PILNE!

WAŻNY KOMUNIKAT

DLA PACJENTÓW DOTYCZĄCY BEZPIECZEŃSTWA DANYCH OSOBOWYCH

opublikowany 07.09.2026 r.

ZDROWIE Elżbieta Gliniak informuje o naruszeniu ochrony danych osobowych, które objęło system MyDr EDM oferowany przez naszego dostawcę MyDr sp. z o.o. z siedzibą w Warszawie (02-844), ul. Puławska 465 (KRS: 0000704950).

System stał się celem cyberataku, w wyniku którego doszło do naruszenia poufności Państwa danych osobowych.

Co się wydarzyło?

Zostaliśmy poinformowani przez MyDr sp. z o.o., że doszło do naruszenia ochrony danych przetwarzanych w ich środowisku cyfrowym. Z przekazanych nam informacji wynika, że nieuprawniona osoba trzecia uzyskała dostęp do kopii zapasowych baz danych w systemie MyDr EDM, czyli oprogramowania do prowadzenia m.in. dokumentacji medycznej. W toku analizy ustalono, że kopia zapasowa bazy danych z 12 kwietnia 2024 r. została pozyskana przez osoby nieuprawnione.

MyDr poinformował, że incydent został opanowany, system zabezpieczono i nie ma dowodów na dalszy nieuprawniony dostęp.

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

Na dzień przekazania nam informacji MyDr nie stwierdził również przypadków publicznego ujawnienia ani niewłaściwego wykorzystania danych objętych incydentem.

Nie można jednak całkowicie wykluczyć ryzyka ich wykorzystania w przyszłości, dlatego prosimy Pacjentów o zachowanie ostrożności i zastosowanie opisanych poniżej środków bezpieczeństwa.

Jakie dane mogły zostać objęte incydentem?

Zakres danych może być różny dla poszczególnych osób. W zależności od informacji znajdujących się w systemie MyDr incydent mógł obejmować – jeżeli takie dane zostały przez Państwa podane – m.in.:

- *imię i nazwisko,*

- *numer PESEL,*
- *adres zamieszkania,*
- *dane kontaktowe,*
- *dane dotyczące zdrowia,*
- *dane dotyczące ubezpieczenia społecznego,*
- *informacje dotyczące pracodawcy,*
- *inne dane umożliwiające identyfikację.*

Dane przetwarzane w systemie MyDr EDM w placówce obejmują w szczególności dane dotyczące samego faktu korzystania z usług świadczonych przez naszą placówkę, kody chorób (zgodnie z systemem ICD-10). Także te dane są uznawane za dane dotyczące zdrowia. W niektórych przypadkach informacje mogą obejmować również dane dotyczące wystawionych na Państwa rzecz zwolnień lekarskich.

Z tego względu, a także dlatego, że dane mogą obejmować numer PESEL, zdarzenie traktujemy z najwyższą powagą i starannością.

Co rekomendujemy?

W przypadku, gdy ujawniony został Państwa numer PESEL:

- *można bezpłatnie zastrzec numer PESEL w aplikacji mobilnej mObywatel, przez Internet na stronie mObywatel.gov.pl lub osobiście w urzędzie gminy lub miasta. Prosimy zachować dowód dokonania zastrzeżenia! Instytucje finansowe są obecnie zobowiązane weryfikować przy zawieraniu umów, czy PESEL jest zastrzeżony, co ogranicza ryzyko użycia danych do nieuprawnionego zaciągania zobowiązań na Państwa szkodę Zastrzeżenie numeru 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;*
- *monitorowanie zdolności kredytowej. Mogą Państwo uruchomić usługę alertów w BIK (https://www.bik.pl) raz w biurach informacji gospodarczej (BIG InfoMonitor, KRD, ERIF);*
- *można poinformować inne placówki medyczne, z których usług Państwo korzystają, że osoby trzecie mogą chcieć wykorzystać Państwa PESEL w celu weryfikacji tożsamości w tych placówka;*
- *przyjmij podwyższony standard ostrożności wobec kontaktu telefonicznego i elektronicznego. Przestępcy mogą próbować wykorzystać pozyskane dane w celu popełnienia oszustwa lub nakłonienia Państwa do podjęcia niekorzystnych działań. Szczególną czujność należy zachować, gdy nieznana osoba powołuje się na dotyczące Państwa informacje, prosi o podanie dodatkowych*

danych osobowych, nakłania do dokonania płatności lub przelewu bądź przesyła link/załącznik i prosi o jego otwarcie;

