

Zawiadomienie o naruszeniu ochrony danych osobowych

Dotyczy: incydentu bezpieczeństwa w systemie MyDr EDM - danych opiekuna prawnego, przedstawiciela ustawowego lub osoby upoważnionej

Szanowna Pani / Szanowny Panie,

Co się stało?

Z przykrością informujemy, że doszło do cyberataku na infrastrukturę zewnętrznego systemu elektronicznej dokumentacji medycznej MyDr EDM, którego dostawcą jest MyDr sp. z o.o. z siedzibą w Warszawie. MyDr przetwarza dane osobowe na rzecz Centrum Medycznego Wilsona w związku ze świadczeniem usług elektronicznej dokumentacji medycznej.

W wyniku tego zdarzenia doszło do naruszenia poufności danych osobowych znajdujących się w środowisku MyDr.

Według informacji przekazanych nam przez MyDr, na dzień otrzymania przez CMW zindywidualizowanego zawiadomienia nie stwierdzono dowodów, aby dane objęte incydem zostały wykorzystane niezgodnie z prawem lub publicznie ujawnione.

MyDr poinformowało również, że przeprowadzona przy wsparciu zewnętrznych ekspertów analiza wykazała, iż incydem został opanowany i nie ma dowodów wskazujących na dalszy nieuprawniony dostęp do systemów. MyDr prowadzi monitoring sytuacji.

Ustalenia przekazane przez MyDr wskazują, że osoba nieuprawniona uzyskała dostęp do środowiska serwerów chmurowych MyDr i skopiowała m.in. kopię zapasową bazy danych datowaną na 12 kwietnia 2024 r. W przypadku części osób incydem mógł również obejmować dane znajdujące się w anulowanych skierowaniach wystawionych po tej dacie.

Dodatkowa analiza przeprowadzona przez CMW wykazała, że w części dokumentacji Pacjentów znajdowały się również dane innych osób - m.in. opiekunów prawnych, przedstawicieli ustawowych oraz osób upoważnionych do uzyskiwania informacji o stanie zdrowia, dokumentacji medycznej albo odbioru recept i zleceń. Niniejsze zawiadomienie dotyczy Pani/Pana własnych danych zapisanych w takim charakterze.

Jakie dane mogły zostać objęte incydem?

W zależności od informacji zapisanych w systemie MyDr, wśród danych dotyczących Pani/Pana mogły znajdować się:

- imię i nazwisko;
- numer telefonu i inne zapisane dane kontaktowe;
- adres zamieszkania - jeżeli został zapisany;
- numer PESEL lub inny numer identyfikacyjny - jeżeli został zapisany;
- informacja o pokrewieństwie, relacji z Pacjentem lub statusie przedstawiciela ustawowego;
- informacja o zakresie udzielonego upoważnienia, np. do dokumentacji medycznej, informacji o stanie zdrowia albo odbioru recept i zleceń.

Ważne rozróżnienie

Sam fakt zapisania Pani/Pana jako opiekuna, przedstawiciela ustawowego lub osoby upoważnionej nie oznacza, że Pani/Pan był/a Pacjentem CMW ani że ten wpis obejmował Pani/Pana własną dokumentację medyczną lub dane dotyczące Pani/Pana zdrowia. Zakres niniejszego zawiadomienia dotyczy danych zapisanych o Pani/Panu jako osobie trzeciej powiązanej z dokumentacją Pacjenta.

Jeżeli jest Pani/Pan jednocześnie Pacjentem CMW, ewentualny zakres dotyczący Pani/Pana własnej dokumentacji medycznej jest oceniany odrębnie.

Jakie ewentualne konsekwencje zidentyfikowaliśmy?

Ryzyko zależy od rodzaju danych zapisanych w danym wpisie. W szczególności, jeżeli w Pani/Pana przypadku znajdował się numer PESEL, jego połączenie z imieniem i nazwiskiem oraz innymi danymi identyfikacyjnymi może w określonych sytuacjach zostać wykorzystane przez osoby nieuprawnione.

- próby zaciągnięcia kredytu lub pożyczki albo zawarcia innej umowy bez Pani/Pana wiedzy;
- próby podszywania się pod Panią/Pana lub wykorzystania danych do potwierdzania tożsamości;
- próby oszustwa, phishingu lub socjotechniki wykorzystujące znajomość Pani/Pana danych;
- niechciane kontakty lub naruszenie prywatności;
- wykorzystanie informacji o Pani/Pana relacji z Pacjentem do uwiarygodnienia oszustwa - np. rozmówca może podawać się za osobę, która wskazała Panią/Pana jako osobę upoważnioną, jej bliskiego albo osobę działającą w jej imieniu.

Szczególnie ważne przy telefonach i wiadomościach

Jeżeli ktoś powołuje się na Pacjenta, znajomego lub członka rodziny i wykorzystuje informacje o Państwa relacji, nie należy traktować samej znajomości tych danych jako potwierdzenia tożsamości rozmówcy.

Najbezpieczniej przerwać rozmowę i samodzielnie skontaktować się z tą osobą na znany wcześniej numer telefonu lub innym niezależnym kanałem. Nie należy oddzwaniać na numer podany przez rozmówcę ani korzystać z linku przesłanego w podejrzanej wiadomości.

Jakie działania może Pani/Pan podjąć?

1. W przypadku numeru PESEL

Jeżeli numer PESEL był zapisany w Pani/Pana danych i nie został jeszcze zastrzeżony, rekomendujemy rozważenie jego zastrzeżenia.

