Informacja o naruszeniu ochrony Państwa danych osobowych

Szanowni Państwo,

z przykrością informujemy o incydencie dotyczącym Państwa danych osobowych, do którego doszło u dostawcy systemu Medyc - Qbusoft sp. z o.o. (KRS: 0000740021, dalej: **Qbusoft**). Wiadomość kierujemy do pacjentów naszego ośrodka w Gdyni, których dane były zapisane w tym systemie.

Charakter oraz okoliczności naruszenia

FutureMeds sp. z o.o. z siedzibą we Wrocławiu (KRS: 0000394487, dalej: **FutureMeds**) korzystała w ośrodku w Gdyni z systemu Medyc, czyli oprogramowania do rejestracji pacjentów i prowadzenia elektronicznej dokumentacji medycznej. System dostarczał i utrzymywał Qbusoft, który odpowiadał również za jego zabezpieczenie. Qbusoft przetwarzał dane naszych pacjentów w naszym imieniu jako podmiot przetwarzający, na podstawie zawartej z nami umowy powierzenia przetwarzania danych osobowych - administratorem Państwa danych pozostaje FutureMeds.

W sierpniu 2026 r. Qbusoft wykrył nieprawidłowości w infrastrukturze systemu Medyc, a 9 września 2026 r. przekazał nam informację o incydencie bezpieczeństwa. Nie potwierdził wtedy, że incydent objął dane naszych pacjentów. Niezwłocznie zwróciliśmy się do Qbusoft o wyjaśnienia i 19 września 2026 r. otrzymaliśmy potwierdzenie, że w wyniku cyberataku osoby nieuprawnione wykradły dane pacjentów, w tym ich dane identyfikacyjne i kontaktowe, i że należy przyjąć, iż dysponują nimi w postaci umożliwiającej odczyt.

Aby rzetelnie ustalić, kogo dotyczy zdarzenie, potrzebowaliśmy od Qbusoft zbioru danych w stanie z dnia wycieku. **Mimo wielokrotnych wezwań otrzymaliśmy go dopiero w październiku 2026 r.** Na tej podstawie ustaliliśmy, że naruszenie dotyczy danych wprowadzonych do systemu do 22 sierpnia 2026 r., i przygotowaliśmy listę osób, do których kierujemy zawiadomienia.

Do naruszenia doszło w systemach Qbusoft, a nie w systemach informatycznych ani w siedzibie FutureMeds. Według informacji publicznych sprawą zajmuje się Centralne Biuro Zwalczania Cyberprzestępczości Policji. Po otrzymaniu od Qbusoft potwierdzenia wycieku wstrzymaliśmy korzystanie z systemu Medyc i przygotowujemy zmianę dostawcy.

Według naszej wiedzy na dzień wysłania tej wiadomości dane objęte incydentem nie zostały opublikowane ani wystawione na sprzedaż. Nie możemy jednak wykluczyć, że ktoś spróbuje je wykorzystać, dlatego prosimy o zapoznanie się z zaleceniami poniżej.

Bardzo przepraszamy za tę sytuację. Wiemy, że taka wiadomość może budzić niepokój.

Jakiego zakresu danych dotyczy naruszenie?

Na podstawie informacji przekazanych przez Qbusoft oraz analizy zbioru, który od niego otrzymaliśmy:

1. **wyciek na pewno objął:** imię i nazwisko, adres zamieszkania, numer telefonu i adres e-mail (w zakresie, w jakim były zapisane w systemie). W zbiorze, którego wyciek potwierdził Qbusoft, nie było zapisanego Państwa numeru PESEL;
2. **wysoce prawdopodobny jest wyciek** plików dołączonych do kartoteki pacjenta, czyli zdjęć i dokumentów PDF, w tym zawierających dokumentację medyczną i wyniki badań laboratoryjnych;

3. **nie można wykluczyć wycieku** pozostałych danych zapisanych w systemie - w szczególności danych dotyczących zdrowia zawartych w dokumentacji medycznej (informacji o wizytach, rozpoznań, zaleceń, recept, skierowań, zwolnień lekarskich i wyników badań), a także - jeżeli zostały podane - danych dokumentu tożsamości i informacji o rozliczeniach za wizyty. Zbiór danych objętych wyciekiem, który otrzymaliśmy od Qbusoft, nie zawiera tych danych - obejmuje wyłącznie dane wskazane w pkt 1. Qbusoft nie ustalił jednak, czy pozostałe dane zostały wyprowadzone, i nie wyklucza tego - dlatego z daleko idącej ostrożności przyjmujemy, że mogły zostać objęte wyciekiem.

