POSTĘPOWANIE PO NARUSZENIU

Co powinien zrobić gabinet korzystający z systemu MyDr

Przewodnik dla lekarzy i podmiotów leczniczych występujących w roli administratora danych osobowych. Kolejność czynności, terminy, wzory pism i formularze.

stan na 12 sierpnia 2026 r.
wydanie pierwsze

ZAKRES OPRACOWANIA

Przewodnik obejmuje wyłącznie stronę praktyczną: co, w jakiej kolejności i w jakim terminie należy zrobić. Nie zawiera opisu przebiegu incydentu ani jego analizy technicznej.

Niniejszy przewodnik ma charakter wyłącznie pomocniczy. Stanowi materiał porządkujący kolejność czynności oraz terminy, nie zastępuje natomiast wewnętrznych regulacji obowiązujących u administratora – w szczególności polityki ochrony danych, procedury reagowania na naruszenia ani przyjętej metodyki analizy ryzyka.

Administrator, który dysponuje własną procedurą analizy ryzyka lub oceny skutków dla ochrony danych, przeprowadza ją zgodnie z tą procedurą. Formularze i propozycje sformułowań zawarte w załącznikach mają charakter wzorcowy i wymagają dostosowania do stanu faktycznego oraz do dokumentacji obowiązującej w danej placówce.

Za ocenę zdarzenia, kwalifikację naruszenia, decyzję o zgłoszeniu organowi nadzorczemu oraz o zawiadomieniu osób, których dane dotyczą, a także za sposób i terminowość wykonania tych obowiązków, odpowiada indywidualnie każdy administrator. Odpowiedzialności tej nie wyłącza ani nie ogranicza posłużenie się niniejszym opracowaniem.

Materiał odzwierciedla stan faktyczny i prawny na dzień 12 sierpnia 2026 r. Postępowanie wyjaśniające dostawcy oprogramowania oraz czynności organów nie zostały zakończone; kolejne ustalenia mogą wymagać uzupełnienia zgłoszeń oraz weryfikacji przyjętych ocen. Opracowanie nie stanowi porady prawnej w indywidualnej sprawie, nie stanowi też podstawy do formułowania przez administratorów dotkniętych naruszeniem pytań o interpretację w indywidualnych przypadkach.

WPROWADZENIE

Jak korzystać z przewodnika

Punkt wyjścia jest jeden: administratorem danych pacjentów jest gabinet, praktyka albo przychodnia, a nie dostawca oprogramowania. Naruszenie wystąpiło w infrastrukturze dostawcy, lecz obowiązki wobec organu nadzorczego i wobec pacjentów obciążają placówkę. Nikt nie wykona ich w jej zastępstwie.

Materiał podzielono na sześć etapów uporządkowanych chronologicznie. Terminy liczone są od dnia stwierdzenia naruszenia, oznaczonego dalej literą D. Za dzień D przyjmuje się dzień, w którym placówka powzięła wiarygodną informację o incydencie – w praktyce dzień wpływu wiadomości od dostawcy – a nie dzień ustalenia pełnego zakresu zdarzenia.

> ZANIM ZACZNIEMY
>
> *Zanim przejdą Państwo dalej: proszę odszukać w skrzynce pocztowej wiadomość od dostawcy systemu i zapisać jej datę oraz godzinę. Warto sprawdzić także folder wiadomości niechcianych (SPAM). Od tej daty biegną wszystkie terminy opisane niżej, a jej ustalenie będzie pierwszą rzeczą, o którą zapyta organ nadzorczy.*

Mapa etapów

Etap	Przedmiot	Termin	Rezultat
I	Uruchomienie procedury, zabezpieczenie dowodów, ustalenie ekspozycji	D – D+1	Log postępowania, komplet dowodów, wykaz danych
II	Zabezpieczenie dostępu do systemu	D – D+3	Nowe hasła, 2FA, przegląd uprawnień, własna kopia danych
III	Zgłoszenie do Prezesa UODO	do D+3 (72 godziny)	Potwierdzenie zgłoszenia, wpis do rejestru naruszeń
IV	Zawiadomienie pacjentów	bez zbędnej zwłoki	Wysłane zawiadomienia, komunikat publiczny
V	Obowiązki sektorowe i wystąpienie do dostawcy	D+2 – D+14	Zgłoszenia sektorowe, wezwanie do dostawcy
VI	Wnioski systemowe	D+30 – D+60	Zaktualizowana analiza ryzyka, procedury, szkolenie

Załączniki od 1 do 8 zawierają gotowe do wypełnienia formularze, wzory pism oraz materiały przeznaczone dla pacjentów i dla personelu rejestracji. Do każdego etapu odsyłamy w treści.

ETAP I

Pierwsza doba

1. Uruchomienie procedury

1. Odnotować datę i godzinę uruchomienia wewnętrznej procedury reagowania na naruszenie ochrony danych.
2. Zawiadomić inspektora ochrony danych. Jeżeli w placówce go nie wyznaczono – wskazać imiennie osobę koordynującą sprawę.
3. Zawiadomić kierownika podmiotu leczniczego. Decyzja o zgłoszeniu naruszenia należy do administratora, a nie do inspektora; inspektor ją przygotowuje i opiniuje.
4. Założyć chronologiczny log postępowania: data, godzina, opis czynności, osoba wykonująca. To najprostszy sposób wykazania staranności i najczęściej pomijany.

2. Zabezpieczenie dowodów

Dowody należy zabezpieczyć od razu, ponieważ strony internetowe bywają aktualizowane, a regulaminy zmieniane jednostronnie przez dostawcę.

- Wiadomość od dostawcy – zapisać jako plik źródłowy (.eml albo .msg), z nagłówkami, nie jako wydruk ani zrzut ekranu.
- Komunikat dostawcy publikowany pod adresem pro.mydr.pl/portal-info wraz z sekcją pytań i odpowiedzi – zapisać do pliku PDF z widoczną datą pobrania.
- Komunikaty Ministerstwa Cyfryzacji z 10 i 12 sierpnia 2026 r. – zarchiwizować w ten sam sposób.
- Regulamin świadczenia usług oraz umowę powierzenia w brzmieniu obowiązującym w okresie objętym naruszeniem (a także podpisane przy zawieraniu umowy z dostawcą usługi MyDr, z umową o świadczenie usług), wraz z załącznikiem określającym zakres powierzonych danych i listą dalszych podmiotów przetwarzających.
- Faktury albo potwierdzenia płatności dokumentujące okres korzystania z systemu.

3. Ustalenie własnej ekspozycji

Zakres obowiązków placówki zależy od tego, jakie dane i za jaki okres znajdowały się w systemie. Ustalenia wymagają następujące okoliczności.

