
Zawiadomienie o naruszeniu ochrony danych osobowych

Dotyczy: incydentu bezpieczeństwa w systemie MyDr EDM

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 Pani/Pana danych osobowych.

Według informacji przekazanych nam przez MyDr, na dzień otrzymania przez CMW zindywidualizowanego zawiadomienia nie stwierdzono dowodów, aby dane objęte incydemem 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.

W Pani/Pana przypadku incydem mógł obejmować dane znajdujące się w dokumentacji zapisanej w systemie MyDr przed 12 kwietnia 2024 r. oraz – jeżeli dotyczy – dane znajdujące się w anulowanych skierowaniach wystawionych po tej dacie. Zgodnie z klasyfikacją przekazaną przez MyDr, w dokumentacji należącej do tej grupy nie znajdowały się dane opiekuna prawnego ani osoby upoważnionej do wglądu do dokumentacji medycznej.

Jakie dane mogły zostać objęte incydemem?

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

- imię i nazwisko;
- adres zamieszkania;
- dane kontaktowe;
- **numer PESEL;**
- **dane dotyczące zdrowia;**
- dane dotyczące ubezpieczenia społecznego – jeżeli zostały podane i zapisane w systemie;
- informacje dotyczące pracodawcy – jeżeli zostały podane i zapisane w systemie;
- inne dane identyfikacyjne – jeżeli znajdowały się w systemie.

Pomimo że monitoring prowadzony przez MyDr nie wykazał dotychczas dowodów na publiczne ujawnienie danych ani na ich wykorzystanie niezgodnie z prawem, nie można wykluczyć takiego ryzyka w przyszłości.

Ze względu na charakter danych, w szczególności możliwość połączenia numeru PESEL z danymi identyfikacyjnymi oraz informacjami dotyczącymi zdrowia, Centrum Medyczne Wilsona oceniło, że naruszenie może powodować wysokie ryzyko dla praw i wolności osób, których dane dotyczą.

Dlatego przekazujemy informacje o możliwych konsekwencjach oraz działaniach, które mogą ograniczyć potencjalne skutki incydentu.

Jakie ewentualne konsekwencje zidentyfikowaliśmy?

Wśród danych objętych naruszeniem mógł znajdować się numer PESEL. W połączeniu z imieniem i nazwiskiem oraz innymi danymi identyfikacyjnymi może on w określonych sytuacjach zostać wykorzystany przez osoby nieuprawnione, w szczególności do:

- próby zaciągnięcia kredytu lub pożyczki albo zawarcia innej umowy bez Pani/Pana wiedzy;
- prób podszywania się pod Panią/Pana;
- prób wykorzystania Pani/Pana danych do potwierdzania tożsamości;
- prób uzyskania dostępu do informacji w miejscach, w których numer PESEL wykorzystywany jest jako jeden z elementów identyfikacji;
- kierowania bardziej wiarygodnie wyglądających prób oszustwa, phishingu lub wyłudzenia.

Incydent mógł również obejmować dane dotyczące zdrowia. Ich nieuprawnione wykorzystanie może prowadzić w szczególności do:

- naruszenia prywatności;
- nieuprawnionego ujawnienia informacji dotyczących stanu zdrowia lub leczenia;
- wykorzystania informacji o zdrowiu w sposób niekorzystny dla Pani/Pana;
- prób oszustwa wykorzystujących wiedzę dotyczącą leczenia lub stanu zdrowia, np. poprzez oferowanie nieoczekiwanych usług medycznych, pseudomedycznych lub terapeutycznych.

Na obecnym etapie nie stwierdzono dowodów wykorzystania ani publicznego ujawnienia danych. Ze względu na ich charakter zalecamy jednak zachowanie zwiększonej ostrożności.

Jakie działania może Pani/Pan podjąć?

W przypadku numeru PESEL

Rekomendujemy rozważenie zastrzeżenia numeru PESEL, jeżeli nie został jeszcze zastrzeżony.

Numer PESEL można bezpłatnie zastrzec:

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

Serwis ten jest usługą państwową i nie jest prowadzony przez Centrum Medyczne Wilsona ani przez MyDr.

Zalecamy również:

- zachowanie zwiększonej ostrożności wobec wiadomości e-mail, SMS-ów oraz telefonów od nieznanymi osób, szczególnie jeżeli rozmówca zna Pani/Pana dane osobowe lub informacje dotyczące leczenia;
- zwracanie uwagi na nietypowe operacje na rachunkach;
- zwracanie uwagi na korespondencję dotyczącą umów, kredytów, pożyczek lub usług, których Pani/Pan nie zamawiał/a;
- niezależne weryfikowanie kontaktów od osób lub instytucji powołujących się na dane osobowe dotyczące Pani/Pana.

W przypadku danych dotyczących zdrowia

Prosimy zachować szczególną ostrożność:

- wobec osób, które nie powinny znać informacji dotyczących Pani/Pana zdrowia, a mimo to powołują się na takie informacje;
- wobec nieoczekiwanych ofert usług medycznych, pseudomedycznych lub terapeutycznych;
- wobec wiadomości lub telefonów wykorzystujących wiedzę o leczeniu, rozpoznaniu, badaniach lub innych informacjach medycznych w celu wzbudzenia zaufania.

W przypadku podejrzenia, że dane zostały wykorzystane niezgodnie z prawem, można zgłosić sprawę Policji.

Informacje dotyczące zgłaszania przestępstw znajdują się pod adresem:

<https://www.gov.pl/web/gov/zglos-przestepstwo>

Podkreślamy, że według informacji przekazanych przez MyDr prowadzony monitoring nie wykazał dotychczas dowodów na wykorzystanie ani publiczne ujawnienie danych objętych incydemtem.

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

Jakie działania zostały już podjęte?

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

1. opanowało incydemtem 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 incydemtem;
3. zgłosiło incydemtem 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 incydemtem;
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 incydemtem i ocenę ryzyka dla Pacjentów;
- rozpoczęło proces indywidualnego powiadamiania osób, których dane zostały objęte naruszeniem;
- uruchomiło dedykowaną publiczną stronę informacyjną dla Pacjentów;
- podjęło dodatkowe działania organizacyjne i dotyczące bezpieczeństwa;
- realizuje obowiązki związane ze zgłoszeniem naruszenia Prezesowi Urzędu Ochrony Danych Osobowych.

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.