- w aplikacji mObywatel;
- przez Internet;
- osobiście w urzędzie gminy lub miasta.

Zastrzeżenie numeru PESEL ogranicza możliwość wykorzystania go m.in. do nieuprawnionego zaciągania zobowiązań. Nie uniemożliwia ono rejestracji u lekarza ani realizacji recepty.

Więcej informacji: <https://www.gov.pl/web/gov/zastrzez-swoj-numer-pesel-lub-cofnij-zastrzezenie>

Można również sprawdzić swój numer PESEL w państwowym serwisie: <https://bezpiecznedane.gov.pl/>

2. W przypadku podejrzanego telefonu, SMS-a lub e-maila

- nie podawać haseł, kodów SMS, danych karty płatniczej ani innych danych służących do potwierdzania tożsamości;
- nie wykonywać przelewów ani płatności pod presją czasu;
- jeżeli rozmówca powołuje się na konkretną znaną Pani/Panu osobę - samodzielnie zadzwonić do niej na numer, który Pani/Pan znał/a wcześniej, i potwierdzić, czy rzeczywiście próbowała się skontaktować;
- nie klikać w linki i nie korzystać z danych kontaktowych zawartych w podejrzanej wiadomości;
- zwracać uwagę na nietypowe operacje na rachunkach oraz korespondencję dotyczącą umów lub usług, których Pani/Pan nie zamawiał/a.

Prosimy pamiętać

Centrum Medyczne Wilsona nie będzie w związku z tym incydem prosiło Pani/Pana o podanie hasła, kodu SMS, danych karty płatniczej ani o wykonanie przelewu na „bezpieczne konto”.

Jeżeli otrzyma Pani/Pan wiadomość rzekomo od CMW i ma wątpliwości co do jej autentyczności, prosimy nie korzystać z danych kontaktowych zawartych w tej wiadomości. Kontakt należy zweryfikować za pośrednictwem oficjalnej strony Centrum Medycznego Wilsona.

Jakie działania zostały już podjęte?

Według informacji przekazanych przez MyDr, w celu ograniczenia skutków incydemu MyDr sp. z o.o. podjęło m.in. następujące działania:

1. opanowało incydem i wdrożyło dodatkowe środki techniczne i organizacyjne mające ograniczyć ryzyko podobnych zdarzeń w przyszłości;
2. zaangażowało wyspecjalizowaną firmę z zakresu cyberbezpieczeństwa w celu przeprowadzenia szczegółowej analizy incydemu;
3. zgłosiło incydem właściwym organom ścigania i współpracuje z odpowiednimi służbami;
4. współpracuje z Ministerstwem Cyfryzacji, Centrum e-Zdrowia, CSIRT NASK oraz CSIRT Centrum e-Zdrowia;
5. współpracuje z Urzędem Ochrony Danych Osobowych;
6. kontynuuje monitoring systemów pod kątem ewentualnych skutków incydemu;
7. prowadzi monitoring Internetu w celu wykrycia ewentualnego publicznego udostępnienia danych.

Centrum Medyczne Wilsona, jako administrator danych osobowych, po otrzymaniu zindywidualizowanego zawiadomienia od MyDr:

- przeprowadziło analizę incydemu i ocenę ryzyka;
- rozpoczęło proces indywidualnego powiadamiania osób, których dane zostały objęte naruszeniem;
- uruchomiło dedykowaną publiczną stronę informacyjną;
- podjęło dodatkowe działania organizacyjne i dotyczące bezpieczeństwa;
- przeprowadziło dodatkową analizę danych opiekunów prawnych, przedstawicieli ustawowych i osób upoważnionych;
- realizuje obowiązki związane ze zgłoszeniem naruszenia Prezesowi Urzędu Ochrony Danych Osobowych.

Informacja o źródle i zakresie danych

Ze względów bezpieczeństwa niniejsze zawiadomienie nie wskazuje danych Pacjenta, z którego dokumentacją Pani/Pana dane były powiązane. Po odpowiedniej weryfikacji tożsamości CMW może wyjaśnić źródło i zakres posiadanych danych w granicach dopuszczalnych prawem.

W części historycznych wpisów dane kontaktowe mogły być nieaktualne, współdzielone albo niejednoznaczne. CMW wykorzystuje do bezpośredniego kontaktu wyłącznie kanały, które można z odpowiednim poziomem pewności przypisać do właściwej osoby.

Dokładny zakres danych może różnić się pomiędzy poszczególnymi osobami i zależy od informacji, które znajdowały się w systemie MyDr.

Gdzie można uzyskać dalsze informacje?

Aktualne informacje dotyczące incydentu, możliwych konsekwencji, zalecanych działań ochronnych oraz odpowiedzi na najczęściej zadawane pytania publikujemy na oficjalnej stronie Centrum Medycznego Wilsona:

<https://centrumwilsona.pl/dane>

W przypadku pytań dotyczących Pani/Pana indywidualnej sytuacji, danych przetwarzanych przez Centrum Medyczne Wilsona lub realizacji praw wynikających z RODO prosimy o kontakt:

rodo@centrumwilsona.pl

W przypadku pytań dotyczących technicznego zakresu incydentu po stronie MyDr można również kontaktować się z MyDr:

dane@mydr.pl

MyDr udostępniło również stronę informacyjną dla Pacjentów:

<https://pacjent.mydr.pl>

Z poważaniem

Adam Włodarczak
Prezes Zarządu
Centrum Medyczne Wilsona sp. z o.o.