Co ustalić	Dlaczego to istotne
Data rozpoczęcia korzystania z systemu	Naruszenie objęło dane historyczne do kwietnia 2024 r. Rozpoczęcie współpracy po tej dacie może oznaczać brak ekspozycji – wymaga to jednak pisemnego potwierdzenia dostawcy, a nie własnego domysłu.
Data zakończenia korzystania, jeżeli placówka już z systemu nie korzysta	Umowa powierzenia przewiduje przechowywanie danych jeszcze przez rok po zakończeniu usług. Placówki, które odeszły od dostawcy, mogą być objęte naruszeniem.
Przybliżona liczba pacjentów w bazie w okresie do kwietnia 2024 r.	Element obowiązkowy zgłoszenia do organu nadzorczego.
Wykaz wykupionych modułów	Rozliczenia z NFZ, powiadomienia i kampanie SMS, zwolnienia lekarskie, integracja z Platformą P1, asystent notatek, portal pacjenta – każdy moduł poszerza katalog danych.

Czy wykonywano import danych z poprzedniego oprogramowania	Import mógł wprowadzić do systemu dane pacjentów sprzed rozpoczęcia współpracy, w tym pacjentów już nieaktywnych.
Czy w systemie umieszczono certyfikat ZUS albo inny materiał kryptograficzny placówki	Jeżeli tak – należy wystąpić o ponowne wydanie certyfikatu. Ten punkt bywa pomijany, a dotyczy poświadczeń umożliwiających wystawianie zwolnień.
Wykaz osób z personelu posiadających konta w okresie objętym naruszeniem	Dane personelu również zostały powierzone: numer prawa wykonywania zawodu, dane logowania, w części przypadków numer PESEL.

> **BRAK POWIADOMIENIA OD DOSTAWCY**
>
> *Jeżeli placówka nie otrzymała od dostawcy żadnej wiadomości, nie oznacza to, że naruszenie jej nie dotyczy. Za dzień D przyjmuje się wówczas dzień powzięcia informacji z innego źródła, na przykład z komunikatu Ministerstwa Cyfryzacji z 12 sierpnia 2026 r. Okoliczność braku powiadomienia należy odnotować w rejestrze naruszeń i podnieść w wystąpieniu do dostawcy.*

ETAP II

Zabezpieczenie dostępu

Czynności z tego etapu mają dwa cele: ograniczyć skutki zdarzenia oraz wykazać, że placówka zareagowała aktywnie. Drugi z nich bywa niedoceniany, a to on decyduje o ocenie organu nadzorczego w razie kontroli.

4. Konta i uprawnienia

1. Wymusić zmianę haseł wszystkich użytkowników konta placówki. Sprawdzić, czy te same hasła nie były używane w innych serwisach – jeżeli były, zmienić je również tam.
2. Włączyć uwierzytelnianie dwuskładnikowe, jeżeli funkcja jest dostępna, a nie została dotąd uruchomiona. Do czasu, gdy dostawca uczyni ją obowiązkową, decyzja należy do placówki, a jej zaniechanie po incydencie będzie oceniane surowo.
3. Przejrzeć listę użytkowników i odebrać dostęp osobom, które zakończyły współpracę. Za zarządzanie dostępami odpowiada wyłącznie placówka, nie dostawca.
4. Ograniczyć korzystanie z oprogramowania zdalnego dostępu wykorzystywanego przez wsparcie techniczne dostawcy. Uruchamiać je wyłącznie na wyraźną prośbę, w obecności pracownika i wyłączać po zakończeniu sesji.
5. Wystąpić o ponowne wydanie certyfikatu ZUS, jeżeli był przechowywany w systemie.

5. Własna kopia danych

Dostawca zobowiązuje się wykonywać kopie bezpieczeństwa nie rzadziej niż raz w tygodniu i przechowywać wyłącznie ostatnią z nich. Dla dokumentacji medycznej, która podlega wieloletnim okresom przechowywania, jest to zabezpieczenie niewystarczające.

- Wykonać i zapisać poza systemem własną kopię danych z konta placówki.
- Ustalić stały cykl wykonywania takich kopii i wskazać osobę odpowiedzialną.
- Przechowywać kopie w sposób zaszyfrowany, w miejscu odrębnym od stanowisk roboczych.

ETAP III

Zgłoszenie do Prezesa UODO

6. Czy zgłoszenie jest obowiązkowe

Tak, jeżeli placówka korzystała z systemu w okresie objętym naruszeniem. Zwolnienie ze zgłoszenia przysługuje wyłącznie wtedy, gdy jest mało prawdopodobne, by naruszenie skutkowało ryzykiem dla praw lub wolności osób. W tej sprawie przesłanka ta nie zachodzi: naruszenie objęło dane o zdrowiu oraz numer PESEL, ma charakter nieodwracalny, a zbiór znajduje się w rękach osób żądających okupu.

Od zgłoszenia można odstąpić jedynie wówczas, gdy placówka dysponuje pisemnym potwierdzeniem dostawcy, że dane jej pacjentów nie znalazły się w zbiorze objętym incydentem. Potwierdzenie takie należy dołączyć do wpisu w rejestrze naruszeń. Ustne zapewnienie ani ogólny komunikat na stronie internetowej nie wystarczą.

> **NAJCZĘSTSZY BŁĄD**
> *Nie należy czekać na wyniki postępowania dostawcy. Obowiązek zgłoszenia powstaje z chwilą stwierdzenia naruszenia, a nie z chwilą ustalenia jego pełnego zakresu. Brakujące informacje uzupełnia się później, w trybie zgłoszenia uzupełniającego. Zwłoka w oczekiwaniu na komplet danych jest najczęstszym błędem popełnianym w takich sprawach.*

7. Jak zgłosić

1. Zgłoszenia dokonuje się elektronicznie – przez formularz udostępniony przez Urząd Ochrony Danych Osobowych, przez e-Doręczenia albo pismem opatrzonym podpisem kwalifikowanym lub zaufanym.
2. Zaleca się złożenie zgłoszenia wstępnego, ze wskazaniem, których informacji jeszcze nie ustalono i kiedy zostaną uzupełnione. Jest to rozwiązanie standardowe, a nie wyraz braku przygotowania.
3. Po otrzymaniu ustaleń od dostawcy złożyć zgłoszenie uzupełniające, powołując się na numer sprawy nadany zgłoszeniu pierwotnemu.
4. Jeżeli termin 72 godzin już upłynął – zgłosić niezwłocznie i wyjaśnić przyczynę opóźnienia. Rezygnacja ze zgłoszenia z powodu upływu terminu pogarsza sytuację placówki, nigdy jej nie poprawia.