Zakres danych zapisanych w systemie zależy od tego, jakie informacje zostały podane przy rejestracji i z jakich świadczeń korzystali Państwo w naszym ośrodku. Jeżeli chcą Państwo poznać dokładny zakres swoich danych przetwarzanych w systemie Medyc, prosimy o kontakt na dane wskazane w części **„Gdzie mogą Państwo uzyskać więcej informacji?”**.

Przeciwdziałanie negatywnym skutkom naruszenia

Aby ograniczyć ewentualne negatywne skutki naruszenia, zalecamy zachowanie szczególnej ostrożności, w tym przede wszystkim:

1. **z ostrożności - bezpłatne zastrzeżenie numeru PESEL.** W zbiorze, którego wyciek potwierdził Qbusoft, nie było Państwa numeru PESEL. Nie możemy jednak wykluczyć, że numer ten znajdował się w dokumentach dołączonych do kartoteki (np. w wynikach badań), dlatego zalecamy jego zastrzeżenie:
   - w aplikacji mObywatel;
   - na stronie mobywatel.gov.pl;
   - osobiście w dowolnym urzędzie gminy.

   Banki i inne instytucje mają obowiązek sprawdzić status numeru PESEL przed zawarciem umowy, np. kredytu lub pożyczki, więc zastrzeżenie realnie utrudnia posłużenie się Państwa danymi. Zastrzeżenie nie wpływa na korzystanie z leczenia i można je w każdej chwili cofnąć, np. gdy sami będą Państwo chcieli zawrzeć taką umowę;
2. **z ostrożności - jeżeli przy rejestracji podawali Państwo numer dowodu osobistego lub paszportu:** zapytanie w swoim banku o możliwość zastrzeżenia dokumentu w systemie Dokumenty Zastrzeżone, z którego korzystają m.in. banki przy weryfikacji tożsamości;
3. **sprawdzenie, czy Państwa login lub adres e-mail pojawił się w innych wyciekach, w rządowym serwisie bezpiecznedane.gov.pl (po zalogowaniu profilem zaufanym)** - serwis pokazuje wyłącznie wycieki, których bazy zostały do niego wprowadzone; nie mamy informacji, aby trafiły do niego dane z systemu Medyc;
4. zachowanie czujności wobec nieoczekiwanych telefonów, SMS-ów i e-maili powołujących się na nasz ośrodek, wizytę, wyniki badań, dopłatę albo „wyciek danych”. Nie należy podawać haseł, kodów z SMS-ów ani danych karty, instalować aplikacji ani klikać w linki na prośbę rozmówcy. Numer wyświetlany na ekranie może być podrobiony - w razie wątpliwości najlepiej się rozłączyć i samodzielnie zadzwonić na oficjalny numer. Podejrzane SMS-y można bezpłatnie przesłać do CERT Polska na numer 8080;
5. **zachowanie ostrożności** wobec osób powołujących się na wiedzę o Państwa badaniach, leczeniu lub dokumentacji medycznej - w szczególności, jeżeli proponują skorzystanie z usług medycznych, pseudomedycznych lub terapeutycznych;
6. **rozważenie zmiany danych, które uległy ujawnieniu, w zakresie, w jakim to możliwe** (np. numeru telefonu lub adresu e-mail), a także włączenie logowania dwuskładnikowego w poczcie e-mail i bankowości elektronicznej;
7. **regularne sprawdzanie Internetowego Konta Pacjenta** (pacjent.gov.pl) - czy nie pojawiły się w nim wystawione na Państwa dane recepty, skierowania lub zwolnienia lekarskie, o których Państwo nie wiedzą;
8. zgłoszenie sprawy na Policję w przypadku podejrzenia, że Państwa dane zostały wykorzystane niezgodnie z prawem - informacje o sposobie zgłoszenia znajdują się na stronie gov.pl/web/gov/zglos-przestepstwo;

9. rozważenie skorzystania ze środków ochrony dóbr osobistych przewidzianych w Kodeksie cywilnym i Kodeksie postępowania cywilnego (np. powództwo o zadośćuczynienie lub odszkodowanie za naruszenie dóbr osobistych);
10. skorzystanie ze wsparcia psychologicznego w sytuacji silnego stresu lub niepokoju.

W związku z naruszeniem mogą Państwo również wnieść skargę do Prezesa Urzędu Ochrony Danych Osobowych (ul. Stanisława Moniuszki 1A, 00-014 Warszawa).

