For English see below

Informacja o naruszeniu ochrony danych osobowych – MyDr EDM

I. CO SIĘ STAŁO?

Z przykrością informujemy, że system naszego podmiotu przetwarzającego, tj. MyDr sp. z o.o. z siedzibą w Warszawie (dalej: MyDr), padł ofiarą cyberataku, w wyniku którego doszło do naruszenia poufności Pani/Pana danych osobowych. MyDr jest dostawcą specjalistycznego oprogramowania do prowadzenia elektronicznej dokumentacji medycznej, wykorzystywanego przez liczne podmioty z sektora ochrony zdrowia w Polsce.

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 analizy śledcze potwierdziły, że incydent został opanowany oraz że nie ma dowodów wskazujących na dalszy nieuprawniony dostęp do systemów.

Ustalenia dotyczące incydentu wskazują, że mógł on objąć dane przetwarzane przed 12 kwietnia 2024 r. W pojedynczych przypadkach zakres incydentu mógł obejmować również dane zawarte w anulowanych skierowaniach na badania medyczne wystawionych po tej dacie. W zależności od zakresu danych przetwarzanych w systemie, wśród danych objętych incydentem mogły znajdować się: imię i nazwisko, adres zamieszkania, dane kontaktowe, numer PESEL lub inne dane identyfikacyjne, dane dotyczące zdrowia, dane dotyczące ubezpieczenia społecznego oraz (jeżeli zostały podane) informacje dotyczące pracodawcy.

Dotychczasowy stały monitoring prowadzony przez MyDr nie wykazał przypadków wykorzystania ani publicznego ujawnienia danych objętych incydentem. Nie można jednak wykluczyć, że dane te mogą zostać w przyszłości wykorzystane w sposób nieuprawniony, co w zależności od okoliczności może wiązać się z ryzykiem dla Pani/Pana praw lub wolności.

Mając to na uwadze, przekazujemy Pani/Panu poniżej informacje o możliwych konsekwencjach incydentu oraz praktyczne zalecenia dotyczące działań, które mogą pomóc w zwiększeniu bezpieczeństwa Pani/Pana danych osobowych i ograniczeniu ewentualnych skutków ich nieuprawnionego wykorzystania.

II. JAKIE EWENTUALNE KONSEKWENCJE ZIDENTYFIKOWALIŚMY?

W przypadku gdy wśród danych objętych incydentem znajdował się Pani/Pana numer PESEL, jego połączenie z imieniem i nazwiskiem oraz innymi danymi identyfikacyjnymi lub kontaktowymi może, w określonych okolicznościach, zostać wykorzystane przez osoby nieuprawnione do działań niezgodnych z prawem. W szczególności, jeśli dane te zostałyby publicznie ujawnione, mogłyby zostać użyte 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.

Jeżeli osoby nieuprawnione uzyskałyby dostęp do danych dotyczących zdrowia, ich wykorzystanie mogłoby z kolei prowadzić do naruszenia Pani/Pana prywatności, a w określonych okolicznościach również do:

- wykorzystania ich 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.

Należy jednak podkreślić, że są to potencjalne scenariusze związane z charakterem danych objętych incydentem. Dotychczasowy monitoring prowadzony przez MyDr nie wykazał, aby dane objęte incydentem zostały wykorzystane lub publicznie ujawnione.

III. 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, ew. dzielnicy). 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.

IV. JAKIE DZIAŁANIA ZOSTAŁY JUŻ PODJĘTE?

Aby ograniczyć negatywne skutki wykrytego ataku – MyDr 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 - jako administrator Pani/Pana danych osobowych, po otrzymaniu zawiadomienia o naruszeniu od MyDr, dokonała zgłoszenia tego naruszenia do Prezesa Urzędu Ochrony Danych Osobowych.

V. GDZIE MOŻNA UZYSKAĆ DALSZE INFORMACJE?

W przypadku dodatkowych pytań dotyczących zakresu incydentu prosimy o kontakt pod adresem e-mail: dane@mydr.pl

Z poważaniem
Zespół Healthcare International sp. j.

Personal Data Breach Notification – MyDr EDM

I. WHAT HAPPENED?

We regret to inform you that the system of our processor, i.e. MyDr sp. z o.o. with its registered office in Warsaw (hereinafter: "MyDr"), was the target of a cyberattack, which resulted in a breach of the confidentiality of your personal data. MyDr is a provider of specialized software for maintaining electronic medical records, used by numerous healthcare providers in Poland.

We would like to emphasize that this does not mean that your data has been read, used or made publicly available. MyDr teams and external experts are continuously monitoring the situation and have not detected any public disclosure of the data affected by the incident. The forensic investigations conducted have confirmed that the incident has been contained and that there is no evidence of any further unauthorized access to the systems.