8. Co wpisać w zgłoszeniu

Poniżej podano gotowe sformułowania odpowiadające okolicznościom tej sprawy. Wymagają uzupełnienia wyłącznie w zakresie danych własnych placówki.

Pole zgłoszenia	Proponowana treść
Charakter naruszenia	Naruszenie poufności. Nieuprawniony dostęp i pobranie danych ze środowiska podmiotu przetwarzającego, któremu administrator powierzył przetwarzanie na podstawie umowy powierzenia. Naruszenie nie wystąpiło w infrastrukturze administratora.
Kategorie osób	Pacjenci, byli i przyszli pacjenci, przedstawiciele ustawowi osób małoletnich, osoby upoważnione do wglądu do dokumentacji medycznej, personel placówki posiadający konta w systemie.

Liczba osób	Liczba pacjentów placówki figurujących w bazie w okresie do kwietnia 2024 r. Przy braku możliwości ustalenia liczby dokładnej – przedział, z zaznaczeniem, że pochodzi z własnych rejestrów administratora.
Kategorie danych	Imię i nazwisko, numer PESEL, data urodzenia, dane kontaktowe i adresowe, oddział wojewódzki NFZ, dane o stanie zdrowia (rozpoznania, wystawione recepty, historia wizyt, zalecenia), dane z systemu eWUŚ, dane zwolnień lekarskich.
Możliwe konsekwencje	Kradzież tożsamości i zaciągnięcie zobowiązań finansowych na dane pacjenta; ukierunkowane oszustwa telefoniczne i wiadomości podszywające się pod placówkę, aptekę, NFZ lub bank, wykorzystujące wiedzę o stanie zdrowia i przyjmowanych lekach; ujawnienie informacji objętych tajemnicą zawodową; ryzyko stygmatyzacji wobec danych o uzależnieniach, chorobach zakaźnych, ciąży i zdrowiu psychicznym; szkoda niemajątkowa polegająca na utracie kontroli nad danymi.
Środki zastosowane	Po stronie administratora: zmiana danych uwierzytelniających, uruchomienie uwierzytelniania dwuskładnikowego, przegląd uprawnień, wystąpienie do podmiotu przetwarzającego, zawiadomienie pacjentów. Po stronie podmiotu przetwarzającego, zgodnie z jego komunikatem: odłączenie zaatakowanej struktury, zaangażowanie zewnętrznych ekspertów, zawiadomienie organów ścigania.

Ocenę ryzyka, na której opiera się zgłoszenie, dokumentuje się na formularzu stanowiącym załącznik nr 7. Sam wpis do rejestru naruszeń – załącznik nr 3.

ETAP IV

Zawiadomienie pacjentów

9. Kiedy zawiadomienie jest obowiązkowe

Zawiadomienie pacjentów jest obowiązkowe, gdy naruszenie może powodować wysokie ryzyko dla ich praw lub wolności. W tej sprawie przesłanka ta jest spełniona. Przemawiają za tym: objęcie danych o zdrowiu, objęcie numeru PESEL, skala zdarzenia, kontekst żądania okupu oraz to, że dane nie były zaszyfrowane w sposób uniemożliwiający ich odczytanie.

10. W jaki sposób zawiadomić

Rekomendujemy model mieszany, który zabezpiecza także tych pacjentów, do których placówka nie ma aktualnych danych kontaktowych.

- Zawiadomienie indywidualne – kanałem, którym placówka zwykle komunikuje się z pacjentem: pocztą elektroniczną, wiadomością SMS odsyłającą do pełnej treści, przez konto pacjenta. Wzór stanowi załącznik nr 4.
- Komunikat publiczny – na stronie internetowej oraz wywieszony w widocznym miejscu w rejestracji. Wzór stanowi załącznik nr 6.
- Materiał informacyjny do wręczenia pacjentom przy okienku – załącznik nr 5.
- Udokumentowanie sposobu i daty wykonania zawiadomienia dla każdego z kanałów. Sam fakt wysłania trzeba umieć wykazać.

> **FORMA ZAWIADOMIENIA**
>
> *Zawiadomienie nie może stać się narzędziem w rękach oszustów. Po ujawnieniu incydentu należy spodziewać się fali wiadomości podszywających się pod placówki medyczne.*
>
> *Dlatego zawiadomienie nie powinno zawierać: odnośników do formularzy wymagających logowania, żądania potwierdzenia tożsamości, prośby o podanie numeru PESEL, danych karty płatniczej ani jakichkolwiek haseł, a także załączników wykonywalnych.*
>
> *Warto natomiast wprost napisać, że placówka nigdy nie zwraca się o takie dane drogą elektroniczną, i podać oficjalny numer telefonu do weryfikacji autentyczności korespondencji.*

11. Czego nie mówić

Personel rejestracji jest pierwszym punktem kontaktu i to jemu pacjenci zadadzą pytania. Jednolity, zgodny z prawdą przekaz przygotowano w postaci skryptu stanowiącego załącznik nr 8. Trzy zasady są nienegocjowalne.

- Nie zapewniać, że nic się nie stało, ani nie bagatelizować zdarzenia.
- Nie potwierdzać i nie zaprzeczać okolicznościom, które nie zostały ustalone; nie podawać liczb.
- Nie weryfikować tożsamości pacjenta przez telefon wyłącznie na podstawie numeru PESEL. Ten numer mogą znać obecnie osoby nieuprawnione – należy stosować weryfikację wielopoziomową.

ETAP V

Obowiązki sektorowe i rozliczenie dostawcy

12. Zgłoszenia poza organem nadzorczym

Adresat	Zakres i termin
CERT Polska	Zgłoszenie incydentu przez formularz incydent.cert.pl. Zalecane niezależnie od statusu placówki, do D+3.
Właściwy CSIRT – krajowy system cyberbezpieczeństwa	Znowelizowana ustawa obowiązuje od 3 kwietnia 2026 r. i objęła sektor ochrony zdrowia. Model opiera się na samoidentyfikacji: placówka sama ocenia, czy jest podmiotem kluczowym albo ważnym. Jeżeli tak – obsługa i zgłoszenie incydentu w trybie ustawowym.
Centrum e-Zdrowia	Zalecane dla podmiotów działających w systemie ochrony zdrowia, zwłaszcza zintegrowanych z Platformą P1.
Oddział wojewódzki NFZ	Sprawdzić, czy zawarta umowa przewiduje obowiązek notyfikacji incydentów bezpieczeństwa. Ocenić wpływ zdarzenia na terminowość sprawozdawczości.
Rzecznik Praw Pacjenta	Zgłoszenie nie jest wymagane, lecz warto przygotować stanowisko placówki na wypadek wystąpienia Rzecznika. Naruszenie poufności dokumentacji dotyka prawa pacjenta do zachowania tajemnicy.

