jest już zdarzeniem wyjątkowym. W krótkim czasie doszło do czterech poważnych incydentów bezpieczeństwa. Dla podmiotów leczniczych ryzyko jest szczególne – przetwarzają dane dotyczące zdrowia, dokumentację medyczną i informacje objęte tajemnicą zawodową. Do naruszenia może dojść także u dostawcy oprogramowania lub innego podmiotu przetwarzającego. To jednak podmiot leczniczy jako administrator musi wiedzieć, jak zareagować: ustalić zakres zdarzenia, ocenić ryzyko, zdecydować o zgłoszeniu do UODO i ewentualnym zawiadomieniu pacjentów. Podczas szkolenia pokażemy krok po kroku, co zrobić od chwili otrzymania informacji o incydencie aż do jego prawidłowego udokumentowania i zamknięcia. To nie będzie kolejne ogólne szkolenie z RODO. Ma przygotować Państwa na sytuację, w której przychodzi wiadomość: „doszło do wycieku danych” – i trzeba wiedzieć, co zrobić dalej.

I. Naruszenie ochrony danych w podmiocie leczniczym – jak rozpoznać problem? Incydent bezpieczeństwa a naruszenie ochrony danych osobowych – podstawowe różnice.

1. Naruszenie poufności, integralności i dostępności danych.
2. Przykładowe zdarzenia w szpitalu i przychodni:
 - 1) cyberatak na system informatyczny podmiotu leczniczego;
 - 2) wyciek danych u dostawcy oprogramowania lub innego podmiotu przetwarzającego;
 - 3) atak ransomware – zaszyfrowanie lub zablokowanie dostępu do dokumentacji;
 - 4) omyłkowe przekazanie dokumentacji medycznej niewłaściwej osobie;
 - 5) utrata komputera, telefonu lub innego nośnika zawierającego dane;
 - 6) nieuprawniony dostęp pracownika do dokumentacji medycznej;
 - 7) niewłaściwe udostępnienie dokumentacji medycznej lub danych pacjenta.
3. Czy każdy incydent bezpieczeństwa jest naruszeniem RODO?
4. Kto w podmiocie leczniczym powinien otrzymać informację o incydencie?
5. Pierwsze działania po stwierdzeniu naruszenia – zabezpieczenie danych i dowodów.

II. Szczególny charakter danych przetwarzanych przez podmioty lecznicze

1. Dane dotyczące zdrowia jako szczególna kategoria danych – art. 9 RODO.
2. Jakie informacje mogą stanowić dane dotyczące zdrowia?
3. Dokumentacja medyczna, wyniki badań, diagnostyka obrazowa, informacje o świadczeniach, e-receptach i skierowaniach.



FIC Szkolenia Ignacy Chruszczyński
Biuro Szkoleń: ul. Kinowa 18/80 04-017 Warszawa
tel: 601 35 44 88 **fax:** 0 22 292 38 50

e-mail: fic-szkolenia@data.pl www.fic-szkolenia.home.pl
<https://www.facebook.com/FIC-Szkolenia-114573930240521/>

NIP: 712-005-13-92 **REGON:** 430044616

4. Dane zawarte w systemach administracyjnych, finansowych i rozliczeniowych – kiedy również mogą ujawniać informacje o zdrowiu?
5. Tajemnica zawodowa osób wykonujących zawody medyczne.
6. Prawo pacjenta do zachowania w tajemnicy informacji z nim związanych.
7. Obowiązek poufności pracowników administracyjnych i innych osób mających dostęp do danych pacjentów.
8. Naruszenie tajemnicy zawodowej jako element oceny skutków naruszenia ochrony danych.
9. Czy ujawnienie danych medycznych zawsze oznacza wysokie ryzyko dla praw i wolności pacjenta?