- *nie podawaj kodów autoryzacyjnych ani haseł przez telefon, nie należy otwierać linków lub załączników otrzymanych za pośrednictwem SMS-ów lub e-maili. Podejrzane wiadomości mogą Państwo przekazać bezpłatnie do CERT Polska: SMS-em na numer 8080, wiadomością e-mail na adres: cert@cert.pl (najlepiej jako załącznik) lub za pośrednictwem formularza online na stronie: https://incydent.cert.pl;*

W przypadku, gdy ujawnione zostały Państwa dane dotyczące zdrowia:

- *w razie potwierdzenia wykorzystania danych przez osoby nieuprawnione mogą Państwo skorzystać ze środków ochrony dóbr osobistych wskazanych w Kodeksie cywilnym oraz Kodeksie postępowania cywilnego, w tym dochodzić swoich praw na drodze sądowej;*
- *warto zachować szczególną ostrożność wobec wszelkich kontaktów z nieznanymi osobami, które nie powinny znać informacji o Państwa stanie zdrowia, a które proponują Państwu skorzystanie z oferowanych przez nie usług medycznych, pseudomedycznych lub terapeutycznych, powołując się na informacje dotyczące Państwa zdrowia;*
- *jeżeli incydent wywołał u Państwa silny stres lub niepokój, mogą Państwo skorzystać z profesjonalnej pomocy psychologicznej.*

Bez względu na zakres danych osobowych, w przypadku podejrzenia, że dane zostały wykorzystane do popełnienia przestępstwa, sprawę mogą Państwo zgłosić organom ścigania. Informacje o tym, jak zgłosić przestępstwo, dostępne są na https://www.gov.pl/web/gov/zglos-przestepstwo.

Podkreślamy, że na obecnym etapie prowadzony przez MyDr monitoring nie wykazał dotychczas żadnych przypadków wykorzystania ani publicznego ujawnienia danych. Niezależnie od tego chcemy pomóc Państwu 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 działania zostały podjęte?

Zgodnie z informacjami przekazanymi przez MyDr, dostawca opanował incydent i wdrożył dodatkowe środki techniczne i organizacyjne mające zapobiegać podobnym zdarzeniom w przyszłości. W szczególności zaangażował wyspecjalizowaną firmę zajmującą się cyberbezpieczeństwem, zgłosił incydent Centralnemu Biuru Zwalczania Cyberprzestępczości oraz współpracuje m.in. z Urzędem Ochrony Danych Osobowych, Ministerstwem Cyfryzacji, Centrum e-Zdrowia, CSIRT NASK oraz CSIRT Centrum e-Zdrowia.

Co więcej, dostawca kontynuuje monitoring systemów w celu wykrycia ewentualnych skutków incydentu i niezwłocznego reagowania na pojawiające się zagrożenia, a także prowadzi stały monitoring Internetu w celu wykrycia, czy dane, których dotyczy incydent, zostały upublicznione.

Jako administratorzy dokonaliśmy już zgłoszenia naruszenia Prezesowi Urzędu Ochrony Danych Osobowych, a także pozostajemy w bieżącym kontakcie z dostawcą, by jak najskuteczniej ograniczyć dalsze ryzyko.

Jakie mogą być konsekwencje zdarzenia?

Wśród danych objętych naruszeniem mógł znajdować się numer PESEL, który w połączeniu z imieniem i nazwiskiem oraz danymi kontaktowymi mógłby w określonych sytuacjach 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 Państwa wiedzy;*
- *uzyskania dostępu do Państwa danych dotyczących zdrowia w instytucjach medycznych, w których uwierzytelnianie osób następuje za pomocą numeru PESEL.*

Incydent mógł również obejmować dane dotyczące zdrowia, których nieuprawnione użycie może naruszać Państwa prawa, w szczególności, gdyby osoby trzecie próbowały wykorzystać te informacje:

- *w sposób dla Państwa niekorzystny, w tym prowadzący do naruszenia praw, gorszego traktowania w środowisku zamieszkania/pracy bądź innych form dyskryminacji lub nierównego traktowania;*
- *w celu dokonania oszustwa, np. poprzez kontakt z Państwem lub bliskimi w celu zaoferowania alternatywnych metod leczenia zdiagnozowanych u Państwa 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.

Gdzie możesz pozyskać dalsze informacje?

MyDr Sp. z o.o. uruchomiła dedykowany punkt kontaktowy dla osób mających pytania o zakres incydentu pod adresem: dane@mydr.pl. Aktualne informacje dotyczące naruszenia mogą Państwo również uzyskać pod adresem: https://pacjent.mydr.pl/.

Mogą Państwo skontaktować się z nami bezpośrednio, pod adresem: 68-120 Iłowa, ul. Surzyna 5 lub telefonicznie pod nr: 683774258 lub pod adresem: egzdrowie@gmail.com.

Chętnie udzielimy Państwu niezbędnych informacji i wsparcia.

ELŻBIETA GLINIAK