> **TERMINY USTAWOWE**
>
> *Niezależnie od bieżącego incydentu: termin złożenia wniosku o wpis do wykazu podmiotów kluczowych i ważnych upływa 3 października 2026 r., pełne wdrożenie obowiązków – 3 kwietnia 2027 r., pierwszy audyt – 3 kwietnia 2028 r. Placówka, która nie dokonała jeszcze samoidentyfikacji, powinna zrobić to teraz. W razie kontroli obie kwestie będą badane łącznie.*

13. Wystąpienie do dostawcy

Placówka nie jest w stanie prawidłowo indywidualnie zawiadomić pacjentów, dopóki nie otrzyma od dostawcy wykazu osób objętych naruszeniem (w pierwszej kolejności stosuje zawiadomienie publiczne). Wystąpienie należy skierować niezwłocznie, w postaci pisemnej, na adres inspektora ochrony danych dostawcy, zachowując potwierdzenie wysłania. Gotowe pismo stanowi załącznik nr 2 i obejmuje pięć grup zagadnień.

1. Ustalenie, czy dane pacjentów placówki znalazły się w zbiorze objętym naruszeniem, oraz przekazanie wykazu tych osób wraz z zakresem ujawnionych danych.
2. Okoliczności naruszenia: daty, przyczyna źródłowa, czas utrzymywania się dostępu, wywołane alerty.
3. Izolacja środowisk: czy naruszeniem objęte były także inne usługi dostawcy oraz kanały komunikacji z pacjentami, w tym bramki SMS.
4. Podstawa przechowywania danych historycznych i zachowanie terminów retencji.
5. Wykaz zastosowanych środków bezpieczeństwa, logi dostępu do konta placówki, zakres deklarowanego wsparcia oraz informacja o ubezpieczeniu odpowiedzialności cywilnej.

14. Uprawnienia placówki wobec dostawcy

- Żądanie wszelkich informacji niezbędnych do wykazania, że dostawca wywiązał się ze swoich obowiązków.
- Prawo do audytu lub inspekcji. Umowa ogranicza je do jednego audytu w roku, z zawiadomieniem na piśmie z czternastodniowym wyprzedzeniem i imiennym wskazaniem audytorów.
- Żądanie wsparcia w wykonaniu obowiązków związanych ze zgłoszeniem i zawiadomieniami.
- Żądanie wydania danych do pobrania w formacie nadającym się do odczytu maszynowego, w terminie do trzydziestu dni od złożenia wniosku.

15. Roszczenia

Umowa ogranicza odpowiedzialność dostawcy do kwoty wynagrodzenia zapłaconego w ciągu dwunastu miesięcy poprzedzających szkodę i rozciąga to ograniczenie wprost na przetwarzanie powierzonych danych. Trzy uwagi praktyczne.

1. Ograniczenie to nie działa wobec pacjentów. Wobec nich administrator i podmiot przetwarzający odpowiadają solidarnie, niezależnie od treści umowy.
2. Placówka, która wypłaci pacjentowi odszkodowanie, może następnie dochodzić zwrotu od dostawcy w części odpowiadającej jego odpowiedzialności. Roszczenie to warto zastrzec pisemnie już teraz.
3. Ograniczenie odpowiedzialności nie obejmuje szkody wyrządzonej umyślnie. Ocena, czy zachodzi rażące niedbalstwo, zależy od ustalenia przyczyny źródłowej – stąd znaczenie pytań z załącznika nr 2.

Odrębnie należy zgłosić żądanie pokrycia kosztów obsługi incydentu po stronie placówki: korespondencji z pacjentami, obsługi prawnej, ewentualnego audytu oraz ponownego wydania certyfikatów.

ETAP VI

Wnioski na przyszłość

Ostatni etap decyduje o tym, jak placówka wypadnie w razie kontroli. Orzecznictwo organu nadzorczego pokazuje, że kary są nakładane nie tyle za sam incydent, ile za brak rzetelnej analizy ryzyka i za nieprzygotowanie organizacyjne. Placówki audytowane regularnie traktowane są łagodniej nawet wtedy, gdy do naruszenia doszło.

16. Dokumentacja

1. Zaktualizować analizę ryzyka i ocenę skutków dla ochrony danych w części dotyczącej korzystania z zewnętrznego systemu dokumentacji medycznej. Analizę prowadzi się z perspektywy pacjenta, a nie placówki.
2. Zaktualizować rejestr czynności przetwarzania oraz rejestr kategorii czynności o aktualną listę dalszych podmiotów przetwarzających.
3. Uzupełnić procedurę reagowania na naruszenia o scenariusz naruszenia występującego po stronie dostawcy oprogramowania – z podziałem ról, wzorami pism i terminami. Ten scenariusz zwykle w procedurach brakuje.

17. Dostawcy

1. Wprowadzić okresową weryfikację dostawców. Minimalny zestaw pytań: certyfikaty systemu zarządzania bezpieczeństwem informacji, wyniki testów penetracyjnych, polityka zarządzania podatnościami, deklarowany czas powiadomienia o naruszeniu, zasady retencji danych po rozwiązaniu umowy.
2. Przy najbliższym przedłużeniu umowy dążyć do wprowadzenia konkretnego terminu powiadomienia o naruszeniu. Zapis mówiący wyłącznie o powiadomieniu niezwłocznym nie zabezpiecza placówki, która ma na zgłoszenie 72 godziny. Standardem rynkowym jest 24 albo 48 godzin.
3. Ustalić własny cykl wykonywania kopii danych, niezależny od kopii dostawcy.

18. Ludzie

1. Przeszkolić personel w rozpoznawaniu prób oszustwa wykorzystujących wiedzę o incydencie, ze szczególnym uwzględnieniem rejestracji.
2. Wprowadzić zasadę weryfikacji wielopoziomowej tożsamości pacjenta przy kontakcie telefonicznym.
3. Odnotowywać zgłoszenia pacjentów o próbach oszustwa – mogą okazać się materiałem dla organów ścigania oraz argumentem w sprawie przeciwko dostawcy.

ZAŁĄCZNIK NR 1

Check-lista czynności

Formularz do wypełnienia i przechowywania w aktach sprawy. Kolumnę „Termin" liczy się od dnia stwierdzenia naruszenia (D). Wypełniony arkusz stanowi dowód dochowania staranności.

