KOMUNIKAT

w sprawie naruszenia ochrony danych osobowych w systemie MyDr EDM.

Informacja dla Pacjentów, ich przedstawicieli ustawowych i osób upoważnionych oraz personelu

Szanowni Państwo,

Grupa Panda Med Holding sp. z o.o. z siedzibą w Katowicach, (dalej jako: „Administrator", „Administrator danych osobowych", „Grupa Panda Med Holding"), działając jako administrator danych osobowych pacjentów, informuje, że w systemie elektronicznej dokumentacji medycznej **MyDr EDM**, wykorzystywanym przez placówkę do obsługi dokumentacji medycznej pacjentów, doszło do incydentu bezpieczeństwa, w wyniku którego nieuprawniona osoba trzecia uzyskała dostęp do danych osobowych części pacjentów.

Poniżej przedstawiamy szczegółowe informacje dotyczące incydentu.

1. PRZEBIEG I OKOLICZNOŚCI INCYDENTU

Placówki medyczne należące do Grupy Panda Med korzystają z systemu MyDr EDM - oprogramowania służącego do prowadzenia elektronicznej dokumentacji medycznej oraz obsługi działalności placówek/ Dostawcą systemu jest firma MyDr, która odpowiada za jego utrzymanie, zabezpieczenie oraz tworzenie kopii zapasowych danych.

MyDr przetwarza dane osobowe pacjentów w imieniu Grupa Panda Med Holding, na podstawie zawartej umowy o współpracy. Oznacza to, że MyDr pełni funkcję podmiotu przetwarzającego, natomiast administratorem Państwa danych pozostaje Grupa Panda Med Holding.

W dniu 2 września 2026 r. otrzymaliśmy od MyDr informację o cyberataku na systemy tego dostawcy. W wyniku ataku osoby nieuprawnione uzyskały dostęp do baz danych zawierających kopie zapasowe systemu MyDr EDM, a następnie pozyskały kopię zapasową bazy danych z dnia 12 kwietnia 2024 r. Zdarzenie to doprowadziło do naruszenia poufności danych osobowych, w tym danych pacjentów placówek należących do Grupy Panda Med.

Chociaż sam cyberatak miał miejsce wcześniej, a informacje na jego temat zostały podane do wiadomości publicznej już w sierpniu 2026 r., dopiero 2 września 2026 r. otrzymaliśmy potwierdzenie, że naruszenie objęło również dane przetwarzane w ramach działalności naszych placówek. Niezwłocznie po uzyskaniu tej informacji podjęliśmy działania mające na celu ocenę skutków incydentu oraz ochronę danych osobowych pacjentów, opisane w dalszej części niniejszego komunikatu.

Zgodnie z informacjami przekazanymi przez MyDr, incydent został opanowany, a system MyDr EDM został zabezpieczony i funkcjonuje prawidłowo.

Na dzień publikacji niniejszego komunikatu nie stwierdzono przypadków wykorzystania ani publicznego udostępnienia danych osobowych pacjentów objętych incydentem.

2. GDZIE DOSZŁO DO NARUSZENIA I KTO ZA NIE ODPOWIADA?

Naruszenie ochrony danych osobowych nastąpiło w infrastrukturze informatycznej MyDr, będącego zewnętrznym dostawcą oprogramowania wykorzystywanego przez Grupę Panda Med Holding. Incydent nie był wynikiem ataku na systemy informatyczne ani infrastrukturę placówek należących do Grupy Panda Med Holding. Za cyberatak odpowiadają osoby nieuprawnione, które uzyskały dostęp do danych przechowywanych w systemach dostawcy.

Na podstawie zawartej umowy powierzenia przetwarzania danych osobowych oraz art. 28 i 32 RODO, MyDr, jako podmiot przetwarzający, jest zobowiązany do stosowania odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzanych danych. Obowiązki te obejmują w szczególności zabezpieczenie systemu MyDr EDM oraz przechowywanych w nim kopii zapasowych.

Jednocześnie **Grupa Panda Med Holding pozostaje administratorem danych osobowych swoich pacjentów** i realizuje wynikające z RODO obowiązki związane z naruszeniem ochrony danych. Obejmują one w szczególności ocenę ryzyka związanego z incydentem, dokonanie wymaganego zgłoszenia do Prezesa Urzędu Ochrony Danych Osobowych oraz poinformowanie osób, których dane dotyczą, o potencjalnych zagrożeniach i możliwych

sposobach ochrony. Zapewniamy również możliwość uzyskania dodatkowych informacji oraz zgłaszania pytań dotyczących zdarzenia.
Szczegółowe informacje dotyczące przebiegu incydentu oraz działań podjętych przez dostawcę oprogramowania zostały przedstawione przez MyDr w komunikacie **„MyDr - Informacja dla pacjentów”**, dostępnym pod adresem: https://pacjent.mydr.pl.

