

Zawiadomienie o naruszeniu ochrony danych osobowych

Szanowni Państwo,

działając zgodnie z art. 34 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 („RODO”), przekazujemy Państwu informację o naruszeniu ochrony danych osobowych pacjentów Estebelle.

Zależy nam na przekazaniu tej informacji w sposób możliwie jasny i na przedstawieniu działań, które mogą Państwo podjąć w celu ograniczenia potencjalnych negatywnych skutków zdarzenia.

1. Co się wydarzyło?

Estebelle korzysta z systemu informatycznego MEDYC dostarczanego przez Qbusoft sp. z o.o. Dostawca systemu przetwarza dane osobowe pacjentów na rzecz Estebelle jako podmiot przetwarzający.

25.09.2026 r. otrzymaliśmy informację, że doszło do cyberataku na system MEDYC i nieuprawnionego dostępu do danych znajdujących się w tym systemie.

Naruszenie nastąpiło w środowisku informatycznym dostawcy systemu MEDYC. Incydent nie był wynikiem włamania do wewnętrznych systemów informatycznych Estebelle.

Po otrzymaniu informacji o zdarzeniu rozpoczęliśmy działania mające na celu ustalenie jego zakresu, ocenę ryzyka dla naszych pacjentów oraz ograniczenie możliwych negatywnych konsekwencji.

2. Jakie dane zostały objęte naruszeniem?

Z posiadanych przez nas informacji wynika, że nieuprawniony dostęp mógł objąć dane osobowe pacjentów znajdujące się w systemie MEDYC, w tym w szczególności:

- imię i nazwisko;
- numer PESEL;
- dane kontaktowe, w tym numer telefonu i adres e-mail jeżeli były zapisane w systemie;
- dane adresowe jeżeli były zapisane w systemie;
- dane dotyczące wizyt i korzystania ze świadczeń;
- dane zawarte w dokumentacji medycznej;
- informacje dotyczące stanu zdrowia;
- informacje dotyczące przeprowadzonych konsultacji, badań, diagnoz, zabiegów, leczenia i innych świadczeń medycznych;
- inne informacje dotyczące zdrowia i procesu leczenia znajdujące się w dokumentacji prowadzonej w systemie MEDYC.

3. Jakie mogą być konsekwencje naruszenia?

Ze względu na zakres danych objętych incydem, w szczególności ujawnienie numeru PESEL oraz danych dotyczących zdrowia, naruszenie może powodować wysokie ryzyko dla praw i wolności osób, których dane dotyczą.

Potencjalne konsekwencje mogą obejmować w szczególności:

- wykorzystanie danych do prób podszywania się pod Państwa;
- próby wyłudzenia dodatkowych danych osobowych lub informacji finansowych;
- wykorzystanie danych w próbach oszustwa lub kradzieży tożsamości;
- próby zaciągnięcia zobowiązań z wykorzystaniem danych osobowych;
- kierowanie do Państwa spersonalizowanych wiadomości phishingowych, SMS-ów lub telefonów, w których sprawcy mogą wykorzystywać znajomość Państwa danych;
- próby uzyskania dostępu do informacji lub dokumentacji medycznej;
- wykorzystanie informacji dotyczących zdrowia w sposób niezgodny z Państwa wolą;
- utratę kontroli nad informacjami dotyczącymi Państwa zdrowia i życia prywatnego;
- naruszenie prywatności lub dobrego imienia;
- szkody materialne lub niematerialne.

Samo wystąpienie naruszenia nie oznacza, że powyższe konsekwencje wystąpią, jednak ze względu na charakter ujawnionych informacji rekomendujemy podjęcie opisanych poniżej środków ostrożności.

4. Co rekomendujemy Państwu zrobić?

Zastrzeżenie numeru PESEL

Rekomendujemy zastrzeżenie numeru PESEL.

Można to zrobić bezpłatnie:

- w aplikacji mObywatel;
- przez serwis gov.pl;
- osobiście w urzędzie gminy.

Zastrzeżenie numeru PESEL ogranicza możliwość wykorzystania go m.in. do zaciągania określonych zobowiązań finansowych na Państwa dane.

