

Szanowni Państwo!

Na podstawie pozyskanych informacji, z przykrością informujemy, że systemy informatyczne dostawcy usług w zakresie zarządzania udzielaniem świadczeń zdrowotnych (podmiotu przetwarzającego) Qbusoft Sp. z o.o. (producenta oprogramowania Medyc), padły ofiarą cyberataku, w wyniku którego doszło do naruszenia poufności jednostkowych danych medycznych w tym danych osobowych pacjentów naszej kliniki.

Pozyskane do tej pory od Qbusoft Sp. z o.o. oraz innych źródeł fragmentaryczne informacje wskazują, że incydent może posiadać, ze względu na jego charakter i skalę duży wpływ na realizację Państwa praw lub wolności. Jednocześnie zapewnimy z mocą, że klinika podjęła niezwłocznie działania w celu dogłębnego wyjaśnienia incydentu i utrzymywania w przyszłości możliwie najwyższego poziomu bezpieczeństwa powierzanych danych.

W ramach prowadzonych działań związanych z obsługą incydentu realizujemy procedurę informowania organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych.

W celu zminimalizowania potencjalnych skutków incydentu prosimy o zastosowanie szczególnych środków ostrożności.

W tym celu należy mieć na uwadze, że wśród danych objętych ujawnieniem znajduje się numer PESEL, który w połączeniu z imieniem, nazwiskiem oraz danymi kontaktowymi może posłużyć przestępcom m.in. do:

1. zaciągnięcia zobowiązania finansowego (kredytu, pożyczki) lub zawarcia innych umów cywilnoprawnych bez Pani/Pana wiedzy;
2. uzyskania dostępu do Pani/Pana danych zdrowia w innych instytucjach medycznych, w których uwierzytelnianie osób następuje wyłącznie przy pomocy numeru PESEL.
3. zakładania kont w mediach społecznych i publikowania opinii oraz informacji mogących wpływać na państwa i innych osób dobra osobiste (np. publikując na nich obraźliwe komentarze).

Incydent dotyczy również danych wrażliwych (danych o zdrowiu i procesie leczenia).

Ich nieuprawnione użycie może naruszać Państwa prawo do prywatności, w sposób szczególny wpływać na dobra osobiste. W szczególności, udostępnienie tego rodzaju danych podmiotom nieuprawnionym (przestępcom) może spowodować:

1. stygmatyzowanie w środowisku zamieszkania i pracy;
2. próby oszustwa, wyłudzenia pieniędzy poprzez kontakt telefoniczny, powoływanie się na wiedzę o odbytym leczeniu i oferowanie fikcyjnych usług medycznych czy terapeutycznych;
3. próbę szantażu, traktując wiedzę o Państwa zdrowiu jako narzędzie nacisku dla pozyskania okupu lub innych korzyści.

Mając powyższe na uwadze:

1. w odniesieniu do numeru PESEL rekomendujemy:

- 1) sprawdzenie statusu swoich danych w rządowym serwisie: bezpiecznedane.gov.pl
- 2) niezwłoczne zastrzeżenie numeru PESEL – można to zrobić całkowicie bezpłatnie w rządowej aplikacji mobilnej mObywatel, przez internet na stronie obywatel.gov.pl lub osobiście w dowolnym Urzędzie Gminy/Miasta. Instytucje finansowe mają ustawowy obowiązek weryfikować status PESEL przed zawarciem umowy pożyczki, co zablokuje przestępcom możliwość wyłudzenia pieniędzy na Państwa konto; zastrzeżenie PESEL nie wpływa na rejestrację do lekarza, zakup leków czy załatwianie spraw urzędowych. Więcej szczegółów znajdą Państwo na stronie Ministerstwa w zakładce: Zastrzeż swój numer PESEL;

- 3) poinformowanie innych świadczeniodawców, iż podmioty nieuprawnione weszły w posiadanie Pani/Pana danych i mogą podjąć próby pozyskania informacji oraz dostępu do dokumentacji medycznej;
- 4) jeśli masz taką możliwość, włączenie alertów BIK lub monitoringu kredytowego oraz regularne sprawdzanie historii swojego konta bankowego;
- 5) jeśli korzystałeś(-aś) z portalu pacjenta Medyc, zmianę hasła, także w innych serwisach, w których było ono takie samo.

2. W przypadku danych kontaktowych oraz danych o zdrowiu rekomendujemy:

- 1) zachować szczególną ostrożność i zasadę ograniczonego zaufania wobec wszelkich niespodziewanych kontaktów telefonicznych (głosowych), wiadomości SMS oraz e-mail od nieznanymi osób, instytucji, firm, które powołują się na historię Państwa zdrowia;
- 2) zachowanie szczególnej ostrożności wobec nieoczekiwanych telefonów, SMS-ów i e-maili z powołaniem na naszą placówkę; GOYA Medical nigdy nie prosi o podanie haseł, danych karty ani o dopłaty przez link w SMS-ie; w razie wątpliwości rozłącz się i zadzwoń do nas na numer ze strony internetowej;
- 3) w przypadku podejrzenia, że Państwa dane zostały już wykorzystane przez oszustów (np. otrzymali Państwo podejrzany SMS lub informację o próbie logowania), należy jak najszybciej zgłosić ten fakt na Policję; instrukcja, jak dokonać takiego zgłoszenia, znajduje się na stronie:

<https://www.gov.pl/web/gov/zglos-przestepstwo>

Jesteśmy w pełni świadomi, potencjalnych skutków incydentu, a w szczególności jego wpływu na Państwa życie osobiste i zawodowe. Kierując się poczuciem odpowiedzialności zawodowej i koniecznością dochowania wysokich standardów związanych z szeroko pojętym bezpieczeństwem pacjenta pozostajemy do Państwa pełnej informacyjnej dyspozycji.

Monitorujemy funkcjonowanie dostarczanego przez Qbusoft Sp. z o.o. systemu rejestracji i prowadzenia dokumentacji medycznej, obejmując jednocześnie naszą infrastrukturę IT wzmożonym nadzorem.

Istotne dla Państwa informacje dot. incydentu będą publikowane na bieżąco w naszym serwisie internetowym i podawane do publicznej wiadomości w siedzibie kliniki zgodnie z obowiązującymi w tym zakresie przepisami prawa.

W sprawach dot. incydentu mogą Państwo kontaktować się bezpośrednio z naszą kliniką pod adresem e-mail: naruszenie_medyc@goyamedical.pl

Z wyrazami szacunku,
GOYA Medical sp. z o.o.