3. KOGO DOTYCZY NARUSZENIE?

Naruszenie ochrony danych osobowych dotyczy informacji wprowadzonych do systemu MyDr EDM przed dniem 12 kwietnia 2024 r. W pojedynczych przypadkach mogło również objąć dane zawarte w anulowanych skierowaniach na badania medyczne, wystawionych po tej dacie.

Zgodnie z dotychczasowymi ustaleniami incydent objął dane osobowe następujących grup osób, których informacje były przetwarzane w systemie MyDr EDM przez placówki należące do Grupy Panda Med Holding:

1. Pacjentów korzystających ze świadczeń medycznych w naszych placówkach.
2. Przedstawicieli prawnych pacjentów oraz osób upoważnionych do dostępu do ich dokumentacji medycznej.
3. Personelu medycznego i pozostałych pracowników placówek należących do Grupy Panda Med Holding.

Osoby, których dane zostały objęte naruszeniem i z którymi posiadamy możliwość bezpośredniego kontaktu, zawiadamiamy indywidualnie, za pośrednictwem poczty elektronicznej, wiadomości SMS lub korespondencji listownej.

Niniejszy komunikat kierujemy do wszystkich wymienionych grup. Jego celem jest zapewnienie możliwie szerokiego dostępu do informacji o zdarzeniu, również osobom, z którymi nie możemy skontaktować się bezpośrednio.

Jeżeli chcą Państwo ustalić, czy incydent objął również Państwa dane osobowe lub uzyskać szczegółowe informacje dotyczące zakresu danych objętych naruszeniem, prosimy o kontakt pod adresem poczty elektronicznej: rodo@grupapandamed.pl

Ze względu na charakter zdarzenia weryfikujemy tożsamość osób, które się z nami kontaktują, w sposób wzmocniony. Prosimy o wyrozumiałość - służy to ochronie Państwa danych.

4. JAKIEGO ZAKRESU DANYCH DOTYCZY NARUSZENIE?

Zakres danych osobowych objętych incydentem jest zróżnicowany i zależy od rodzaju relacji danej osoby z placówkami Grupy Panda Med Holding, a także od informacji przekazanych podczas rejestracji, udzielania świadczeń medycznych lub w ramach współpracy.

Poniżej przedstawiamy kategorie danych osobowych, które mogły zostać objęte naruszeniem. Należy podkreślić, że nie wszystkie wymienione informacje dotyczą każdej osoby rzeczywisty zakres danych zależy od informacji znajdujących się w systemie MyDr EDM.

1. Pacjenci

W przypadku pacjentów naruszenie mogło obejmować:

- imię i nazwisko;
- adres zamieszkania;
- dane kontaktowe, w tym numer telefonu i adres e-mail;
- numer PESEL;
- informacje dotyczące stanu zdrowia, w szczególności dane zawarte w dokumentacji medycznej prowadzonej w systemie MyDr EDM;
- dane dotyczące ubezpieczenia społecznego, jeżeli zostały wprowadzone do systemu;
- informacje o pracodawcy oraz inne dane identyfikacyjne, jeżeli były przetwarzane w systemie.

2. Przedstawiciele prawni pacjentów i osoby upoważnione

W przypadku przedstawicieli prawnych oraz osób upoważnionych do dostępu do dokumentacji medycznej pacjentów naruszenie mogło obejmować:

- imię i nazwisko;
- adres zamieszkania;
- dane kontaktowe, w tym numer telefonu i adres e-mail;
- numer PESEL;
- informacje dotyczące stopnia pokrewieństwa lub charakteru relacji z pacjentem.

3. Personel placówek Grupy Panda Med Holding

W przypadku personelu medycznego oraz pozostałych osób współpracujących z placówkami naruszenie mogło obejmować:

- imię i nazwisko;
- numer PESEL – w odniesieniu do personelu medycznego;
- numer prawa wykonywania zawodu (PWZ) – w odniesieniu do osób wykonujących zawody medyczne, dla których taki numer jest nadawany;
- informacje o specjalizacji lub wykonywanym zawodzie;
- informacje dotyczące pełnionej funkcji oraz harmonogramu pracy, jeżeli znajdowały się w systemie.

