Indywidualna Specjalistyczna
Praktyka Lekarska Tomasz Cieśliński

Plac Konstytucji 3 Maja 3
10-501 Olsztyn

Olsztyn, 15 września 2026 r.

Zawiadomienie o naruszeniu ochrony danych osobowych

dotyczy danych pacjentów z okresu **od 1 lipca 2021 do 12 kwietnia 2024**

Co się stało?

Z przykrością informuję, że moja Indywidualna Specjalistyczna Praktyka Lekarska znalazła się wśród ponad 12 tysięcy innych podmiotów medycznych w Polsce korzystających z usług MyDr Sp. z o.o., tj. dostawcy oprogramowania do prowadzenia elektronicznej dokumentacji medycznej. **MyDr Sp. o.o. z siedzibą w Warszawie padł ofiarą cyberataku**, w wyniku którego doszło do naruszenia danych obejmujących łącznie prawie 19 milionów osób w Polsce korzystających z kilkunastu tysięcy placówek.

W przypadku moich **Pacjentów korzystających w okresie od 1 lipca 2021 do 12 kwietnia 2024 z wizyt lekarskich w Indywidualnej Specjalistycznej Praktyce Lekarskiej Tomasz Cieśliński w Olsztynie**, z przykrością zawiadamiam jako administrator danych osobowych, iż doszło do naruszenia poufności Pani/Pana danych osobowych, a w niektórych przypadkach również danych osobowych Pani/Pana przedstawiciela ustawowego.

Nie oznacza to, że Pani/Pana dane zostały odczytane, wykorzystane lub upublicznione. Zespoły MyDr oraz zewnętrzni eksperci stale monitorują sytuację i nie wykryli, aby dane objęte incydentem zostały publicznie udostępnione. MyDr potwierdził, że **incydent został opanowany oraz że nie ma dowodów wskazujących na dalszy nieuprawniony dostęp do systemów.**

O jakie dane chodzi?

Dane pacjenta z okresu od 1 lipca 2021 do 12 kwietnia 2024 r. Wśród danych objętych incydentem mogły znaleźć się Pani/Pana: imię, nazwisko, adres zamieszkania, dane kontaktowe, numer PESEL, dane dotyczące zdrowia, ubezpieczenia społecznego i (jeśli zostały podane) inne dane identyfikacyjne.

Dane przedstawiciela ustawowego. Jeżeli jest Pani/Pan przedstawicielem ustawowym pacjenta z wyżej wymienionego okresu, zakres danych objętych incydentem mógł zawierać Pani/Pana dane wskazane w tej dokumentacji, w tym imię i nazwisko, adres zamieszkania, dane kontaktowe, numer PESEL i (jeśli zostały podane) inne dane identyfikacyjne oraz informacja o stopniu pokrewieństwa lub rodzaju relacji z pacjentem.

Mimo że prowadzony przez MyDr stały monitoring nie wykazał dotychczas żadnych przypadków wykorzystania ani publicznego ujawnienia danych, nie można wykluczyć, że, ze względu na charakter incydentu, w określonych okolicznościach może on potencjalnie wiązać się z wysokim ryzykiem dla praw lub wolności osób, których dane zostałyby niewłaściwie wykorzystane. Chcąc

pomóc Pani/Panu zachować bezpieczeństwo na wypadek zmiany okoliczności, przekazuję informacje o ewentualnych konsekwencjach oraz zalecanych środkach ostrożności, które mogą pomóc w ochronie danych osobowych i ograniczeniu potencjalnych skutków incydentu.

Jakie ewentualne konsekwencje zidentyfikowano?

Wśród danych objętych incydentem mógł znajdować się numer PESEL, który w połączeniu z imieniem i nazwiskiem oraz danymi kontaktowymi, w określonych sytuacjach, mógłby posłużyć osobom nieuprawnionym do działań niezgodnych z prawem. W szczególności, jeśli dane te zostałyby publicznie ujawnione, mogłyby zostać użyte przez osoby nieuprawnione do:

- zaciągnięcia kredytu, pożyczki lub zawarcia innych umów bez Pani/Pana wiedzy;
- uzyskania dostępu do Pani/Pana danych dotyczących zdrowia w instytucjach medycznych, w których uwierzytelnianie osób następuje przy pomocy numeru PESEL.

