

Zawiadomienie o naruszeniu danych osobowych osoby, której dane dotyczą

**Niepubliczny Zakład Opieki Zdrowotnej
Zespół Lekarza Rodzinnego „WIGOR” s.c.
ul. Szafrana 8,
65-242 Zielona Góra
telefon: 68 328 2441;**

**Pacjenci
Osoby upoważnione przez Pacjentów
Pełnomocnicy
Przychodni WIGOR S.C.**

INFORMUJE PAŃSTWA O ZAISTNIAŁEJ SYTUACJI ZWIĄZANEJ Z NARUSZENIEM PAŃSTWA DANYCH OSOBOWYCH

Z przykrością informujemy, że system internetowy MyDr obsługujący naszą Przychodnię Wigor padł ofiarą cyberataku. W wyniku ataku doszło do naruszenia poufności Państwa danych osobowych, a także danych osobowych Państwa przedstawicieli ustawowych, osób upoważnionych do dostępu do dokumentacji medycznej oraz pracowników Przychodni.

Z informacji przekazywanych na bieżąco przez firmę MyDr sp. z o.o. z siedzibą w Warszawie nie wynika, że Państwa dane zostały odczytane, wykorzystane lub upublicznione. Zespoły firmy MyDr oraz zewnętrzni eksperci stale monitorują sytuację i nie stwierdzili, aby dane objęte incydem 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.

Przychodnia Wigor informuje, że z informacji uzyskanych od firmy MyDr wynika, że incydent obejmował ograniczony zakres danych wprowadzonych do systemu przed 12 kwietnia 2024 r. W nielicznych przypadkach mógł również obejmować dane zawarte w anulowanych skierowaniach na badania medyczne wystawionych po tej dacie.

W przypadku pacjentów Przychodni naruszeniem poufności zostały objęte następujące dane: imię, nazwisko, adres zamieszkania, dane kontaktowe, numer PESEL, dane dotyczące zdrowia, ubezpieczenia społecznego oraz - jeśli zostały podane - informacje dotyczące pracodawcy lub inne dane identyfikacyjne.

Zakres danych objętych naruszeniem mógł również obejmować dane Państwa przedstawiciela ustawowego lub osoby upoważnionej do dostępu do dokumentacji medycznej. W zależności od zakresu informacji przekazanych przez tę osobę może to dotyczyć takich danych jak: imię i nazwisko, adres zamieszkania, dane kontaktowe, numer PESEL oraz informacja o stopniu pokrewieństwa lub rodzaju relacji z pacjentem.

Firma MyDr zapewnia naszą Przychodnię Wigor, że stale monitoruje sytuację pod kątem ewentualnego wykorzystania lub publicznego ujawnienia danych. Działania te mają na celu zapewnienie bezpieczeństwa na wypadek zmiany okoliczności. Ze względu na charakter naruszenia nie można wykluczyć, że może on potencjalnie wiązać się z wysokim ryzykiem dla praw lub wolności osób, których dane mogłyby zostać niewłaściwie wykorzystane. Dlatego Przychodnia Wigor zaleca, aby zachować wszelkie środki ostrożności, które mogą pomóc w ochronie danych osobowych i ograniczeniu potencjalnych skutków naruszenia.

Jakie ewentualne konsekwencje mogą wiązać się dla Państwa z zaistniałym naruszeniem?

Jeżeli wśród danych objętych naruszeniem znajdował się numer PESEL, który wraz z imieniem, nazwiskiem oraz danymi kontaktowymi mógłby zostać wykorzystany przez osoby nieuprawnione, istnieje ryzyko, że dane te posłużą do:

- zaciągnięcia kredytu, pożyczki lub zawarcia innych umów bez Państwa wiedzy i zgody;
- uzyskania dostępu do Państwa danych dotyczących zdrowia w innych placówkach medycznych, w których numer PESEL jest wykorzystywany do potwierdzenia tożsamości pacjenta.

Naruszeniem objęte zostały Państwa dane dotyczące zdrowia, których nieuprawnione użycie może naruszać Państwa prawa, w szczególności, gdyby osoby trzecie próbowały wykorzystać te informacje:

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

Przychodnia Wigor zaleca, aby zachować ostrożność i czujność. Jednocześnie informuje Państwa, że firma MyDr powiadomiła naszą Przychodnię, że stale nadzoruje sytuację, mając na celu śledzenie przypadków wykorzystania lub upublicznienia danych. Zapewnia także że dotychczasowy prowadzony monitoring nie wykazał żadnych przypadków wykorzystania ani publicznego ujawnienia danych. Nie ma zatem powodów do niepokoju.

Jakie działania możecie Państwo podjąć celem zachowania ostrożności?

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 Państwa usługi, iż osoby trzecie mogą chcieć wykorzystać Państwa PESEL w celu przejścia procesu autoryzacji w tych jednostkach.

W przypadku danych dotyczących zdrowia:

- w razie potwierdzenia wykorzystania danych przez osoby nieuprawnione możecie Państwo 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 Państwa zdrowia, a które proponują Państwu 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>.

Mając na względzie powyżej przekazane Państwu informację firma MyDr zapewnia naszą Przychodnię Wigor, że prowadzony przez nią monitoring w momencie przekazywania Państwu tego komunikatu nie wykazał żadnych przypadków wykorzystania ani publicznego ujawnienia danych.

Jakie działania zostały już podjęte przez firmę MyDr, z którą Przychodnia Wigor ma podpisaną umowę na świadczenie usług?

Przychodnia Wigor została poinformowana przez firmę MyDr, o podjętych działaniach mających na celu ograniczanie negatywnych skutków wykrytego ataku na system internetowy firmy MyDr Sp. z o.o. obsługujący naszą Przychodnię oraz podjęła następujące działania:

1. niezwłocznie opanowała i zakończyła incydent, a także wdrożyła dodatkowe, ukierunkowane środki techniczne i organizacyjne mające na celu zapobieganie podobnym incydentom w przyszłości;
2. zaangażowała wyspecjalizowaną firmę z zakresu cyberbezpieczeństwa w celu przeprowadzenia szczegółowej analizy incydentu;
3. zgłosiła 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;
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 przypadku dodatkowych pytań w możecie Państwo dzwonić do Przychodni pod numer telefonu: **609 810 100** oraz pisać na adres e-mail: **naruszenia@szafrana.pl**, który Przychodnia specjalnie uruchomiła w celu ułatwienia kontaktu. Jednocześnie informujemy Państwa, że możecie skorzystać w kontakcie, który został utworzony przez MyDr w celu uzyskania dodatkowych informacji o naruszeniu na adres e-mail: **dane@mydr.pl**.

Z poważaniem

Kierownik NZOZ „Wigor”

Elżbieta Joanna Orchel
lekarz chorób wewnętrznych
specjalista medycyny rodzinnej