Ważne informacje dotyczące zakresu naruszenia

W przypadku osób, które korzystały ze świadczeń medycznych w placówkach Grupy Panda Med Holding, a jednocześnie występowały jako przedstawiciele prawni lub osoby upoważnione przez innych pacjentów, naruszenie mogło obejmować dane związane z obiema tymi rolami. Szczególnego podkreślenia wymaga fakt, że wśród danych objętych incydentem mogły znajdować się informacje dotyczące stanu zdrowia pacjentów. Są to dane należące do szczególnych kategorii danych osobowych w rozumieniu art. 9 RODO, podlegające podwyższonej ochronie prawnej. Informacje zawarte w dokumentacji medycznej są ponadto chronione przepisami dotyczącymi tajemnicy medycznej.

Mając na uwadze charakter tych informacji oraz potencjalne konsekwencje ich nieuprawnionego ujawnienia, Grupa Panda Med Holding traktuje zaistniałe zdarzenie z należytą powagą, podejmując działania zmierzające do ograniczenia ryzyka dla osób, których dane mogły zostać objęte naruszeniem.

5. JAKIE MOGĄ BYĆ SKUTKI NARUSZENIA?

W związku z nieuprawnionym dostępem do danych osobowych istnieje ryzyko ich wykorzystania przez osoby trzecie, w szczególności do:

1. podszywania się pod osobę, której dane dotyczą, lub podejmowania prób wyłudzenia dodatkowych informacji;
2. podejmowania prób zawarcia umów lub zaciągania zobowiązań z wykorzystaniem cudzych danych osobowych;

3. podejmowania prób uzyskania dostępu do usług, kont lub innych zasobów przy wykorzystaniu danych identyfikacyjnych;

4. kierowania spreparowanych wiadomości e-mail, SMS lub wykonywania połączeń telefonicznych mających na celu wyłudzenie dalszych danych, środków pieniężnych, danych logowania lub nakłonienie do wykonania określonych działań;

5. wykorzystania danych do innych form oszustwa lub kradzieży tożsamości.

Z uwagi na fakt, że naruszeniem objęte zostały również dane dotyczące zdrowia, możliwymi konsekwencjami mogą być ponadto:

1. nieuprawnione ujawnienie informacji dotyczących stanu zdrowia;

2. naruszenie prywatności, intymności, godności oraz prawa do zachowania informacji dotyczących zdrowia w poufności;

3. niekorzystne traktowanie lub dyskryminacja związana z ujawnieniem informacji dotyczących stanu zdrowia;

4. ostracyzm społeczny lub inne negatywne reakcje otoczenia wynikające z ujawnienia informacji dotyczących zdrowia;

5. stres, poczucie dyskomfortu, niepokoju lub utraty kontroli nad własnymi danymi wynikające ze świadomości, że informacje dotyczące zdrowia znalazły się w posiadaniu osoby nieuprawnionej.

Administrator podkreśla, że wskazane powyżej skutki mają charakter potencjalny. Informacja o naruszeniu danych nie oznacza, że którykolwiek z tych skutków rzeczywiście wystąpił lub wystąpi.

6. ZALECANE DZIAŁANIA PO STRONIE OSÓB OBJĘTYCH INDYDENTEM

W celu ograniczenia możliwości wykorzystania danych objętych naruszeniem Administrator zaleca osobom, których dane mogły zostać objęte incydentem, zachowanie zwiększonej ostrożności, a w szczególności:

1. zastrzeżenie numeru PESEL, np. za pośrednictwem aplikacji mObywatel, serwisu mObywatel.gov.pl lub w urzędzie gminy;

2. zachowanie szczególnej ostrożności wobec podejrzanych telefonów, wiadomości SMS, wiadomości e-mail i innych form kontaktu, w szczególności zawierających prośby o podanie dodatkowych danych osobowych, danych logowania, kodów autoryzacyjnych, dokonanie płatności lub kliknięcie w przesłany link;
3. niewykonywanie poleceń przekazywanych przez osoby, których tożsamości nie można zweryfikować, nawet jeżeli powołują się one na znajomość danych osobowych lub informacji dotyczących zdrowia;
4. okresową kontrolę informacji dotyczących zobowiązań finansowych, w szczególności poprzez sprawdzenie w Biurze Informacji Kredytowej, czy z wykorzystaniem danych nie zostało zaciągnięte nieznane zobowiązanie;
5. w przypadku podejrzenia wykorzystania danych dokumentu tożsamości, skontaktowanie się z właściwym organem lub instytucją w celu ustalenia, czy zachodzi potrzeba jego zastrzeżenia albo wymiany;
6. w przypadku utraty, kradzieży lub podejrzenia wykorzystania danych dokumentu tożsamości, rozważenie zastrzeżenia dokumentu w Międzybankowym Systemie Dokumenty Zastrzeżone;
7. niezwłoczne reagowanie na wszelkie nietypowe informacje o zobowiązaniach, umowach, wnioskach kredytowych, rachunkach lub innych czynnościach, których dana osoba nie podejmowała.