Możliwe skutki naruszenia ochrony danych osobowych

Na dzień wysłania tej wiadomości **nie mamy informacji, aby Państwa dane zostały wykorzystane w sposób nieuprawniony**. Z daleko idącej ostrożności wskazujemy jednak, że następstwem zdarzenia mogą być:

1. jeżeli Państwa numer PESEL znajdował się w dokumentach dołączonych do kartoteki - próby posłużenia się nim, np. przy zaciąganiu kredytu lub pożyczki, korzystaniu ze świadczeń opieki zdrowotnej albo wystawianiu recept, skierowań lub zwolnień lekarskich;
2. kierowanie do Państwa spersonalizowanych wiadomości wyłudzających (tzw. phishing), w których nadawca podaje się za naszą placówkę, przychodnię, bank lub urząd i powołuje się na Państwa dane, aby wydawać się wiarygodny;
3. próby oszustwa lub szantażu z wykorzystaniem wiedzy o Państwa stanie zdrowia, badaniach lub korzystaniu z określonych świadczeń, w tym oferowanie „alternatywnych" metod leczenia;
4. niechciane wiadomości, telefony lub korespondencja na adres zamieszkania od osób, które weszły w posiadanie Państwa danych;
5. naruszenie Państwa dóbr osobistych lub dyskryminacja - ze względu na to, że naruszenie mogło objąć dane dotyczące zdrowia, czyli dane szczególnej kategorii.

Działania podjęte w związku z naruszeniem

Zgodnie z obowiązkiem prawnym ciążącym na FutureMeds naruszenie zostało zgłoszone Prezesowi Urzędu Ochrony Danych Osobowych. Kolejnym krokiem jest skierowanie do Państwa tego zawiadomienia. Ponadto FutureMeds:

1. wielokrotnie wzywała Qbusoft do wyjaśnień oraz do przekazania pełnych informacji o zdarzeniu i danych objętych wyciekiem;
2. wstrzymała korzystanie z systemu Medyc i przygotowuje zmianę dostawcy;
3. uruchomiła dedykowaną infolinię i adres e-mail do obsługi pytań w tej sprawie (dane poniżej);
4. opublikowała komunikat dotyczący naruszenia na swojej stronie internetowej: futuremeds.pl/medyc.

Qbusoft poinformował publicznie, że zgłosił incydent właściwym organom, w tym Policji i Prezesowi Urzędu Ochrony Danych Osobowych.

Co robimy, aby taka sytuacja nie powtórzyła się w przyszłości?

Przygotowujemy zmianę dostawcy systemu do prowadzenia dokumentacji medycznej dla ośrodka w Gdyni. Przy wyborze nowego dostawcy szczególną uwagę zwracamy na stosowane przez niego środki bezpieczeństwa - preferujemy podmioty posiadające certyfikaty w zakresie bezpieczeństwa informacji (np. ISO/IEC 27001). Przeglądamy także zasady współpracy z pozostałymi dostawcami, którym powierzamy dane, oraz wzmacniamy zasady weryfikacji tożsamości osób kontaktujących się z naszym ośrodkiem.

Gdzie mogą Państwo uzyskać więcej informacji?

W przypadku jakichkolwiek pytań lub chęci przekazania nam dodatkowych informacji w związku ze zdarzeniem prosimy o kontakt z zespołem powołanym do obsługi naruszenia:

1. e-mail: **alert@futuremeds.com**;
2. infolinia: **713 940 810**, od poniedziałku do czwartku w godz. 9:00-15:00.

Mogą Państwo również skontaktować się z naszym Inspektorem Ochrony Danych - Roksaną Lejpamer: **iod@futuremeds.com**.

Ewentualne dalsze aktualizacje będziemy publikować na naszej stronie internetowej: futuremeds.pl/medyc.

Jak rozpoznać, że ta wiadomość pochodzi od nas?

Ta wiadomość nie zawiera załączników ani linków do logowania i nie prosimy w niej o podanie żadnych danych ani o płatność. Jej treść mogą Państwo porównać z komunikatem na stronie futuremeds.pl/medyc. Jeżeli ktoś, powołując się na to zdarzenie, prosi o dane, hasła, kody lub płatność - **to nie jest wiadomość od nas.**

Adnotacja prawna do zawiadomienia

Przekazana informacja stanowi realizację obowiązku wynikającego z art. 34 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych; RODO).

Jeżeli dowiedzą się Państwo, że ktoś wykorzystał Państwa dane, prosimy o jak najszybsze przekazanie nam tej informacji na adres alert@futuremeds.com.

Z wyrazami szacunku
FutureMeds sp. z o.o.