KOMUNIKAT DOTYCZĄCY NARUSZENIA OCHRONY DANYCH OSOBOWYCH ZWIĄZANY Z INCYDENETEM BEZPIECZEŃSTWA SYSTEMU MYDR SP. Z O.O.

Szanowni Państwo,

Informujemy, że zewnętrzny dostawca systemu informatycznego wykorzystywanego przez Old Town Clinic – firma MyDr Sp. z o.o. – padł ofiarą cyberataku, w wyniku którego mogło dojść do naruszenia poufności danych części Pacjentów.

Chociaż cyberatak został powstrzymany, a monitoring nie wykazał, aby dane zostały upublicznione, istnieje potencjalne ryzyko, które wymaga podjęcia kroków ostrożnościowych.

Poniżej znajdują się najważniejsze informacje o incydencie:

WAŻNA INFORMACJA – BEZPIECZEŃSTWO ZDJĘĆ Z BADAŃ

Zdjęcia z badań wideodermatoskopowych SĄ CAŁKOWICIE BEZPIECZNE i NIE PODLEGAJĄ WYCIEKOWI. Wszystkie materiały fotograficzne oraz dokumentacja obrazowa z badań wideodermatoskopowych są przechowywane wyłącznie w **odrębnym, wewnętrznym systemie klinicznym**, który nie ma połączenia z systemem zewnętrznym MyDr i nie został objęty zdarzeniem.

Charakter naruszenia

Doszło do cyberataku na system zewnętrznego podmiotu MyDr Sp. z o.o., w wyniku którego naruszono poufność danych pacjentów zgromadzonych przed 12 kwietnia 2024 roku. Atak został już opanowany i zabezpieczony.

Kategorie danych objętych naruszeniem

Wyciek mógł objąć następujące informacje:

Imię, nazwisko, adres zamieszkania, dane kontaktowe, numer PESEL, dane dotyczące zdrowia, ubezpieczenia społecznego, i (jeśli zostały podane) informacje dotyczące pracodawcy, lub inne dane identyfikacyjne.

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.

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.

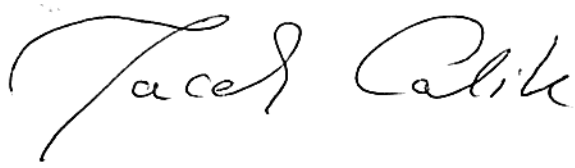
Bez względu na zakres danych osobowych, w przypadku podejrzenia, że zostały one wykorzystane niezgodnie z prawem, można zgłosić to na Policję.

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.

Punkt kontaktowy

W przypadku dodatkowych pytań dotyczących zakresu naruszenia Twoich danych, możesz skontaktować się bezpośrednio pod adresem e-mail: **dane@mydr.pl**.

Dr hab. n.med. Jacek Calik

Kierownik Przychodni