Zawiadomienie o naruszeniu ochrony danych osobowych

Centrum Medyczne Wilsona sp. z o.o.

ul. Głogowska 58/6

60-737 Poznań

Co się stało?

Z przykrością informujemy, że zewnętrzny system elektronicznej dokumentacji medycznej MyDr EDM, którego dostawca – MyDr sp. z o.o. z siedzibą w Warszawie – przetwarza dane osobowe na rzecz naszej placówki, padł ofiarą cyberataku. W wyniku tego zdarzenia doszło do naruszenia poufności Pani/Pana danych osobowych.

Według informacji przekazanych nam przez MyDr, na dzień otrzymania zawiadomienia nie stwierdzono dowodów, aby dane objęte incydentem zostały wykorzystane niezgodnie z prawem lub publicznie ujawnione. Zespoły MyDr oraz zewnętrzni eksperci prowadzą monitoring sytuacji. Przeprowadzona przez MyDr analiza wykazała również, że incydent został opanowany i nie ma dowodów wskazujących na dalszy nieuprawniony dostęp do systemów.

Ustalenia dokonane przez MyDr przy wsparciu ekspertów zajmujących się analizą śledczą wskazują, że w Pani/Pana przypadku incydent obejmował ograniczony zakres danych znajdujących się w anulowanym e-skierowaniu na badanie lub świadczenie medyczne.

Wśród danych objętych incydentem mogły znajdować się Pani/Pana: imię i nazwisko, adres zamieszkania, dane kontaktowe, numer PESEL, ograniczony zakres danych dotyczących zdrowia zawartych w anulowanym e-skierowaniu. Jeżeli posiada Pani/Pan przedstawiciela ustawowego, informacje zawarte w skierowaniu mogły również obejmować jego imię i nazwisko, adres zamieszkania oraz dane kontaktowe.

Pomimo że monitoring prowadzony przez MyDr nie wykazał dotychczas przypadków publicznego ujawnienia danych ani potwierdzonych przypadków ich wykorzystania 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 Pani/Panu informacje o możliwych konsekwencjach oraz zalecanych działaniach, które mogą ograniczyć potencjalne skutki incydentu.

Jakie ewentualne konsekwencje zidentyfikowaliśmy?

Wśród danych objętych naruszeniem mógł znajdować się numer PESEL, który w połączeniu z imieniem i nazwiskiem oraz innymi danymi identyfikacyjnymi może w określonych

sytuacjach zostać wykorzystany przez osoby nieuprawnione do działań niezgodnych z prawem, w szczególności do:

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

Incydent mógł również dotyczyć danych dotyczących zdrowia. Ich nieuprawnione wykorzystanie może prowadzić w szczególności do:

- naruszenia Pani/Pana prywatności;
- wykorzystania informacji o stanie zdrowia w sposób niekorzystny dla Pani/Pana;
- prób oszustwa wykorzystujących wiedzę o Pani/Pana leczeniu lub stanie zdrowia, np. poprzez oferowanie 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 i zastosowanie opisanych poniżej środków ochronnych.

Jakie działania może Pan/Pani podjąć?

W przypadku numeru PESEL:

- można bezpłatnie zastrzec numer PESEL w aplikacji mObywatel, przez Internet albo 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
- mogą Państwo dodatkowo sprawdzić swój numer PESEL w państwowym serwisie: https://bezpiecznedane.gov.pl/
- warto zachować zwiększoną ostrożność wobec wiadomości e-mail, SMS-ów oraz telefonów od nieznanych osób, szczególnie jeśli rozmówca zna Pani/Pana dane osobowe lub informacje dotyczące leczenia;
- warto zwracać uwagę na nietypowe operacje na rachunkach, korespondencję dotyczącą umów, pożyczek lub usług, których Pani/Pan nie zamawiał/a.

W przypadku danych dotyczących zdrowia:

- prosimy zachować szczególną ostrożność wobec kontaktów z osobami, które nie powinny znać informacji dotyczących Pani/Pana zdrowia, a mimo to powołują się na takie informacje;
- należy zachować szczególną ostrożność wobec ofert usług medycznych, pseudomedycznych lub terapeutycznych, których Pani/Pan nie oczekiwał/a;
- w przypadku potwierdzonego wykorzystania danych przez osoby nieuprawnione może Pani/Pan korzystać z przewidzianych prawem środków ochrony.

Bez względu na zakres danych osobowych, w przypadku podejrzenia, że zostały one wykorzystane niezgodnie z prawem, można zgłosić to na Policję.

Informacje o sposobie zgłoszenia znajdują się pod adresem: https://www.gov.pl/web/gov/zglos-przestepstwo.

Podkreślamy ponownie, że według informacji przekazanych przez MyDr prowadzony monitoring nie wykazał dotychczas dowodów na wykorzystanie ani publiczne ujawnienie danych objętych incydentem. Prosimy również pamiętać, że Centrum Medyczne Wilsona nie będzie w związku z tym incydentem prosiło Pani/Pana o podanie hasła, kodu SMS, danych karty płatniczej ani wykonanie przelewu na „bezpieczne konto".

Jakie działania zostały już podjęte?

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

1. opanowało incydent i wdrożyło dodatkowe środki techniczne i organizacyjne mające ograniczyć ryzyko podobnych zdarzeń w przyszłości;
2. zaangażowało wyspecjalizowaną firmę z zakresu cyberbezpieczeństwa w celu przeprowadzenia analizy incydentu;
3. zgłosiło incydent Centralnemu Biuru Zwalczania Cyberprzestępczości Policji i współpracuje z właściwymi służbami;
4. współpracuje z Ministerstwem Cyfryzacji, Centrum e-Zdrowia, CSIRT NASK i CSIRT Centrum e-Zdrowia;
5. współpracuje z Urzędem Ochrony Danych Osobowych;
6. kontynuuje monitoring systemów pod kątem ewentualnych skutków incydentu;
7. prowadzi monitoring Internetu w celu wykrycia ewentualnego publicznego udostępnienia danych.

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

- przeprowadziło analizę incydentu i ocenę ryzyka dla Pacjentów;
- rozpoczęło indywidualne powiadamianie osób, których dane zostały objęte naruszeniem;
- uruchomiło dedykowaną stronę informacyjną dla Pacjentów;
- podjęło dodatkowe działania organizacyjne i bezpieczeństwa;
- realizuje obowiązki związane ze zgłoszeniem naruszenia Prezesowi Urzędu Ochrony Danych Osobowych.

Gdzie można uzyskać dalsze informacje?

Aktualne informacje dotyczące incydentu, zalecanych działań ochronnych oraz odpowiedzi na najczęściej zadawane pytania publikujemy na stronie:

- 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 bezpośrednio 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.