PISMO INFORMACYJNE w sprawie naruszenia danych osobowych

Szanowni Państwo,

Z przykrością informujemy, że system naszego podmiotu przetwarzającego, tj. MyDr Sp. z o.o. z siedzibą w Warszawie, padł ofiarą cyberataku, w wyniku którego doszło do naruszenia poufności Pani/Pana danych osobowych.

Chcielibyśmy podkreślić, że **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. Przeprowadzone przez MyDr analizy śledzcze 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.

Do osób, których dane zostały ujawnione, stosownie do art. 34 RODO skierowaliśmy indywidualne powiadomienia za pomocą środków komunikacji elektronicznej .

Niezależnie od powyższego, z uwagi na wysokie ryzyko naruszenia praw lub wolności osób fizycznych, kierując się dobrem pacjentów i osób, do których z przyczyn od nas niezależnych nie możemy doręczyć indywidualnego powiadomienia, zamieszczamy jego treść również na naszej stronie internetowej.

Jakie ewentualne konsekwencje zidentyfikowaliśmy?

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.

Raz jeszcze chcemy podkreślić, że warto zachować ostrożność i czujność, jednak na obecnym etapie prowadzony przez **MyDr monitoring nie wykazał żadnych przypadków wykorzystania ani publicznego ujawnienia danych. Nie ma zatem powodów do niepokoju.**

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 NZOZ Arte-medica Edyta Artemiuk - 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 przypadku dodatkowych pytań dotyczących zakresu incydentu prosimy o kontakt dane@mydr.pl lub do Inspektora Danych Osobowych Pana Jędrzeja Żychskiego jedrek44@gmail.com

Z poważaniem

Edyta Artemiuk

Właściciel przychodni