Ustrzyki Dolne, dnia 26 października 2026 r.

Administrator Danych:
Rodzinne Centrum Medyczne "Kresy" Sp. z o.o.
ul. 29 Listopada 34C
38-700 Ustrzyki Dolne
biuro@rcmkresy.pl
NIP: 6891237639

Zawiadomienie o naruszeniu danych osobowych

(działanie w trybie art. 34 Rozporządzenia 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 – dalej jako RODO)

Szanowni Państwo,

Jako Rodzinne Centrum Medyczne „Kresy" bezpieczeństwo Państwa danych osobowych oraz danych medycznych traktujemy z najwyższą powagą i odpowiedzialnością. W związku z powyższym zawiadamiamy Państwa o wystąpieniu incydentu u zewnętrznego dostawcy oprogramowania medycznego, z którego usług korzysta nasza placówka.

Co się stało?

W dniu 07 października 2026 r. o godzinie 20:35 nasza placówka została poinformowana przez zewnętrznego dostawcę oprogramowania medycznego – FELG SOFTWARE – o zorganizowanym cyberataku na infrastrukturę informatyczną tego systemu. W wyniku ataku osoba nieuprawniona uzyskała dostęp do baz danych przechowywanych na serwerach dostawcy. Incydent miał miejsce wyłącznie po stronie zewnętrznej infrastruktury FELG Software, a nie w wewnętrznej sieci komputerów naszej placówki.

Dostawca oprogramowania zadeklarował, że w kolejnych dniach sukcesywnie będzie przekazywać gabinetom objętym zdarzeniem szczegółowe informacje dotyczące ich pacjentów, w szczególności: kategorie danych objętych zdarzeniem, okres z którego dane pochodzą, dokładną liczbę osób objętych naruszeniem i inne informacje jakie mogą nam pomóc w ocenie ryzyka.

Pomimo upływu czasu, FELG Software do chwili obecnej nie przekazał naszej placówce zindywidualizowanej listy osób ani szczegółowych danych technicznych.

Dlatego, kierując się troską o Państwa bezpieczeństwo oraz zasadą ostrożności, podjęliśmy decyzję o bezzwłocznym zawiadomieniu Państwa o potencjalnym ryzyku, nie czekając na zakończenie czynności wyjaśniających przez dostawcę oprogramowania. Równolegle wystąpiliśmy do FELG Software z formalnymi żądaniami przedstawienia natychmiastowych wyjaśnień i szczegółowego raportu z incydentu.

Kategorie danych osobowych, których dotyczyło naruszenie.

Z informacji ogólnych przekazanych przez FELG Software wynika, że incydent mógł objąć następujące kategorie danych:

- Imię i nazwisko
- Numer PESEL
- Adres zamieszkania
- Numer telefonu oraz adres poczty elektronicznej
- Daty wizyt, informacje o płatnościach oraz wystawionych receptach.

Możliwe skutki naruszenia ochrony danych osobowych.

Informujemy Państwa o incydencie przede wszystkim po to, aby umożliwić podjęcie standardowych kroków ostrożnościowych. Z punktu widzenia bezpieczeństwa danych, nieuprawniony dostęp do informacji kontaktowych i identyfikacyjnych wiąże się z potencjalnym ryzykiem:

- wykorzystania danych do prób nieautoryzowanego zawierania umów,
- otrzymywania fałszywych wiadomości lub telefonów mających na celu wyłudzenie od Państwa haseł lub płatności (phishing),
- naruszenia poufności podstawowych informacji o zrealizowanych u nas świadczeniach medycznych.

Wierzymy, że podjęcie prostych kroków profilaktycznych (opisanych w kolejnym punkcie) pozwoli w praktyce zneutralizować te zagrożenia.

Środki zaradcze i zalecenia – czyli co należy teraz zrobić?