	Czynność	Termin	Wykonano / data
A · USTALENIA			
1	Ustalenie i udokumentowanie daty oraz godziny wpływu wiadomości od dostawcy (plik źródłowy z nagłówkami)	D	☐
2	Ustalenie daty rozpoczęcia oraz – jeżeli dotyczy – zakończenia korzystania z systemu	D	☐
3	Ustalenie, czy placówka korzystała z systemu w okresie do kwietnia 2024 r.	D	☐
4	Ustalenie wykazu wykupionych modułów (NFZ, SMS, kampanie SMS, zwolnienia, P1, asystent notatek, portal pacjenta)	D	☐
5	Ustalenie przybliżonej liczby pacjentów w bazie w okresie objętym naruszeniem	D+1	☐
6	Ustalenie wykazu osób z personelu posiadających konta w tym okresie	D+1	☐
7	Ustalenie, czy w systemie umieszczono certyfikat ZUS albo inny materiał kryptograficzny	D+1	☐
B · DOWODY			
8	Archiwizacja wiadomości od dostawcy w formacie .eml albo .msg	D	☐
9	Archiwizacja komunikatu i sekcji pytań ze strony dostawcy (PDF z datą pobrania)	D	☐
10	Archiwizacja komunikatów Ministerstwa Cyfryzacji z 10 i 12 sierpnia 2026 r.	D	☐
11	Zabezpieczenie regulaminu i umowy powierzenia w brzmieniu z okresu naruszenia, wraz z załącznikami	D+1	☐
12	Założenie chronologicznego logu postępowania	D	☐
C · ZABEZPIECZENIE DOSTĘPU			

13	Wymuszenie zmiany haseł wszystkich użytkowników konta placówki	D	☐
14	Uruchomienie uwierzytelniania dwuskładnikowego	D	☐
15	Przegląd uprawnień i odebranie dostępu osobom, które zakończyły współpracę	D+2	☐
16	Ograniczenie i nadzór nad oprogramowaniem zdalnego dostępu wsparcia technicznego	D+2	☐
17	Wykonanie i zabezpieczenie własnej kopii danych z systemu	D+3	☐
18	Wystąpienie o ponowne wydanie certyfikatu ZUS, jeżeli był przechowywany w systemie	D+7	☐
D · ZGŁOSZENIA I ZAWIADOMIENIA			
19	Zawiadomienie inspektora ochrony danych i kierownika podmiotu leczniczego	D	☐
20	Przeprowadzenie i udokumentowanie oceny ryzyka (załącznik nr 7)	D+1	☐
21	Zgłoszenie naruszenia Prezesowi UODO – zgłoszenie wstępne	D+3	☐
22	Wpis do wewnętrznego rejestru naruszeń (załącznik nr 3)	D+3	☐
23	Zawiadomienie pacjentów (załącznik nr 4)	bez zwłoki	☐
24	Publikacja komunikatu na stronie i wywieszenie w rejestracji (załącznik nr 6)	bez zwłoki	☐
25	Przekazanie rejestracji skryptu odpowiedzi (załącznik nr 8)	D+3	☐
26	Zgłoszenie do CERT Polska	D+3	☐
27	Weryfikacja statusu placówki w krajowym systemie cyberbezpieczeństwa i zgłoszenie do CSIRT, jeżeli dotyczy	D+3	☐
28	Weryfikacja obowiązków wynikających z umowy z NFZ	D+5	☐
29	Zgłoszenie uzupełniające do UODO po otrzymaniu ustaleń dostawcy	niezwłocznie	☐
E · DOSTAWCA			
30	Wystąpienie do dostawcy (załącznik nr 2)	D+2	☐

31	Żądanie wykazu pacjentów objętych naruszeniem	D+2	☐
32	Żądanie wyjaśnienia podstawy przechowywania danych historycznych	D+2	☐
33	Pisemne zastrzeżenie roszczeń odszkodowawczych i regresowych	D+14	☐
34	Rozważenie audytu (zawiadomienie na 14 dni wcześniej)	D+30	☐

F · WNIOSKI SYSTEMOWE

35	Aktualizacja analizy ryzyka i oceny skutków dla ochrony danych	D+30	☐
36	Aktualizacja rejestru czynności i rejestru kategorii czynności	D+30	☐
37	Uzupełnienie procedury reagowania o scenariusz naruszenia u dostawcy	D+30	☐
38	Szkolenie personelu, w szczególności rejestracji	D+30	☐
39	Wdrożenie okresowej weryfikacji dostawców	D+60	☐
40	Wniosek o wpis do wykazu podmiotów kluczowych i ważnych	do 3.10.2026	☐

ZAŁĄCZNIK NR 2

Wystąpienie do dostawcy systemu

Pismo kierowane do inspektora ochrony danych dostawcy, z zachowaniem potwierdzenia wysłania.

……., dnia ……. 2026 r.

[nazwa podmiotu leczniczego, adres, numer w rejestrze podmiotów wykonujących działalność leczniczą, NIP, identyfikator konta w systemie]

MyDr sp. z o.o.
ul. Puławska 465, 02-844 Warszawa
Inspektor Ochrony Danych

Wezwanie do udzielenia informacji

w związku z naruszeniem ochrony danych osobowych powierzonych do przetwarzania

Działając jako administrator danych osobowych, w związku z incydentem bezpieczeństwa ujawnionym przez Państwa spółkę w dniu 10 sierpnia 2026 r. i potwierdzonym komunikatem Ministerstwa Cyfryzacji z dnia 12 sierpnia 2026 r., wzywam do udzielenia poniższych informacji w terminie trzech dni roboczych od doręczenia niniejszego pisma.

I. Ekspozycja administratora

1. Czy dane powierzone Państwu przez administratora – dane pacjentów, personelu oraz osób upoważnionych do wglądu do dokumentacji – znalazły się w zbiorze objętym nieuprawnionym dostępem?
2. Jeżeli tak, proszę o wykaz osób, których dane dotyczą, w zakresie umożliwiającym ich identyfikację przez administratora, wraz ze wskazaniem kategorii danych ujawnionych w odniesieniu do każdej z nich. Bez tego wykazu administrator nie jest w stanie wykonać obowiązku zawiadomienia pacjentów.
3. Proszę o wskazanie zakresu czasowego danych objętych incydentem, w szczególności o potwierdzenie, czy objął on wyłącznie dane do kwietnia 2024 r.

II. Okoliczności naruszenia

1. Data i godzina wystąpienia naruszenia oraz jego stwierdzenia przez Państwa spółkę.
2. Data, godzina i kanał przekazania administratorowi pierwszej informacji o naruszeniu.
3. Przyczyna źródłowa: podatność techniczna, błąd konfiguracji, błąd ludzki, działanie osoby posiadającej uprawniony dostęp czy inne zdarzenie.
4. Czy doszło do kompromitacji materiału kryptograficznego przekazanego Państwu przez administratora, w szczególności certyfikatu ZUS.
5. Jakie alerty systemowe zostały wywołane i z jakim skutkiem oraz jak długo utrzymywał się nieuprawniony dostęp.