III. Od informacji o incydencie do decyzji administratora – kto odpowiada i co powinien zrobić?

1. Podmiot leczniczy jako administrator danych.
2. Kierownik podmiotu leczniczego, IOD, dział IT, personel medyczny – podział zadań po wykryciu incydentu.
3. Rola inspektora ochrony danych.
4. Dostawca systemu informatycznego jako podmiot przetwarzający – jego obowiązki wobec administratora.
5. Incydent u dostawcy zewnętrznego – dlaczego podmiot leczniczy nadal musi dokonać własnej oceny?
6. Jakich informacji żądać od dostawcy oprogramowania po stwierdzeniu wycieku?
7. Dokumentowanie czynności podejmowanych od chwili uzyskania informacji o incydencie.

IV. Ocena ryzyka – od niej zależą dalsze obowiązki podmiotu leczniczego

1. Dlaczego każde naruszenie wymaga analizy, ale nie każde wymaga zgłoszenia Prezesowi UODO?
2. Ustalenie zakresu naruszenia.
3. Kryteria oceny ryzyka:
 - 1) rodzaj i charakter danych;
 - 2) szczególne kategorie danych;
 - 3) liczba pacjentów i innych osób objętych naruszeniem;
 - 4) możliwość identyfikacji osób;
 - 5) charakter i okoliczności zdarzenia;
 - 6) potencjalne konsekwencje dla pacjentów;
 - 7) szczególna sytuacja osób, których dane dotyczą;
 - 8) zastosowane zabezpieczenia.
4. Naruszenie tajemnicy zawodowej i poufności danych medycznych a poziom ryzyka.
5. Trzy możliwe konsekwencje przeprowadzonej analizy:
 - 1) brak prawdopodobieństwa ryzyka – dokumentujemy naruszenie;
 - 2) ryzyko dla praw lub wolności – zgłoszenie Prezesowi UODO;
 - 3) wysokie ryzyko – zgłoszenie oraz co do zasady zawiadomienie osób, których dane dotyczą.
6. Jak sporządzić ocenę ryzyka, aby można było wykazać prawidłowość podjętej decyzji?
7. Rejestr naruszeń – również wtedy, gdy incydentu nie zgłoszono Prezesowi UODO.

V. Obowiązki zgłoszeniowe – UODO, 72 godziny i inne kanały raportowania

1. Kiedy powstaje obowiązek zgłoszenia naruszenia Prezesowi UODO?
2. Termin 72 godzin – moment rozpoczęcia jego biegu.
3. Co zrobić, jeżeli administrator nie zna jeszcze wszystkich okoliczności zdarzenia?
4. Zgłoszenie wstępne i możliwość sukcesywnego przekazywania informacji.
5. Elementy zgłoszenia naruszenia.
6. Jak uzasadnić decyzję o niezgłoszeniu incydentu?
7. Czy zgłoszenie dokonane przez dostawcę systemu zwalnia podmiot leczniczy z własnych obowiązków?
8. Incydent cyberbezpieczeństwa a naruszenie ochrony danych – dwa różne reżimy prawne.
9. Zgłoszenia do właściwego CSIRT.



10. Obowiązki wynikające z przepisów o krajowym systemie cyberbezpieczeństwa – kiedy mogą dotyczyć podmiotu leczniczego?

VI. Pacjent po drugiej stronie naruszenia – kiedy i jak należy go zawiadomić?

1. Wysokie ryzyko dla praw i wolności osoby fizycznej – art. 34 RODO.
2. Kiedy administrator musi zawiadomić pacjenta?
3. Jakie informacje powinno zawierać zawiadomienie?
4. Prosty i zrozumiały język komunikatu – czego nie powinno zabraknąć?
5. Wybór sposobu kontaktu z pacjentem.
6. E-mail, SMS, korespondencja tradycyjna – praktyczne problemy.
7. Brak aktualnych danych kontaktowych – co powinien zrobić podmiot leczniczy?
8. Publiczny komunikat na podstawie art. 34 ust. 3 lit. c RODO.
9. Jak informować o naruszeniu, aby samo zawiadomienie nie spowodowało kolejnego ujawnienia informacji o stanie zdrowia?