Zachowanie szczególnej ostrożności

Prosimy również:

- zachować szczególną ostrożność wobec telefonów, wiadomości SMS oraz e-maili, w których nadawca powołuje się na Estebelle, placówkę medyczną, bank, urząd lub inną instytucję;

- nie przekazywać telefonicznie lub przez wiadomości kodów autoryzacyjnych, haseł ani danych logowania;
- nie klikać w linki ani nie otwierać załączników w nieoczekiwanych wiadomościach;
- zwracać szczególną uwagę na wiadomości, w których nadawca zna Państwa imię, nazwisko, PESEL lub informacje związane z leczeniem - posiadanie takich informacji nie oznacza, że nadawca jest osobą uprawnioną;
- monitorować rachunki bankowe oraz informacje dotyczące zobowiązań zaciąganych na Państwa dane;
- rozważyć korzystanie z usług informujących o próbach wykorzystania Państwa danych, w szczególności alertów dotyczących zapytań kredytowych;
- w przypadku podejrzenia wykorzystania Państwa danych przez osoby nieuprawnione niezwłocznie skontaktować się z odpowiednią instytucją oraz rozważyć zawiadomienie Policji.

Jeżeli otrzymają Państwo nietypową wiadomość lub telefon dotyczący wizyty, leczenia lub dokumentacji medycznej, rekomendujemy potwierdzenie autentyczności kontaktu bezpośrednio z placówką przy wykorzystaniu znanych Państwu danych kontaktowych, a nie danych podanych w otrzymanej wiadomości.

5. Jakie działania podjęła Estebelle?

Po otrzymaniu informacji o incydencie podjęliśmy działania zmierzające do ograniczenia jego skutków oraz ochrony osób, których dane dotyczą.

W szczególności:

- rozpoczęliśmy analizę zakresu naruszenia oraz jego potencjalnych konsekwencji dla pacjentów;
- pozostajemy w kontakcie z dostawcą systemu MEDYC i pozyskujemy informacje dotyczące przebiegu, zakresu i skutków incydentu;
- zweryfikowaliśmy ryzyko związane z naruszeniem danych osobowych pacjentów;
- podjęliśmy działania mające na celu ustalenie osób, których dane mogły zostać objęte incydem;
- przekazujemy osobom, których dane dotyczą, niniejsze zawiadomienie wraz z rekomendowanymi środkami ograniczającymi ryzyko;
- monitorujemy dalszy rozwój sytuacji i będziemy podejmować kolejne działania, jeżeli okażą się konieczne.

Naruszenie zostało również zgłoszone Prezesowi Urzędu Ochrony Danych Osobowych.

Współpracujemy z dostawcą systemu w celu uzyskania pełnych informacji dotyczących incydentu oraz zastosowanych przez niego środków naprawczych i zabezpieczających.

6. Kto jest administratorem Państwa danych?

Administratorem Państwa danych osobowych jest:

AGNIESZKA NALEWCZYŃSKA ESTEBELLE spółka z o.o. z siedzibą w Warszawie (kod pocztowy: 02-920), przy ul. Powsińskiej 8, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod numerem KRS: 0001252978, NIP: 9512567401, REGON: 525175552,

System MEDYC jest rozwiązaniem informatycznym dostarczonym przez zewnętrznego dostawcę, który w zakresie danych pacjentów przetwarzanych na rzecz Estebelle działa jako podmiot przetwarzający.

Incydent będący przedmiotem niniejszego zawiadomienia dotyczył systemu MEDYC dostawcy i nie był skutkiem włamania do wewnętrznej infrastruktury informatycznej Estebelle.

7. Gdzie można uzyskać dodatkowe informacje?

Jeżeli mają Państwo pytania dotyczące naruszenia, jego potencjalnych konsekwencji lub działań, które mogą Państwo podjąć, prosimy o kontakt z Inspektorem Ochrony Danych:

Inspektor Ochrony Danych
e-mail: iod@estebelle.com.pl

Prosimy, aby w wiadomościach kierowanych do Inspektora Ochrony Danych nie przysyłać dodatkowych danych dotyczących zdrowia, jeżeli nie jest to konieczne do wyjaśnienia sprawy.

Przepraszamy za sytuację i związane z nią niedogodności. Bezpieczeństwo danych naszych pacjentów traktujemy bardzo poważnie i będziemy monitorować sprawę oraz podejmować dalsze działania adekwatne do pojawiających się informacji.

Klinika Estebelle