III. Izolacja środowisk

1. Czy środowisko objęte incydentem było odseparowane – na poziomie sieci, tożsamości, poświadczeń i danych – od pozostałych usług świadczonych przez Państwa spółkę i podmioty z Państwa grupy, w tym od serwisu umawiania wizyt.

2. Czy incydent objął środowisko usługi asystenta notatek opartej na sztucznej inteligencji, w tym nagrania audio z wizyt, transkrypcje i wygenerowane notatki. Jeżeli nie – jakie środki to zapewniły.
3. Które z dalszych podmiotów przetwarzających wskazanych w załączniku do umowy powierzenia przetwarzały dane objęte incydentem.
4. Czy doszło do nieuprawnionego dostępu do kanałów komunikacji z pacjentami administratora, w tym do bramek wiadomości SMS, oraz czy istnieje ryzyko wysyłki wiadomości podszywających się pod administratora.

IV. Przechowywanie danych historycznych

1. Na jakiej podstawie i na podstawie jakiego udokumentowanego polecenia administratora przechowywali Państwo dane historyczne objęte incydentem.
2. Czy dane te znajdowały się w bieżącym środowisku produkcyjnym, czy w środowisku archiwalnym, i jakie środki bezpieczeństwa wobec niego stosowano.
3. Czy zachowano terminy usunięcia danych wynikające z umowy powierzenia.

V. Środki, dowody i wsparcie

1. Wykaz środków technicznych i organizacyjnych wdrożonych przed naruszeniem, w szczególności w zakresie szyfrowania danych przechowywanych, segmentacji sieci, zarządzania podatnościami, zarządzania kluczami i sekretami oraz monitorowania.
2. Wykaz środków wdrożonych po naruszeniu.
3. Logi dostępu do konta administratora za okres od …… do …… .
4. Zakres wsparcia, jakiego udzielą Państwo administratorowi przy wykonaniu obowiązków wobec organu nadzorczego i pacjentów.
5. Informacja, czy i w jakim zakresie zdarzenie objęte jest ubezpieczeniem odpowiedzialności cywilnej Państwa spółki.

Jednocześnie administrator zastrzega prawo przeprowadzenia audytu na zasadach określonych w umowie powierzenia oraz dochodzenia roszczeń odszkodowawczych i regresowych, w tym roszczenia o zwrot świadczeń wypłaconych osobom, których dane dotyczą.

……

podpis osoby uprawnionej do reprezentacji

ZAŁĄCZNIK NR 3

Wpis do rejestru naruszeń

Rejestr prowadzi się niezależnie od tego, czy naruszenie zgłoszono organowi nadzorczemu. W razie odstąpienia od zgłoszenia w rejestrze dokumentuje się uzasadnienie tej decyzji.

Pozycja	Treść
Sygnatura wpisu	
Data i godzina stwierdzenia naruszenia	
Źródło informacji	Powiadomienie dostawcy / komunikat publiczny / inne
Data wystąpienia naruszenia	Nieustalona – postępowanie wyjaśniające dostawcy w toku
Charakter naruszenia	Naruszenie poufności – nieuprawniony dostęp i pobranie danych ze środowiska podmiotu przetwarzającego
Miejsce naruszenia	Infrastruktura podmiotu przetwarzającego; nie wystąpiło w systemach administratora
Kategorie osób	Pacjenci obecni, byli i przyszli, przedstawiciele ustawowi, osoby upoważnione do wglądu do dokumentacji, personel
Przybliżona liczba osób	
Kategorie danych	Dane identyfikacyjne, PESEL, data urodzenia, dane kontaktowe i adresowe, oddział NFZ, dane o stanie zdrowia, dane eWUŚ, dane zwolnień lekarskich
Ocena ryzyka	Wysokie – uzasadnienie na formularzu z załącznika nr 7
Zastosowane środki	
Zgłoszenie do UODO	tak / nie – data, numer sprawy, forma (wstępne, uzupełniające)
Uzasadnienie odstąpienia od zgłoszenia	wypełnić wyłącznie w razie odstąpienia, ze wskazaniem dowodu braku ekspozycji
Zawiadomienie pacjentów	tak / nie – data, kanał, liczba zawiadomionych, sposób udokumentowania
Zgłoszenia sektorowe	CERT Polska / CSIRT / Centrum e-Zdrowia / NFZ – daty
Sporządzający wpis	
Załączniki	Korespondencja dostawcy, archiwum komunikatów, ocena ryzyka, potwierdzenie zgłoszenia, dowody zawiadomień

ZAŁĄCZNIK NR 4

Zawiadomienie pacjenta

Przed wysyłką usunąć uwagi redakcyjne ujęte w nawiasach kwadratowych.

[nagłówek placówki]

……., dnia …… 2026 r.

Zawiadomienie o naruszeniu ochrony danych osobowych

Szanowna Pani, Szanowny Panie,

jako administrator Pani lub Pana danych osobowych informujemy o naruszeniu ochrony danych, które może dotyczyć również Państwa.

Co się wydarzyło

Nasza placówka korzysta z systemu elektronicznej dokumentacji medycznej MyDr, dostarczanego przez MyDr sp. z o.o. z siedzibą w Warszawie. Spółka ta przetwarza dane naszych pacjentów na nasze zlecenie, na podstawie zawartej umowy.

W dniu 10 sierpnia 2026 r. dostawca poinformował nas, że w jego systemach osoba nieuprawniona uzyskała dostęp do danych. W dniu 12 sierpnia 2026 r. Ministerstwo Cyfryzacji potwierdziło nieuprawniony dostęp do danych historycznych gabinetów lekarskich przechowywanych w tych systemach.

Naruszenie nie wystąpiło w systemach naszej placówki i nie mogliśmy mu zapobiec. Jako administrator Państwa danych mamy jednak obowiązek Państwa o nim powiadomić.

Jakich danych może dotyczyć

- imienia i nazwiska, numeru PESEL, daty urodzenia,
- numeru telefonu, adresu poczty elektronicznej, adresu zamieszkania,
- oddziału wojewódzkiego Narodowego Funduszu Zdrowia,
- informacji dotyczących zdrowia, w tym o wystawionych receptach, przepisanych lekach, rozpoznaniach i historii wizyt.

[wariant po otrzymaniu wykazu od dostawcy: „W odniesieniu do Pani lub Pana danych naruszenie obejmuje: ……”]

Czym to grozi

- próbą zaciągnięcia kredytu, pożyczki albo zawarcia umowy abonamentowej na Państwa dane,
- telefonami i wiadomościami od osób podszywających się pod placówkę medyczną, aptekę, NFZ albo bank, powołujących się na wiedzę o Państwa wizytach lub lekach,
- ujawnieniem osobom nieuprawnionym informacji o stanie zdrowia objętych tajemnicą.