VII. Kontrola UODO i odpowiedzialność podmiotu leczniczego

1. Rola Prezesa UODO po zgłoszeniu naruszenia.
2. Jak może przebiegać postępowanie przed organem nadzorczym?
3. Jakich dokumentów może zażądać Prezes UODO?
4. Znaczenie dokumentacji oceny ryzyka i rejestru naruszeń.
5. Administracyjne kary pieniężne – przesłanki ich nakładania.
6. Specyfika odpowiedzialności publicznych podmiotów leczniczych.
7. Odpowiedzialność cywilna – art. 82 RODO.
8. Szkoda majątkowa i niemajątkowa pacjenta.
9. Naruszenie RODO a naruszenie prawa pacjenta do tajemnicy informacji z nim związanych.
10. Odpowiedzialność za działania pracowników i podmiotów przetwarzających.

Czas trwania 120 minut

PRELEGENTKA: Agnieszka Sienko, radca prawny, interwent kryzysowy, mediator sądowy, coach, szkoleniowiec. Od 26 lat pracuje dla medycyny. Autorka kilku książek, znaczącej liczby artykułów – w tym naukowych, ostatnio pisząca felietony poświęcone aktualnym wydarzeniom w świecie medycznym.

CENA:

350zł netto*

* dla jednostek finansujących udział w szkoleniu w minimum 70% lub w całości ze środków publicznych stawka podatku VAT = zw.

POCZATEK ZAJĘĆ: 10:00

ZGŁOSZENIA:

Wypełnione karty prosimy przesłać za pomocą poczty elektronicznej na adres:

fic-szkolenia@data.pl

WPŁATY:

FIC Szkolenia – Ignacy Chruszczyński

Nr r-ku: mbank 79 1140 2004 0000 3002 2579 5347

Kontakt do Organizatora:

601 35 44 88



FIC Szkolenia Ignacy Chruszczyński

Biuro Szkoleń: ul. Kinowa 18/80 04-017 Warszawa

tel: 601 35 44 88 **fax:** 0 22 292 38 50

e-mail: fic-szkolenia@data.pl www.fic-szkolenia.home.pl

<https://www.facebook.com/FIC-Szkolenia-114573930240521/>

NIP: 712-005-13-92 **REGON:** 430044616



KARTA ZGŁOSZENIA

Naruszenia ochrony danych w podmiocie leczniczym – postępowanie, ocena ryzyka i obowiązki administratora

Online 18 listopada 2026r.

IMIĘ I NAZWISKO:.....

STANOWISKO:.....

NAZWA JEDNOSTKI NA FAKTURĘ (DOKŁADNA NAZWA I ADRES):.....

.....

.....

NIP:..... TEL.:..... TEL.KOM.:..... FAX:.....

..... E-MAIL.....

☐ Oświadczam, że udział ww. osób w szkoleniu finansowany jest ze środków publicznych w rozumieniu Ustawy o finansach publicznych

PŁATNOŚĆ ZA SZKOLENIE: PRZELEWEM -przed szkoleniem

Nr konta: nr r-ku: mbank 79 1140 2004 0000 3002 2579 5347

UPOWAŻNIAM FIC Szkolenia DO WYSTAWIENIA FAKTURY VAT BEZ PODPISU OSOBY ODBIERAJĄCEJ.
PRZY REZYGNACJI PÓŹNIEJ NIŻ 7 DNI ROBOCZYCH OD DATY ROZPOCZĘCIA SZKOLENIA LUB NIEOBECNOŚCI
ZGŁOSZONEGO UCZESTNIKA PONOSIMY KOSZTY SZKOLENIA

.....
pieczętka firmowa

.....
pieczętka imienna dyrektora
lub głównego księgowego

.....
podpis dyrektora
lub głównego księgowego



FIC Szkolenia Ignacy Chruszczyński
Biuro Szkoleń: ul. Kinowa 18/80 04-017 Warszawa
tel: 601 35 44 88 **fax:** 0 22 292 38 50
e-mail: fic-szkolenia@data.pl www.fic-szkolenia.home.pl
<https://www.facebook.com/FIC-Szkolenia-114573930240521/>
NIP: 712-005-13-92 **REGON:** 430044616