The findings regarding the incident indicate that it may have affected data processed before 12 April 2024. In individual cases, the scope of the incident may also have included data contained in cancelled medical examination referrals issued after that date. Depending on the scope of data processed in the system, the data affected by the incident may have included: your first and last name, residential address, contact details, PESEL number or other identification data, health data, social security data and, where provided, information concerning your employer.

The continuous monitoring conducted by MyDr to date has not identified any cases of the use or public disclosure of the data affected by the incident. However, it cannot be ruled out that this data may be used in the future in an unauthorized manner, which, depending on the circumstances, may involve a risk to your rights and freedoms.

With this in mind, we provide below information on the possible consequences of the incident and practical recommendations regarding measures that may help increase the security of your personal data and limit any potential consequences of its unauthorized use.

II. WHAT POTENTIAL CONSEQUENCES HAVE WE IDENTIFIED?

If your PESEL number was among the data affected by the incident, its combination with your first and last name and other identification or contact details could, in certain circumstances, be used by unauthorized persons for unlawful purposes. In particular, if such data were made publicly available, it could be used to:

- take out a loan or credit or enter into other agreements without your knowledge;
- gain access to your health information at medical institutions where individuals are authenticated using their PESEL number.

If unauthorized persons gained access to health data, its use could in turn lead to a violation of your privacy and, in certain circumstances, could also result in:

- the use of such information in a manner detrimental to you, including in a way that could result in a violation of your rights or less favourable treatment in your local community;
- fraud, for example by contacting you or your relatives in order to offer alternative methods of treating illnesses diagnosed in you.

It should nevertheless be emphasized that these are potential scenarios associated with the nature of the data affected by the incident. The monitoring conducted by MyDr to date has not indicated that the data affected by the incident has been used or publicly disclosed.

III. WHAT ACTIONS CAN YOU TAKE?

In relation to your PESEL number:

- **you can have your PESEL number blocked free of charge** using the mObywatel mobile application, online via the mObywatel.gov.pl website, or in person at a municipal office (gmina, city or, where applicable, district office). Financial institutions are currently required to verify, when entering into agreements, whether a PESEL number has been blocked, which reduces the risk of the data being used to incur unauthorized financial obligations. Blocking your PESEL

number does not prevent you from registering with a doctor, filling a prescription or handling matters at a public office. More information is available at: https://www.gov.pl/web/gov/zastrzez-swoj-numer-pesel-lub-cofnij-zastrzezenie;
- **you can inform other medical facilities** where you receive medical services that third parties may attempt to use your PESEL number to pass an authorization or authentication process at those facilities.

In relation to health data:
- if the use of your data by unauthorized persons is confirmed, you may seek to protect your rights against those persons under applicable laws, including the Polish Civil Code;
- you should exercise particular caution with regard to any contact from unknown persons who have information about your medical history that they should not have access to and who offer you medical, alternative or therapeutic services.

Regardless of the type of personal data concerned, if you suspect that your data has been used unlawfully, you may report this to the Police. Information on how to report a crime is available at: https://www.gov.pl/web/gov/zglos-przestepstwo.

We emphasize once again that the monitoring conducted by MyDr has not identified any cases to date of the use or public disclosure of the data.

IV. WHAT ACTIONS HAVE ALREADY BEEN TAKEN?

In order to limit the negative consequences of the detected attack, MyDr has taken the following actions:
1. promptly contained and resolved the incident and implemented additional, targeted technical and organizational measures aimed at preventing similar incidents in the future;
2. engaged a specialized cybersecurity company to conduct a detailed analysis of the incident;
3. reported the incident to a specialized Police unit – the Central Cybercrime Bureau (Centralne Biuro Zwalczania Cyberprzestępczości) – and is cooperating closely with it;
4. is cooperating with the Ministry of Digital Affairs, the e-Health Centre (Centrum e-Zdrowia), CSIRT NASK and CSIRT Centrum e-Zdrowia;
5. is cooperating with the Personal Data Protection Office (Urząd Ochrony Danych Osobowych);
6. continues to monitor its systems in order to detect any potential consequences of the incident and respond promptly to emerging threats;
7. conducts continuous monitoring of the Internet in order to detect whether the data affected by the incident has been made publicly available.

Our facility, as the controller of your personal data, after receiving notification of the breach from MyDr, reported the breach to the President of the Personal Data Protection Office (Prezes Urzędu Ochrony Danych Osobowych).

V. WHERE CAN YOU OBTAIN FURTHER INFORMATION?
If you have any additional questions concerning the scope of the incident, please contact at: dane@mydr.pl

Yours sincerely,
Healthcare International sp. j. Team