Co radzimy zrobić

Szczegółowe wskazówki zawiera załączony materiał. W pierwszej kolejności prosimy o zastrzeżenie numeru PESEL w aplikacji mObywatel, w banku, na poczcie albo w urzędzie gminy oraz o zachowanie ostrożności wobec wiadomości i telefonów dotyczących zdrowia, recept i płatności.

Co zrobiliśmy

[wskazać rzeczywiście podjęte działania, na przykład: wystąpiliśmy do dostawcy o ustalenie zakresu naruszenia i wykaz osób, których ono dotyczy; zgłosiliśmy naruszenie Prezesowi Urzędu Ochrony Danych Osobowych; zmieniliśmy dane logowania i uruchomiliśmy uwierzytelnianie dwuskładnikowe; zweryfikowaliśmy uprawnienia personelu]

Kontakt

Inspektor ochrony danych naszej placówki: …… (adres poczty elektronicznej, telefon). Informacji udziela także rejestracja pod numerem …… .

> **JAK ROZPOZNAĆ WIADOMOŚĆ OD NAS**
>
> *Nigdy nie prosimy o podanie numeru PESEL, hasła, kodu z wiadomości SMS ani danych karty płatniczej w wiadomości elektronicznej lub SMS. Nie wysyłamy odnośników do formularzy wymagających logowania. W razie wątpliwości co do autentyczności otrzymanej wiadomości prosimy o telefon pod oficjalny numer placówki: …… .*

Z wyrazami szacunku

……

podpis osoby uprawnionej do reprezentacji

ZAŁĄCZNIK NR 5

Wytyczne dla pacjentów

Materiał do wręczenia w rejestracji, dołączenia do zawiadomienia albo opublikowania na stronie placówki.

Wyciekły dane medyczne. Co teraz zrobić?

Krok pierwszy. Zastrzeż numer PESEL

To najważniejsze i zajmuje kilka minut. Zastrzeżenia dokonuje się w aplikacji mObywatel, na stronie gov.pl, w dowolnym urzędzie gminy, w placówce bankowej albo na poczcie.

Zastrzeżenie sprawia, że bank ani inna instytucja nie udzieli kredytu ani pożyczki na Państwa dane, nie zostanie założony nowy rachunek bankowy, notariusz nie sporządzi aktu notarialnego dotyczącego nieruchomości, operator nie wyda duplikatu karty SIM, a bank nie wypłaci w placówce gotówki powyżej trzykrotności minimalnego wynagrodzenia.

Zastrzeżenie nie utrudnia korzystania z opieki zdrowotnej. Nadal można umówić się do lekarza i zrealizować receptę.

> UWAGA PRAKTYCZNA
>
> *Jeżeli planują Państwo wypłatę większej kwoty gotówki w oddziale banku, zastrzeżenie trzeba cofnąć przed złożeniem dyspozycji. Cofnięcie go w trakcie nie pomoże, bo bank i tak wstrzyma wypłatę na dwanaście godzin.*

Krok drugi. Sprawdź, czy Twoje dane są w wycieku

Informacje o skradzionych danych mają być udostępniane w serwisie bezpiecznedane.gov.pl. Ponieważ administratorami danych są poszczególne gabinety i placówki, przekazanie informacji do tego serwisu może potrwać kilka dni.

Prosimy nie korzystać z serwisów obiecujących natychmiastowe sprawdzenie wycieku. Same mogą służyć wyłudzeniu danych.

Krok trzeci. Uważaj na telefony i wiadomości

Największe ryzyko pojawia się nie w chwili wycieku, lecz w kolejnych tygodniach i miesiącach. Wiadomości mogą wyglądać wiarygodnie, ponieważ ich autorzy mogą znać Państwa imię, nazwisko, numer PESEL, nazwę leku albo datę wizyty.

- Nie otwierać odnośników w wiadomościach dotyczących recept, wyników badań, dopłat, zwrotów ani weryfikacji danych.
- Nie podawać przez telefon numeru PESEL, hasła, kodu z wiadomości SMS ani danych karty płatniczej. Żadna placówka medyczna, bank ani NFZ o nie nie poprosi.
- Jeżeli rozmówca wywiera presję czasu albo odwołuje się do stanu zdrowia – rozłączyć się i oddzwonić na numer instytucji wyszukany samodzielnie, nigdy podany przez rozmówcę.
- Numer widoczny na wyświetlaczu telefonu może być sfałszowany.
- Nie instalować oprogramowania do zdalnego dostępu na prośbę osoby dzwoniącej.

Krok czwarty. Zabezpiecz konta

- Włączyć uwierzytelnianie dwuskładnikowe w bankowości elektronicznej, poczcie i Internetowym Koncie Pacjenta.

- Zmienić hasła, jeżeli to samo hasło było używane w kilku serwisach.
- Sprawdzać raporty w Biurze Informacji Kredytowej i w biurach informacji gospodarczej pod kątem zapytań kredytowych, których Państwo nie składali.
- Obserwować historię rachunku bankowego przez co najmniej kilka miesięcy.

Krok piąty. Reaguj

- Próbę oszustwa zgłosić do CERT Polska przez formularz incydent.cert.pl albo przesłać podejrzaną wiadomość SMS na numer 8080 – jest to bezpłatne.
- W razie faktycznej szkody złożyć zawiadomienie na Policji albo w prokuraturze.
- Jeżeli na Państwa dane zaciągnięto zobowiązanie – natychmiast zawiadomić instytucję finansową i zażądać wstrzymania wykonania umowy.

Krok szósty. Znaj swoje prawa

Mają Państwo prawo dowiedzieć się od placówki, jakiego zakresu danych dotyczy naruszenie, prawo dostępu do swoich danych, prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych oraz prawo dochodzenia odszkodowania przed sądem.

Prosimy o zachowanie spokoju. Sam fakt ujawnienia danych nie oznacza, że doszło do szkody. Wykonanie powyższych kroków, a przede wszystkim zastrzeżenie numeru PESEL, istotnie ogranicza ryzyko.

ZAŁĄCZNIK NR 6

Komunikat do rejestracji

Krótka forma przeznaczona do wywieszenia w widocznym miejscu przy rejestracji podmiotu.

Komunikat dla pacjentów

Szanowni Państwo, informujemy, że u dostawcy systemu elektronicznej dokumentacji medycznej, z którego korzysta nasza placówka – spółki MyDr – doszło do naruszenia bezpieczeństwa polegającego na uzyskaniu dostępu do danych przez osobę nieuprawnioną. Incydent potwierdziło Ministerstwo Cyfryzacji w dniu 12 sierpnia 2026 r.

