Zawiadomienie o naruszeniu ochrony danych osobowych

Podmiot przetwarzający, którego system został objęty incydentem

MyDr Sp. z o.o.
ul. Puławska 465
02-844 Warszawa
NIP: 5252730290

Administrator danych osobowych

Niepubliczny Zakład Opieki Zdrowotnej "KOLMED" Zespół Lekarza Rodzinnego Maciej Rybacki
ul. Chopina 18, 66-300 Międzyrzecz
REGON: 210144529
NIP: 5961114859

Co się stało?

Z przykrością informujemy, że system firmy MyDr Sp. z o.o. z siedzibą w Warszawie, która przetwarzała Państwa dane osobowe padł ofiarą cyberataku, w wyniku którego doszło do naruszenia poufności Pani/Pana danych osobowych.

Zespoły MyDr oraz zewnętrzni eksperci stale monitorują sytuację i nie wykryli, aby dane objęte incydentem zostały publicznie udostępnione. Przeprowadzone przez MyDr analizy śledcze potwierdziły, że incydent został opanowany oraz że nie ma dowodów wskazujących na dalszy nieuprawniony dostęp do systemów.

Ustalenia dokonane przez MyDr przy wsparciu ekspertów zajmujących się analizą śledczą wskazują, że incydent obejmował ograniczony zakres danych przed 12 kwietnia 2024 r., z wyjątkiem nielicznych przypadków, w których mógł również objąć dane zawarte w anulowanych skierowaniach na badania medyczne wystawione po tej dacie.

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) informacje dotyczące pracodawcy, lub inne dane identyfikacyjne.

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

Jakie ewentualne konsekwencje zostały zidentyfikowane?

Wśród danych objętych naruszeniem 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 zdrowia w instytucjach medycznych, w których uwierzytelnianie osób następuje przy pomocy numeru PESEL.

Incydent mógł również dotyczyć 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 do 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.

Na obecnym etapie nie stwierdzono przypadków wykorzystania ani publicznego ujawnienia danych. Ze względu jednak na charakter danych zalecamy zachowanie wskazanych poniżej środków ostrożności.

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 obecnie zobligowane weryfikować przy zawieraniu umów, czy PESEL jest zastrzeżony, co ogranicza ryzyko użycia danych do nieuprawnionego zaciągania zobowiązań na szkodę innych osób. Zastrzeżenie PESEL nie blokuje jednak możliwości rejestracji u lekarza, realizacji recepty czy załatwienia sprawy w urzędzie – więcej informacji pod linkiem: https://www.gov.pl/web/gov/zastrzez-swoj-numer-pesel-lub-cofnij-zastrzezenie;
- można poinformować inne placówki medyczne, w których świadczone są dla Pani/Pana usługi, iż osoby trzecie mogą chcieć wykorzystać Pani/Pana PESEL w celu przejścia procesu autoryzacji w tych jednostkach.

W przypadku danych dotyczących zdrowia:

- 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;
- 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. Należy również uważać na wiadomości SMS, e-maile i telefony od osób podszywających się pod NZOZ „KOLMED", MyDr, bank lub inną zaufaną instytucję. Nie należy otwierać podejrzanych linków lub załączników ani przekazywać haseł, kodów autoryzacyjnych lub danych do bankowości elektronicznej.

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 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., podjął następujące działania:

1. niezwłocznie opanował i zakończył incydent, a także wdrożył dodatkowe, ukierunkowane środki techniczne i organizacyjne mające na celu zapobieganie podobnym incydentom w przyszłości;
2. zaangażował wyspecjalizowaną firmę z zakresu cyberbezpieczeństwa w celu przeprowadzenia szczegółowej analizy incydentu;
3. zgłosił incydent wyspecjalizowanej jednostce Policji - Centralnemu Biuru Zwalczania Cyberprzestępczości Policji i ściśle z nią współpracuje;
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 w celu wykrycia ewentualnych skutków incydentu i niezwłocznego reagowania na pojawiające się zagrożenia;
7. prowadzi stały monitoring internetu w celu wykrycia, czy dane, których dotyczy incydent, zostały upublicznione.

Nasza placówka - jako administrator Pani/Pana danych osobowych, po otrzymaniu zawiadomienia o naruszeniu od MyDr Sp. z o.o., dokonała zgłoszenia tego naruszenia do Prezesa Urzędu Ochrony Danych Osobowych.

Gdzie można uzyskać dalsze informacje?

W sprawach dotyczących ochrony danych osobowych można kontaktować się z Inspektorem ochrony danych: Filip Łykowski, e-mail: iod@filkom.pl.

W przypadku pytań technicznych dotyczących incydentu prosimy o kontakt z MyDr Sp. z o.o. pod adresem e-mail: dane@mydr.pl.

Informacje wyjaśniające dostępne są również na stronie internetowej https://pro.mydr.pl/portal-info w sekcji „Często zadawane pytania”