Administrator rekomenduje również, aby nie przekazywać telefonicznie ani elektronicznie numeru PESEL, danych dokumentu tożsamości, danych logowania, kodów jednorazowych ani danych bankowych, jeżeli nie ma pewności co do tożsamości osoby lub podmiotu, który o nie występuje.

W przypadku wystąpienia silnego stresu, niepokoju lub innych nasilonych reakcji emocjonalnych związanych z naruszeniem danych zalecamy skonsultowanie się z psychologiem lub innym odpowiednim specjalistą.

7. DZIAŁANIA PODJĘTE W ZWIĄZKU Z INCYDENTEM

Z informacji przekazanych Administratorowi przez dostawcę systemu MyDr wynika, że incydent został opanowany, system został zabezpieczony, a dostawca wdrożył dodatkowe

środki techniczne i organizacyjne mające na celu ograniczenie ryzyka wystąpienia podobnych zdarzeń w przyszłości.

W celu usunięcia skutków incydentu oraz zminimalizowania jego potencjalnych negatywnych konsekwencji podmiot przetwarzający dane, tj. dostawca systemu MyDr, poinformował o podjęciu w szczególności następujących działań:

1. zgłoszeniu incydentu wyspecjalizowanej jednostce Policji, tj. Centralnemu Biuru Zwalczania Cyberprzestępczości (CBZC), oraz podjęciu aktywnej współpracy z tą jednostką;
2. nawiązaniu współpracy z Ministerstwem Cyfryzacji, Centrum e-Zdrowia, CSIRT NASK oraz CSIRT Centrum e-Zdrowia;
3. podjęciu współpracy z Prezesem Urzędu Ochrony Danych Osobowych;
4. przygotowaniu dodatkowych funkcjonalności w systemie EDM MyDr mających usprawnić i przyspieszyć proces zawiadamiania pacjentów przez administratorów za pomocą wiadomości e-mail lub SMS, jeżeli administrator posiada odpowiednie dane kontaktowe;
5. wdrożeniu dodatkowych działań technicznych i organizacyjnych mających na celu zwiększenie bezpieczeństwa systemu.

Podmiot przetwarzający kontynuuje również monitorowanie dostępnych źródeł internetowych w celu ustalenia, czy dane przetwarzane w systemie MyDr zostały ujawnione lub upublicznione przez osobę nieuprawnioną. Z informacji przekazanych Administratorowi wynika, że według stanu na dzień przekazania informacji o incydencie nie stwierdzono, aby dane objęte naruszeniem zostały opublikowane w Internecie lub w inny sposób publicznie udostępnione.

Niezależnie od działań podejmowanych przez dostawcę systemu Administrator utrzymuje dostęp do systemu MyDr EDM wyłącznie dla osób upoważnionych oraz w zakresie niezbędnym do wykonywania powierzonych im obowiązków.

Po otrzymaniu informacji o naruszeniu Administrator dokonał również analizy stosowanych wewnętrznych procedur dotyczących ochrony danych osobowych, dostępu do systemów

informatycznych oraz reagowania na incydenty bezpieczeństwa pod kątem ich adekwatności do zaistniałej sytuacji.

Administrator na bieżąco monitoruje komunikaty i informacje przekazywane przez MyDr dotyczące incydentu, wdrożonych zabezpieczeń oraz ewentualnych dalszych ustaleń. W przypadku uzyskania nowych informacji, które mogą mieć wpływ na ocenę ryzyka dla praw i wolności osób, których dane dotyczą, Administrator dokona ponownej oceny sytuacji oraz, jeżeli będzie to konieczne, podejmie dalsze odpowiednie działania organizacyjne lub techniczne.

