

KOMUNIKAT W SPRAWIE INCYDENTU NARUSZENIA DANYCH OSOBOWYCH W SZCZEGÓLNOŚCI DO OSÓB, KTÓRE OTRZYMAŁY OD HOLIMEDYK INSTYTUT ZDROWIA PSYCHICZNEGO WIADOMOŚĆ TEKSTOWĄ

Szanowni Państwo,

Na podstawie art. 34 ust.1 i ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE („**RODO**”) informujemy, że w związku z przetwarzaniem Pani/Pana danych osobowych przez:

Holimedyk Instytut Zdrowia Psychicznego A. Krawczyk – Syguda, K. Płachecka – Gorajek Spółka jawna, adres siedziby i adres stałego wykonywania działalności gospodarczej: ul. Targowa 5, 42-202 Częstochowa, wpisana przez Sąd Rejonowy w Częstochowie XVII Wydział Gospodarczy Krajowego Rejestru Sądowego do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod numerem 0000962920, posiadająca NIP: 9492254201, REGON: 521578750 („**Administrator**”),

który jest administratorem Pani/Pana danych osobowych, w dniu 12 sierpnia 2026 r. dowiedzieliśmy się, że doszło do incydentu naruszenia Pani/Pana danych osobowych u naszego dostawcy systemu informatycznego do obsługi pacjentów, w wyniku którego mogło dojść do nieuprawnionego ujawnienia Pani/Pana danych osobowych – szczegółowe informacje w tej sprawie zostały wskazane poniżej.

1. Charakter i okoliczności naruszenia

Holimedyk Instytut Zdrowia Psychicznego A. Krawczyk – Syguda, K. Płachecka – Gorajek Spółka jawna, (zwany dalej „Holimedyk Instytut Zdrowia Psychicznego”) korzysta z systemu dokumentacji medycznej, której dostawcą jest spółka MyDr Sp. z o.o. z siedzibą w Warszawie (zwana dalej również „MyDr”). Na podstawie stosownej umowy powierzenia przetwarzania danych osobowych, MyDr Sp. z o.o. jest podmiotem przetwarzającym dane, których administratorem jest Holimedyk Instytut Zdrowia Psychicznego. W dniu 12 sierpnia 2026 r. została przekazana do informacji publicznej wiadomość od spółki MyDr Sp. z o.o. o incydencie związanym z naruszeniem ochrony danych osobowych przetwarzanych przez MyDr Sp. z o.o., co było, jak deklaruje Spółka, efektem zewnętrznego, celowego działania o charakterze przestępczym. Początkowo MyDr Sp. z o.o. nie potwierdzała, czy dane z naszej placówki były przedmiotem wycieku, jednak w ostatnich dniach Holimedyk Instytut Zdrowia Psychicznego został poinformowany, że incydent dotyczył części danych, których administratorem jest nasza placówka.

Jak podkreśla MyDr Sp. z o.o. incydent nie jest jednoznaczny, z tym, że Pani/Pana dane zostały odczytane, wykorzystane lub upublicznione. Jak zapewnia MyDr Sp. z o.o., jego zespoły oraz zewnętrzni eksperci stale monitorują sytuację i nie wykryli, 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. 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.

2. Zakres danych objętych incydem

Wśród danych objętych incydem mogły znaleźć się Pani/Pana dane, a jeśli dotyczy, tożsame dane małoletniego Pacjenta:

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

3. Podjęte działania w związku z wykrytym naruszeniem

Wobec zaistniałego naruszenia zostały wdrożone działania, których celem jest zminimalizowanie bądź całkowite wyeliminowanie negatywnych skutków, jakie mogą łączyć się dla Pani/Pana z tym naruszeniem.

Niezwłocznie po uzyskaniu potwierdzenia zajścia wskazanego incydem, wdrożyliśmy stosowne procedury wynikające z przyjętej w naszym podmiocie polityki bezpieczeństwa danych osobowych (RODO) i w związku z tym złożyliśmy do Prezesa Urzędu Ochrony Danych Osobowych zgłoszenie o incydencie możliwości naruszenia danych osobowych, których administratorem jest Holimedyk Instytut Zdrowia Psychicznego. Równolegle, zwróciliśmy się do Spółki MyDr Sp. z o.o. z wnioskiem o niezwłoczne wyjaśnienie, czy incydent dotyczy danych, których administratorem jest Holimedyk Instytut Zdrowia Psychicznego i po otrzymaniu stosownego powiadomienia podejmujemy dalsze niezbędne czynności informacyjne w odniesieniu do osób, których dane były objęte incydem.