Incydent mógł dotyczyć również danych dotyczących zdrowia, których nieuprawnione użycie może naruszać Pani/Pana prawa, w szczególności, gdyby osoby trzecie próbowały wykorzystać te informacje:

- w sposób niekorzystny dla Pani/Pana, w tym prowadzący do naruszenia Pani/Pana praw lub gorszego traktowania w środowisku zamieszkania;
- w celu dokonania oszustwa, np. poprzez kontakt z Panią/Panem lub bliskimi w celu zaoferowania alternatywnych metod leczenia zdiagnozowanych u Pani/Pana chorób.

Warto zachować ostrożność i czujność. Ale też zachować spokój. Z prowadzonego przez MyDr monitoringu nie wykazano jak dotąd żadnych przypadków wykorzystania ani publicznego ujawnienia danych.

Jakie działania może Pan/Pani podjąć?

W przypadku numeru PESEL:

- **można bezpłatnie zastrzec numer PESEL** w aplikacji mobilnej mObywatel, przez Internet na stronie mObywatel.gov.pl lub osobiście w Urzędzie Gminy (Miasta).
  Instytucje finansowe są zobligowane weryfikować przy zawieraniu umów, czy PESEL jest zastrzeżony, co ogranicza ryzyko użycia danych do nieuprawnionego zaciągania zobowiązań na szkodę innych osób. Więcej informacji pod linkiem:
  https://www.gov.pl/web/gov/zastrzez-swoj-numer-pesel-lub-cofnij-zastrzezenie

Proszę pamiętać, że zastrzeżenie PESEL nie blokuje możliwości rejestracji u lekarza, realizacji recepty czy załatwienia sprawy w urzędzie.

- można poinformować inne placówki medyczne, w których świadczone są dla Pani/Pana usługi, iż osoby trzecie mogłyby chcieć wykorzystać Pani/Pana PESEL w celu przejścia procesu autoryzacji w tych placówkach.

W przypadku danych dotyczących zdrowia:

- warto zachować szczególną ostrożność wobec wszelkich kontaktów z nieznanymi osobami, które nie miały prawa znać historii Pani/Pana zdrowia, a które proponują Pani/Panu

skorzystanie z oferowanych przez nie usług medycznych, pseudomedycznych lub terapeutycznych.

- w razie potwierdzenia wykorzystania danych przez osoby nieuprawnione, może Pani/Pan dochodzić względem nich ochrony swoich praw na podstawie właściwych przepisów, w tym Kodeksu Cywilnego;

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

Prowadzony przez MyDr monitoring nie wykazał dotychczas żadnych przypadków wykorzystania ani publicznego ujawnienia danych.

Jakie działania zostały już podjęte?

Aby ograniczyć negatywne skutki wykrytego ataku, MyDr Sp. z o.o. niezwłocznie opanował i zakończył incydent, a także wdrożył dodatkowe, ukierunkowane środki techniczne i organizacyjne mające na celu zapobieganie podobnym incydentom w przyszłości. Zaangażował wyspecjalizowaną firmę z zakresu cyberbezpieczeństwa w celu przeprowadzenia szczegółowej analizy incydentu. Zgłosił incydent wyspecjalizowanej jednostce Policji - Centralnemu Biuru Zwalczania Cyberprzestępczości Policji i ściśle z nią współpracuje. Współpracuje z Ministerstwem Cyfryzacji, Centrum e-Zdrowia, CSIRT NASK i CSIRT Centrum e-Zdrowia. Współpracuje z Urzędem Ochrony Danych Osobowych. Kontynuuje monitoring systemów w celu wykrycia ewentualnych skutków incydentu i niezwłocznego reagowania na pojawiające się zagrożenia. Prowadzi stały monitoring internetu w celu wykrycia, czy dane, których dotyczy incydent, zostały upublicznione.

Ja jako administrator Pani/Pana danych osobowych, po otrzymaniu od MyDr Sp. z o.o. zawiadomienia o naruszeniu, dokonałem niezwłocznie formalnego zgłoszenia tego naruszenia do Urzędu Ochrony Danych Osobowych.

Gdzie można uzyskać dalsze informacje?

Jeśli nie ma Pan/Pani pewności czy korzystał(a) Pan/Pani z wizyty lekarskiej w okresie od 1 lipca 2021 do 12 kwietnia 2024, można do mnie napisać na adres snwd@wp.pl i udzielę informacji.

W przypadku dodatkowych pytań dotyczących zakresu incydentu naruszenia danych osobowych, można pisać na adres dane@mydr.pl lub skorzystać ze strony **pacjent.mydr.pl**

Z poważaniem

Tomasz Cieśliński