8. MOŻLIWE DZIAŁANIA PRAWNE W PRZYPADKU BEZPRAWNEGO WYKORZYSTANIA DANYCH

Jeżeli stwierdzą Państwo, że w związku z incydentem doszło do bezprawnego wykorzystania jej danych osobowych, naruszenia prywatności, dobrego imienia lub innych dóbr osobistych albo powstania szkody majątkowej lub niemajątkowej, może skorzystać ze środków ochrony przewidzianych w obowiązujących przepisach prawa.

W zależności od charakteru naruszenia oraz jego skutków mogą Państwo w szczególności:

1. wnieść skargę do Prezesa Urzędu Ochrony Danych Osobowych, jeżeli uznają Państwo, że przetwarzanie Państwa danych osobowych narusza przepisy RODO;
2. na podstawie art. 82 RODO dochodzić od administratora danych lub podmiotu przetwarzającego odszkodowania za poniesioną szkodę majątkową lub niemajątkową, jeżeli zachodzą przesłanki ich odpowiedzialności określone w RODO;
3. jeżeli doszło do zagrożenia lub naruszenia dóbr osobistych, w szczególności prywatności, godności lub poufności informacji dotyczących zdrowia, żądać zaniechania naruszenia oraz usunięcia jego skutków na zasadach określonych w przepisach Kodeksu cywilnego;
4. w przypadkach przewidzianych prawem dochodzić zadośćuczynienia pieniężnego lub innych roszczeń związanych z naruszeniem dóbr osobistych;
5. jeżeli dane zostały bezprawnie wykorzystane lub rozpowszechnione przez konkretną osobę lub podmiot, dochodzić odpowiednich roszczeń wobec osoby lub podmiotu odpowiedzialnego za takie działanie;

6. jeżeli istnieje podejrzenie, że dane zostały wykorzystane do popełnienia przestępstwa, w szczególności oszustwa, podszywania się pod inną osobę lub innego czynu zabronionego, zawiadomić Policję lub prokuraturę o podejrzeniu popełnienia przestępstwa.

Zakres dostępnych środków prawnych oraz podmiot, wobec którego mogą być kierowane roszczenia, zależą od okoliczności konkretnej sprawy, w szczególności od tego, kto dopuścił się naruszenia obowiązków wynikających z przepisów o ochronie danych osobowych, czy doszło do dalszego bezprawnego wykorzystania danych oraz czy w związku z naruszeniem powstała szkoda majątkowa lub niemajątkowa.

9. KONTAKT W SPRAWIE NARUSZENIA

W przypadku jakichkolwiek pytań lub chęci przekazania nam dodatkowych informacji w związku z zaistniałym zdarzeniem prosimy o kontakt:

Administrator danych osobowych:
Grupa Panda Med Holding sp. z o.o.
Wrocławska 54, 40-217 Katowice

Inspektor Ochrony Danych:
e-mail: rodo@grupapandamed.pl

Dodatkowe informacje dotyczące incydentu można uzyskać również pod adresem dane@mydr.pl

NAJCZĘŚCIEJ ZADAWANE PYTANIA
(FAQ)

I. INFORMACJE O ZDARZENIU

1. Czy dane wyciekły z placówek Grupy Panda Med Holding?

Nie. Zgodnie z otrzymanymi informacjami naruszenie nastąpiło w infrastrukturze informatycznej MyDr, czyli zewnętrznego dostawcy systemu służącego do prowadzenia elektronicznej dokumentacji medycznej. Osoby nieuprawnione uzyskały dostęp do baz danych zawierających kopie zapasowe systemu MyDr EDM i pozyskały kopię bazy danych z 12 kwietnia 2024 r.

Incydent nie był wynikiem ataku na systemy informatyczne ani infrastrukturę placówek Grupy Panda Med Holding.

2. Dlaczego to Grupa Panda Med Holding informuje mnie o naruszeniu, skoro doszło do niego u MyDr?

MyDr przetwarza dane osobowe w imieniu Grupa Panda Med Holding sp. z o.o. na podstawie zawartej umowy powierzenia przetwarzania danych osobowych. Grupa Panda Med Holding sp. z o.o. jako administrator danych, odpowiada za realizację obowiązków wynikających z RODO, w tym ocenę naruszenia, dokonanie wymaganego zgłoszenia do Prezesa Urzędu Ochrony Danych Osobowych oraz zawiadomienie osób, których dane dotyczą, jeżeli zachodzą przesłanki określone w przepisach. Dlatego przekazujemy Państwu informacje o zdarzeniu, jego potencjalnych konsekwencjach oraz zalecanych środkach ostrożności.