Naruszenie nie wystąpiło w systemach naszej placówki. Podjęliśmy działania, do których jesteśmy zobowiązani jako administrator Państwa danych: wystąpiliśmy do dostawcy o ustalenie zakresu naruszenia, zgłosiliśmy sprawę Prezesowi Urzędu Ochrony Danych Osobowych i zabezpieczyliśmy dostęp do naszego konta.

Naruszenie może obejmować imię i nazwisko, numer PESEL, datę urodzenia, dane kontaktowe, oddział NFZ oraz informacje dotyczące zdrowia, w tym o wystawionych receptach i przebytych wizytach.

Co radzimy zrobić

1. Zastrzec numer PESEL – w aplikacji mObywatel, w banku, na poczcie albo w urzędzie gminy. Zajmuje to kilka minut.

2. Zachować ostrożność wobec telefonów i wiadomości dotyczących zdrowia, recept, badań i płatności.

3. Nie podawać nikomu numeru PESEL, hasła, kodu SMS ani danych karty płatniczej.

4. Sprawdzać w serwisie bezpiecznedane.gov.pl, czy Państwa dane znalazły się w wycieku.

Ważne

Nasza placówka nigdy nie prosi o podanie numeru PESEL, hasła ani danych karty płatniczej w wiadomości elektronicznej lub SMS. W razie wątpliwości prosimy o kontakt pod numerem: …… .

Pełne wytyczne dostępne są …… oraz pod adresem: …… . Kontakt do inspektora ochrony danych: …… .

ZAŁĄCZNIK NR 7

Formularz oceny ryzyka

Wypełniony formularz dokumentuje podstawę decyzji o zgłoszeniu naruszenia i o zawiadomieniu pacjentów.

Kryterium	Ustalenie	Wpływ na ocenę
Rodzaj naruszenia	Naruszenie poufności, trwała utrata kontroli nad danymi	podwyższa
Charakter danych	Dane o zdrowiu oraz numer PESEL	istotnie podwyższa
Łatwość identyfikacji osoby	Pełna – dane jawne, z imieniem, nazwiskiem i numerem PESEL	istotnie podwyższa
Zabezpieczenia techniczne	Brak – dane w ujawnionych próbkach nie były zaszyfrowane	wyłącza zwolnienie z zawiadomienia
Waga skutków	Kradzież tożsamości, oszustwa finansowe, ukierunkowane oszustwa telefoniczne, stygmatyzacja, ujawnienie tajemnicy zawodowej	wysoka
Cechy osób	W zbiorze mogą znajdować się osoby małoletnie, przewlekle chore, w ciąży, z rozpoznaniami wrażliwymi społecznie	podwyższa
Liczba osób	Do ustalenia w skali placówki	podwyższa
Odbiorca danych	Podmiot działający dla korzyści majątkowej, żądający okupu	istotnie podwyższa
Odwracalność skutków	Brak – numeru PESEL ani daty urodzenia nie można zmienić	istotnie podwyższa
Wniosek	**Ryzyko dla praw i wolności osób: wysokie. Zgłoszenie organowi nadzorczemu oraz zawiadomienie pacjentów – obowiązkowe.**	**wysokie**

Datę sporządzenia, imię i nazwisko osoby sporządzającej oraz podpis umieszcza się poniżej formularza.

ZAŁĄCZNIK NR 8

Skrypt dla rejestracji

Materiał wewnętrzny. Zapewnia jednolity przekaz i chroni przed wypowiedziami, które mogłyby zostać odczytane jako przyznanie okoliczności nieustalonych.

Pytanie pacjenta	Odpowiedź
Czy moje dane wyciekły?	Nie mamy jeszcze potwierdzonego wykazu osób, których dotyczy naruszenie. Czekamy na tę informację od dostawcy systemu i skontaktujemy się z Panią lub Panem, gdy tylko ją otrzymamy. Niezależnie od tego zalecamy zastrzeżenie numeru PESEL już teraz.
Czy to wina placówki?	Naruszenie nastąpiło w systemach firmy, która dostarcza nam oprogramowanie do dokumentacji medycznej, a nie w naszych systemach. Jako administrator Państwa danych mamy jednak obowiązek Państwa poinformować i to robimy.
Jakie dokładnie dane wyciekły?	Zgodnie z informacjami podanymi publicznie naruszenie może obejmować imię, nazwisko, numer PESEL, datę urodzenia, dane kontaktowe, oddział NFZ oraz informacje o receptach i wizytach. Dokładny zakres w Państwa przypadku ustalamy.
Co mam teraz zrobić?	Przede wszystkim zastrzec numer PESEL – w mObywatelu, w banku, na poczcie albo w urzędzie gminy. Zajmuje to kilka minut. Proszę też zachować ostrożność wobec telefonów i wiadomości dotyczących zdrowia i płatności. Przygotowaliśmy pisemne wskazówki, proszę bardzo. [wręczyć załącznik nr 5]
Czy mogę żądać odszkodowania?	Przysługuje Państwu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych oraz prawo dochodzenia odszkodowania przed sądem. Nie jestem osobą uprawnioną do udzielania informacji w tym zakresie – proszę o kontakt z naszym inspektorem ochrony danych: …… .
Chcę usunąć moje dane z systemu	Rozumiem Państwa obawy. Dokumentacja medyczna podlega jednak obowiązkowym okresom przechowywania wynikającym z ustawy i nie może zostać usunięta na żądanie. Mogą Państwo natomiast złożyć wniosek dotyczący pozostałego zakresu przetwarzania – przekażę sprawę inspektorowi ochrony danych.
Czy zmieniacie system?	Analizujemy sytuację i podejmiemy decyzję po otrzymaniu pełnych informacji od dostawcy. Teraz priorytetem jest zabezpieczenie danych i poinformowanie pacjentów.
Pytanie dziennikarza	**Nie udzielać wypowiedzi. Przekierować do kierownika placówki albo osoby wyznaczonej do kontaktów z mediami. Nie potwierdzać liczb ani okoliczności nieustalonych.**

ZASADY OGÓLNE DLA PERSONELU

Nie zapewniać, że nic się nie stało. Nie potwierdzać ani nie zaprzeczać okolicznościom nieustalonym. Nie podawać liczb ani nazwisk.

Nie weryfikować tożsamości pacjenta przez telefon wyłącznie na podstawie numeru PESEL – ten numer mogą obecnie znać osoby nieuprawnione.

Odnotowywać zgłoszenia pacjentów o próbach oszustwa. Mogą stanowić materiał dla organów ścigania.