Po ujawnieniu incydem, Administrator dokonał prewencyjnie audytu polityki bezpieczeństwa danych osobowych, dokonano zmiany haseł dostępu do nośników, na których przechowywane są dane. Jako placówka zastosowaliśmy się do rekomendacji dostawców usług informatycznych poprzez zmianę i wdrożenie wskazanych instrumentów.

Wdrażamy dodatkowe procedury weryfikacji tożsamości pacjentów przy bezpośrednim i telefonicznym kontakcie z naszą rejestracją.

Ponadto uzyskaliśmy od MyDr Sp. z o.o., jako podmiotu przetwarzającego dane, zapewnienie, iż w celu ograniczenia negatywnych skutków wykrytego ataku MyDr Sp. z o.o., podjął ze swojej strony 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.

4. Możliwe skutki naruszenia ochrony danych osobowych

Mimo, że jak wskazał MyDr Sp. z o.o. prowadzony przez ten podmiot 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.

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:

- kradzieży lub sfalszowania tożsamości poprzez zaciągnięcia kredytu, pożyczki lub zawarcia innych umów (np. umów abonamentowych) bez Pani/Pana wiedzy bądź podjęcia działań w celu wyłudzenia ubezpieczenia lub środków z ubezpieczenia;
- działań phishingowych (np. fałszywe wiadomości SMS lub e-mail mające na celu wyłudzenie haseł do bankowości);
- 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, w szczególności prawa do prywatności w wyniku ujawnienia informacji o stanie zdrowia i może skutkować bezprawnym naruszeniem Pani/Pana dóbr osobistych

- 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.

5. Proponowane środki i działania w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków

W celu zminimalizowania ewentualnych negatywnych skutków naruszenia, zalecamy, aby Pani/Pan podjął następujące czynności:

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.
- można zarejestrować się na Alert BIK — w celu otrzymania powiadomienia. Jeśli z wykorzystaniem numeru PESEL ktoś złoży wniosek o kredyt, pożyczkę lub kartę kredytową, może to być pomocne w wykryciu prób oszustwa oraz jego zatrzymaniu. Jest to usługa odpłatna oferowana przez Biuro Informacji Kredytowej. Więcej informacji w tym zakresie znajdziecie Państwo w Internecie po wpisaniu w wyszukiwarkę haseł: Alert BIK.

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.

Wzmóžona ostrożność przed użyciem danych osobowych

Prosimy przede wszystkim zachować szczególną ostrożność, szczególnie wobec SMS-ów, e-maili i telefonów i innych prób kontaktu. Zalecamy też nie klikać w żadnego rodzaju linki czy też nie pobierać załączników od niezweryfikowanych nadawców. Wyludzenie dodatkowych informacji może być bardziej efektywne przy wykorzystaniu danych pochodzących z wycieku, które mogą służyć uwiarygodnieniu się ewentualnego oszusta. Próby wyludzenia informacji bywają kierowane także do bliskich, stąd rekomendujemy również uczulenie członków rodziny w tym zakresie.

Bez względu na zakres danych osobowych, jeżeli dowie się Pani/Pan o wykorzystaniu Pani/Pana danych przez osobę nieuprawnioną, prosimy o jak najszybsze przekazanie nam tej informacji. Dodatkowo, jeżeli wykorzystanie wyczerpuje znamiona czynu zabronionego, należy zawiadomić także odpowiednie organy państwowe, w szczególności można zgłosić to na Policję. Informacje o sposobie zgłoszenia znajdują się pod adresem: <https://www.gov.pl/web/gov/zglos-przestepstwo>.

Podkreślamy ponownie, że zgodnie z informacjami przekazanymi przez podmiot przetwarzający, tj. MyDr Sp. z o.o. prowadzony przez MyDr Sp. z o.o. monitoring nie wykazał dotychczas żadnych przypadków wykorzystania ani publicznego ujawnienia danych.

Jednocześnie informujemy o zrealizowaniu przez Administratora obowiązku określonego w art. 33 RODO, tj. Administrator danych dokonał zgłoszenia wyżej opisanego naruszenia danych osobowych organowi nadzorczemu – Prezesowi Urzędu Ochrony Danych Osobowych.

W przypadku jakichkolwiek pytań, prosimy o kontakt na następujące dane kontaktowe Administratora: adres: ul. Targowa 5, 42-202 Częstochowa, e-mail: rejestracja@holimedyk.pl, tel.: +48 695119838.

Dodatkowe informacje znajdują się także pod wskazanym linkiem: <http://pacjent.mydr.pl/a>

Dokładamy wszelkich starań, by wyjaśnić w pełni okoliczności zaistniałego naruszenia i nie dopuścić do wystąpienia podobnych zdarzeń w przyszłości.

W imieniu i na rzecz Administratora

Anna Krawczyk – Syguda
Katarzyna Płachecka - Gorajek