3. Kto ponosi odpowiedzialność za to zdarzenie?

Bezpośrednią przyczyną incydentu było działanie osób nieuprawnionych, które przeprowadziły cyberatak na infrastrukturę informatyczną MyDr. MyDr, jako podmiot przetwarzający, jest zobowiązany do zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzanych danych, w szczególności poprzez stosowanie właściwych środków technicznych i organizacyjnych chroniących system oraz przechowywane w nim kopie zapasowe. Jednocześnie Grupa Panda Med Holding sp. z o.o. jako administrator danych, realizuje własne obowiązki wynikające z RODO.

4. Kiedy Grupa Panda Med dowiedziała się o naruszeniu?

W dniu **2 września 2026 r.** otrzymaliśmy od MyDr informację pozwalającą ustalić, że incydent objął również dane przetwarzane przez Grupę Panda Med. Sam cyberatak miał miejsce wcześniej, a informacje o nim zostały podane do wiadomości publicznej w sierpniu 2026 r. Wcześniej nie dysponowaliśmy jednak potwierdzeniem, że zdarzenie dotyczy danych przetwarzanych w ramach naszej działalności. Po otrzymaniu tej informacji podjęliśmy działania związane z oceną incydentu i realizacją obowiązków wynikających z przepisów o ochronie danych osobowych.

5. Czy system MyDr EDM jest obecnie bezpieczny?

Zgodnie z informacjami przekazanymi przez MyDr, incydent został opanowany, a system MyDr EDM został zabezpieczony i funkcjonuje prawidłowo. Niezależnie od działań podjętych przez dostawcę analizujemy okoliczności naruszenia oraz stosowane zabezpieczenia, aby ograniczyć ryzyko wystąpienia podobnych zdarzeń w przyszłości.

II. CZY NARUSZENIE DOTYCZY MOICH DANYCH?

6. Dlaczego otrzymałam/otrzymałem wiadomość SMS od Grupy Panda Med Holding?

W związku z naruszeniem ochrony danych osobowych w systemie MyDr EDM skierowaliśmy do osób, których dane mogły zostać objęte incydentem, krótkie wiadomości SMS informujące o zaistniałym zdarzeniu.

Wiadomości te miały na celu **możliwie szybkie poinformowanie Państwa o naruszeniu oraz zwrócenie uwagi na konieczność zachowania ostrożności w związku z potencjalnym wykorzystaniem danych osobowych przez osoby nieuprawnione**.

7. Dlaczego wiadomość SMS zawiera jedynie krótką informację?

Ze względu na ograniczoną objętość wiadomości SMS nie jest możliwe przedstawienie w niej wszystkich informacji dotyczących naruszenia, jego potencjalnych konsekwencji oraz zalecanych środków ostrożności. Dlatego szczegółowe informacje udostępniamy w niniejszym komunikacie.

8. Nie otrzymałam/otrzymałem żadnej wiadomości. Czy oznacza to, że moje dane nie zostały objęte naruszeniem?

Niekoniecznie. Brak indywidualnego zawiadomienia nie oznacza, że Państwa dane nie znalazły się wśród informacji objętych incydentem. Może to wynikać między innymi z braku aktualnych danych kontaktowych lub niemożności ustalenia odpowiedniego sposobu kontaktu. Jeżeli chcą Państwo sprawdzić, czy naruszenie dotyczy również Państwa danych osobowych, prosimy o kontakt z administratorem danych.

9. Korzystałam/korzystałem z usług placówki tylko raz, kilka lat temu. Czy moje dane również mogły zostać objęte naruszeniem?

Tak. Naruszenie dotyczy danych znajdujących się w kopii zapasowej systemu MyDr EDM z 12 kwietnia 2024 r., a w pojedynczych przypadkach również danych zawartych w anulowanych skierowaniach wystawionych po tej dacie. Oznacza to, że incydent mógł objąć również dane archiwalne, w tym informacje dotyczące osób, które skorzystały ze świadczeń medycznych jednorazowo.

10. Jestem przedstawicielem ustawowym dziecka. Czy naruszenie mogło objąć również jego dane?

Tak. Naruszenie mogło dotyczyć zarówno danych dziecka jako pacjenta, w tym informacji o jego stanie zdrowia, jak i danych rodziców lub innych przedstawicieli ustawowych. W odniesieniu do danych przedstawiciela ustawowego incydent mógł obejmować między innymi imię i nazwisko, numer PESEL, dane kontaktowe oraz informacje dotyczące relacji z pacjentem.