W celu ochrony, przed sytuacjami, które wskazaliśmy powyżej, rekomendujemy podjęcie następujących działań:

- bezpłatne zastrzeżenie numeru PESEL: korzystając z aplikacji mObywatel, przez stronę internetową gov.pl logując się za pomocą Profilu Zaufanego lub osobiście w dowolnym urzędzie gminy – możecie Państwo zastrzec swój numer PESEL. Dzięki takiemu działaniu wszelkie nieuprawnione czynności związane z wzięciem kredytu, pożyczki itp. są automatycznie zablokowane. UWAGA! Musicie Państwo o tym pamiętać i przed planowaną wizytą w banku konieczne jest każdorazowe cofnięcie zastrzeżenia. Jeśli macie problem z zastrzeżeniem lub cofnięciem zastrzeżenia numeru PESEL możecie Państwo napisać na adres e-mail: zastrzeganie-pomoc@cyfra.gov.pl lub zadzwonić pod numer +48 422 535 460
- aktywacja alertów kredytowych: warto rozważyć uruchomienie usługi powiadomień SMS lub e-mail o próbach zaciągnięcia zobowiązań finansowych na Państwa dane np. poprzez alerty BIK (Biura Informacji Kredytowej) – wszystko załatwicie Państwo w Internecie na dedykowanych stronach BIK.
- wzmożona czujność na próby kontaktu (phishing i wyłudzenia): prosimy zachować szczególną ostrożność wobec niespodziewanych telefonów, wiadomości SMS czy e-mail od osób podających się za banki, firmy kurierskie lub instytucje publiczne. Prosimy nie klikać w podejrzane linki, nie podawać kodów BLIK ani haseł do bankowości.
- weryfikacja historii recept: zalecamy weryfikację zdarzeń medycznych na Państwa internetowym Koncie Pacjenta (pacjent.gov.pl) pod kątem obecności recept, które nie były Państwu przepisywane.

Środki jakie My podjęliśmy w celu zaradzenia naruszeniu

W celu ochrony danych i minimalizacji skutków zdarzenia nasza placówka niezwłocznie wdrożyła procedury naprawcze:

1. Zgłoszono incydent Prezesowi Urzędu Ochrony Danych Osobowych (UODO) w ustawowym terminie.
2. Przeprowadzono wewnętrzny audyt systemów informatycznych oraz natychmiast zmieniono hasła dostępowe do kont w systemie medycznym.
3. Zweryfikowano i zaktualizowano listę personelu posiadającego uprawnienia dostępowe do systemów.
4. Zlecono niezależny audyt dokumentacji ochrony danych osobowych.
5. Umowa powierzenia przetwarzania danych łącząca nas z FELG Software została skierowana do analizy prawnej, a do dostawcy skierowano oficjalne wezwanie do złożenia wyczerpujących wyjaśnień technicznych w celu zabezpieczenia ewentualnych roszczeń.

Kontakt

W przypadku pytań, wątpliwości lub chęci uzyskania wsparcia informacyjnego, prosimy o kontakt z wyznaczoną osobą:

- Osoba wyznaczona do kontaktu: **radca prawny Patrycja Szatkowska**
- Kontakt wyłącznie za pośrednictwem poczty e-mail: **patrycjaszatkowska@outlook.com**

Podsumowanie

Zdajemy sobie sprawę, że ta sytuacja może budzić Państwa niepokój, dlatego zależało nam na pełnej i bezpośredniej komunikacji. Pragniemy wyraźnie zaznaczyć, że incydent jest wyłącznym skutkiem przestępczego cyberataku na infrastrukturę zewnętrznego dostawcy oprogramowania, a nie efektem zaniedbania czy naruszenia zabezpieczeń wewnątrz naszej placówki. Z informacji uzyskanych od FELG Software wynika, że dostawca jest w kontakcie z CERT Polska, CESIRT oraz UODO jak równie złożone zostało zawiadomienie do Prokuratury o popełnieniu przestępstwa.
Państwa spokój i bezpieczeństwo pozostają dla nas absolutnym priorytetem, dlatego sprawę traktujemy z najwyższą powagą. Pozostajemy w stałym kontakcie z właściwymi instytucjami oraz zewnętrznymi ekspertami. Jeżeli otrzymamy od FELG Software wiążące, zindywidualizowane ustalenia wskazujące, że Państwa dane zostały skopiowane przez sprawcę ataku, poinformujemy o tym w osobnym komunikacie.

Z wyrazami szacunku,
Rodzinne Centrum Medyczne "Kresy"