Zawiadomienie o naruszeniu ochrony danych osobowych

Aktualizacja zawiadomienia z dnia 22.10.2026 r uwzględniające dodatkowe informacje dotyczące zakresu danych osobowych objętych naruszeniem

Szanowna Pani, Szanowny Panie,

Klinika Nova Sp. z o.o. jako Administrator Pani lub Pana danych osobowych informuje, że w wyniku nieautoryzowanego dostępu do serwera, na którym funkcjonował system Mantis służący do obsługi zgłoszeń serwisowych związanych z oprogramowaniem medycznym dostarczanym przez firmę Eurosoft, doszło do pozyskania w sposób nieuprawniony, mimo zastosowanych środków ich ochrony, danych osobowych 56 pacjentów Kliniki Nova Sp z o.o. Zdarzenie to dotyczyło danych przetwarzanych przez Eurosoft sp. z o.o, a działania hakerskie skierowane były przeciwko temu podmiotowi, a nie przeciwko Klinice Nova Sp. z o.o.

Co się wydarzyło:

Nasza placówka korzysta z systemu obsługi zgłoszeń serwisowych udostępnianego przez Eurosoft sp. z o.o. z siedzibą w Warszawie, będącą dostawcą użytkowanego przez nas oprogramowania medycznego.

W dniu 19 października 2026 r. dostawca poinformował nas, że w jego systemach do obsługi zgłoszeń osoba nieuprawniona uzyskała dostęp do danych.

Naruszenie nie wystąpiło w systemach Kliniki Nova i nie mogliśmy temu zapobiec. Jako administrator Państwa danych mamy jednak obowiązek Państwa o nim powiadomić.

Jakich danych może dotyczyć:

- imienia i nazwiska, numeru PESEL, daty urodzenia,
- numeru telefonu, adresu zamieszkania
- informacji dotyczących udzielania świadczeń zdrowotnych w zakresie miejsca udzielania świadczeń, np. oddziału lub poradni POZ, rodzaju zabiegu oraz informacji o recepcie na leki, zrealizowanych wizytach
- informacje dotyczące podstawowej opieki zdrowotnej: dane dotyczące aktywnej deklaracji POZ, jej zatwierdzenia przez NFZ oraz dane lekarza.
- dane dotyczące zdrowia: w przypadku jednego pacjenta pojedynczy wynik badania laboratoryjnego

Dane te znajdowały się w treści zgłoszenia serwisowego.

Dodatkowe ustalenia dotyczące zakresu naruszenia

W toku dalszych czynności wyjaśniających uzyskaliśmy dodatkowe informacje dotyczące danych osobowych znajdujących się w zgłoszeniach serwisowych.

Potwierdzono, że zakres danych objętych naruszeniem był w niektórych przypadkach szerszy niż wskazany w pierwotnym zawiadomieniu. Dodatkowe ustalenia dotyczyły w szczególności danych identyfikacyjnych, kontaktowych, informacji o udzielonych świadczeniach zdrowotnych, deklaracjach POZ oraz wynikach badań laboratoryjnych. Zakres danych został ustalony indywidualnie na podstawie informacji i dokumentacji przekazanej przez dostawcę oprogramowania. Osoby, w przypadku których potwierdzono dodatkowe kategorie danych objętych naruszeniem, są informowane indywidualnie, stosownie do wyników oceny ryzyka.

Czym to grozi? Naruszenie może skutkować w szczególności:

- próbą zaciągnięcia kredytu, pożyczki albo zawarcia umowy abonamentowej na Państwa dane bez Pani/Pana wiedzy,
- telefonami i wiadomościami od osób podszywających się pod placówkę medyczną, aptekę, NFZ albo bank, powołujących się na wiedzę o Państwa wizytach lub lekach,
- ujawnieniem osobom nieuprawnionym informacji o stanie zdrowia objętych tajemnicą.

Co radzimy zrobić:

- W pierwszej kolejności osobom pełnoletnim rekomendujemy zastrzeżenie numeru PESEL w aplikacji mObywatel, w banku albo w urzędzie gminy oraz o zachowanie ostrożności wobec wiadomości i telefonów dotyczących zdrowia, recept i płatności. Zastrzeżenie w aplikacji mObywatel, serwis gov.pl lub w urzędzie miasta, gminy jest bezpłatne i można je cofnąć.

- Zalecamy zachowanie szczególnej ostrożności wobec wiadomości e-mail, SMS i połączeń telefonicznych od osób powołujących się na znajomość Pani/Pana danych osobowych lub kontaktów z naszą placówką.

- W razie podejrzenia oszustwa lub zauważenia nieuprawnionej transakcji prosimy niezwłocznie skontaktować się z bankiem, a w przypadku podejrzenia przestępstwa zawiadomić Policję i zachować otrzymane wiadomości oraz inne dowody.

- Podejrzane SMS-y można przekazywać do CERT Polska na numer **8080** — przesłanie wiadomości jest bezpłatne na terenie Polski. Podejrzane wiadomości e-mail i strony internetowe można zgłaszać przez formularz na stronie incydent.cert.pl.

Co zrobiliśmy:

Aby ograniczyć skutki wykrytego ataku Eurosoft sp. z o.o. procesor opanował incydent i wdrożył dodatkowe, ukierunkowane na ograniczenie negatywnych skutków incydentu, środki techniczne i organizacyjne dla zapobieżenia wystąpienia podobnych naruszeń w przyszłości. Eurosoft sp. z o.o. współpracuje z organami ścigania, w tym z właściwą miejscową prokuraturą rejonową oraz Prezesem Urzędu Ochrony Danych Osobowych.

Klinika Nova Sp. z o.o – jako Administrator Pani/Pana danych osobowych, po otrzymaniu zawiadomienia o naruszeniu od Eurosoft sp. z o.o., przeprowadziła wewnętrzną analizę skali i

charakteru potencjalnego wpływu tego zdarzenia na dane naszych pacjentów, a nadto podjęła działania wymagane przepisami dotyczącymi ochrony danych osobowych, w tym dokonała oceny naruszenia i jego potencjalnych konsekwencji dla osób, których dane dotyczą, w szczególności zgłosiła naruszenie ochrony danych osobowych do Prezesa Urzędu Ochrony Danych osobowych (UODO), zgodnie z wymogami RODO. Współpracujemy z dostawcą systemu (Eurosoft sp. z o.o.), aby uzyskać jak najwięcej informacji.

W związku z uzyskaniem dodatkowych informacji od Eurosoft sp. z o.o. dokonaliśmy ponownej analizy zakresu danych objętych naruszeniem oraz aktualizacji oceny ryzyka. Przygotowaliśmy zgłoszenie uzupełniające do Prezesa PUODO, a osoby w przypadku których stwierdzono wysokie ryzyko naruszenia ich praw lub wolności, zostały objęte działaniami informacyjnymi.

Kontakt:

ze strony Eurosoft: iod @ eurosoft .com. pl

Inspektor ochrony danych naszej placówki: e-mail: Zaklina Janiak tel. 777070113
e-mail: iodo @klinikanova .pl

Informacji udziela także rejestracja pod numerem: 77 70 70 100

Kędzierzyn-Koźle, 28 października 2026 r.

Wersja II z dnia 28.10.2026 r

Z wyrazami szacunku

Zarząd Kliniki NOVA Sp. z o.o.