Zalecamy zachowanie szczególnej ostrożności wobec prób podszywania się pod placówki medyczne i uzyskiwania informacji dotyczących dziecka. Możliwość zastrzeżenia numeru PESEL dotyczy obecnie osób pełnoletnich.

11. Korzystałam/korzystałem z usług placówki jako dziecko, ale obecnie jestem osobą pełnoletnią. Czy naruszenie może mnie dotyczyć?

Tak, jeżeli Państwa dane znajdowały się w systemie MyDr EDM w okresie objętym incydentem.

Zawiadomienie mogło zostać skierowane do rodzica lub opiekuna prawnego, jeżeli to jego dane kontaktowe były wskazane w dokumentacji medycznej. Jako osoby pełnoletnie mogą Państwo samodzielnie skorzystać z dostępnych środków ochrony tożsamości, w tym zastrzec numer PESEL.

12. Jestem lub byłam/byłem członkiem personelu Grupy Panda Med. Czy moje dane również mogły zostać objęte incydentem?

Tak. Naruszenie mogło objąć także dane personelu medycznego oraz innych osób, których informacje były przetwarzane w systemie MyDr EDM. W zależności od zakresu danych zapisanych w systemie mogły to być między innymi imię i nazwisko, numer PESEL, numer prawa wykonywania zawodu, specjalizacja, pełniona funkcja oraz harmonogram pracy. W celu uzyskania informacji o indywidualnym zakresie naruszenia prosimy o kontakt z administratorem danych.

III. ZAKRES DANYCH I POTENCJALNE ZAGROŻENIA

13. Jakie dokładnie moje dane zostały objęte naruszeniem?

Zakres danych objętych incydentem jest indywidualny i zależy od informacji wprowadzonych do systemu MyDr EDM podczas rejestracji, udzielania świadczeń medycznych lub w ramach współpracy z placówką. Naruszenie mogło obejmować między innymi dane identyfikacyjne, kontaktowe, numery PESEL oraz informacje dotyczące stanu zdrowia i udzielonych świadczeń medycznych.

Szczegółowy wykaz kategorii danych przedstawiliśmy we wcześniejszej części komunikatu.

14. Czy naruszenie objęło moją dokumentację medyczną, w tym wyniki badań, rozpoznania lub informacje o leczeniu?

Naruszenie mogło objąć również informacje dotyczące zdrowia zawarte w dokumentacji medycznej prowadzonej w systemie MyDr EDM. Mogły to być między innymi informacje o rozpoznaniach, wynikach badań, wystawionych receptach, skierowaniach oraz przebiegu leczenia, o ile znajdowały się w danych objętych incydentem. Nie oznacza to jednak, że wszystkie wymienione informacje dotyczą każdej osoby. Szczegółowy zakres zależy od zawartości dokumentacji przechowywanej w systemie.

15. Czy moje dane zostały opublikowane w internecie lub darknecie?

Zgodnie z informacjami przekazanymi przez MyDr, prowadzony przez dostawcę monitoring nie wykazał dotychczas przypadków publicznego udostępnienia danych objętych incydentem. Nie oznacza to jednak, że można całkowicie wykluczyć ich nieuprawnione wykorzystanie w przyszłości. Grupa Panda Med Holding sp. z o.o. nie ma możliwości samodzielnego zweryfikowania wszystkich potencjalnych sposobów wykorzystania pozyskanych danych, dlatego zalecamy stosowanie wskazanych w komunikacie środków ostrożności.

16. Czy ktoś może wykorzystać moje dane, aby podszyć się pode mnie lub uzyskać świadczenia medyczne?

Nie można całkowicie wykluczyć prób wykorzystania danych osobowych do podszywania się pod inną osobę. Nieuprawnione osoby mogą podejmować próby wyłudzenia dodatkowych informacji, na przykład poprzez kontakt telefoniczny lub wiadomości sugerujące konieczność potwierdzenia danych pacjenta, opłacenia świadczenia albo weryfikacji recepty. Zalecamy, aby nie przekazywać danych osobowych osobom, których tożsamości nie można wiarygodnie potwierdzić, oraz zachować szczególną ostrożność w kontaktach z podmiotami podającymi się za placówki medyczne.

IV. JAK CHRONIĆ SWOJE DANE?

17. Co powinnam/powinienem zrobić w pierwszej kolejności?

W związku z naruszeniem zalecamy przede wszystkim:

1. **Zastrzeżenie numeru PESEL** - jeżeli są Państwo osobami pełnoletnimi. Można to zrobić między innymi za pośrednictwem aplikacji mObywatel, serwisu mObywatel.gov.pl lub w urzędzie gminy.
2. **Zachowanie ostrożności wobec podejrzanych wiadomości i telefonów**, szczególnie dotyczących dokumentacji medycznej, recept, wyników badań lub konieczności potwierdzenia tożsamości.
3. **Nieudostępnianie haseł, kodów autoryzacyjnych oraz danych finansowych** osobom kontaktującym się z Państwem w nieoczekiwany sposób.
4. **Monitorowanie podejrzanych działań związanych z Państwa tożsamością**, w tym ewentualnych prób zaciągania zobowiązań finansowych lub uzyskiwania dostępu do kont internetowych.

18. Czy zastrzeżenie numeru PESEL utrudni mi korzystanie z usług medycznych?

Nie. Zastrzeżenie numeru PESEL nie ogranicza możliwości korzystania ze świadczeń zdrowotnych. Mechanizm ten służy przede wszystkim ograniczeniu ryzyka nieuprawnionego wykorzystania numeru PESEL przy określonych czynnościach prawnych, w szczególności przy zawieraniu umów kredytowych lub pożyczkowych. Zastrzeżenie można również czasowo cofnąć, gdy jest to konieczne do dokonania określonej czynności.

19. Czy mogę samodzielnie sprawdzić, czy moje dane znalazły się wśród informacji objętych wyciekiem?

Tak. Zachęcamy do skorzystania z rządowego serwisu **bezpiecznedane.gov.pl**, który umożliwia sprawdzenie informacji o danych objętych określonymi incydentami bezpieczeństwa. W celu uzyskania dodatkowych informacji dotyczących danych przetwarzanych przez Grupę Panda Med Holding mogą Państwo również zwrócić się bezpośrednio do nas.

20. Otrzymałam/otrzymałem podejrzaną wiadomość lub telefon od osoby podającej się za pracownika przychodni. Co powinnam/powinienem zrobić?

Zalecamy zachowanie szczególnej ostrożności i nieprzekazywanie żadnych dodatkowych danych osobowych do czasu potwierdzenia tożsamości rozmówcy. Nie należy klikać podejrzanych linków ani podawać haseł, kodów SMS czy danych kart płatniczych. Podejrzaną wiadomość warto zachować i zgłosić administratorowi danych. Próby oszustwa internetowego można zgłaszać również do CERT Polska, a w przypadku podejrzenia popełnienia przestępstwa - Policji.

V. PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ

21. Czy mogę uzyskać informację, jakie dane na mój temat były przetwarzane w systemie MyDr EDM?

Tak. Zgodnie z art. 15 RODO przysługuje Państwu prawo dostępu do danych osobowych, w tym uzyskania informacji o zakresie przetwarzanych danych. Wniosek w tej sprawie można skierować bezpośrednio do administratora danych lub Inspektora Ochrony Danych. Ze względów bezpieczeństwa w określonych przypadkach może być konieczna dodatkowa weryfikacja tożsamości osoby składającej wniosek.

22. Czy mogę zażądać usunięcia moich danych osobowych?

Tak. Przysługuje Państwu prawo wystąpienia z żądaniem usunięcia danych osobowych na zasadach określonych w art. 17 RODO. Należy jednak pamiętać, że prawo to nie ma charakteru bezwzględnego. W szczególności dokumentacja medyczna podlega ustawowym obowiązkom przechowywania przez określony czas, co może wyłączać możliwość jej usunięcia na żądanie pacjenta. Każdy wniosek rozpatrujemy indywidualnie, z uwzględnieniem obowiązujących przepisów.

23. Czy mogę złożyć skargę do organu nadzorczego?

Tak. Jeżeli uważają Państwo, że przetwarzanie danych osobowych narusza przepisy RODO, mają Państwo prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych. Informacje dotyczące składania skarg dostępne są na stronie internetowej Urzędu Ochrony Danych Osobowych: https://uodo.gov.pl.

24. Czy w związku z naruszeniem mogę dochodzić odszkodowania?

Zgodnie z art. 82 RODO osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia przepisów o ochronie danych osobowych, może dochodzić odszkodowania od podmiotu odpowiedzialnego za szkodę. Możliwość uzyskania odszkodowania zależy od okoliczności konkretnej sprawy, w tym wystąpienia naruszenia przepisów RODO, powstania szkody oraz istnienia związku przyczynowego pomiędzy naruszeniem a szkodą. Samo wystąpienie incydentu nie oznacza automatycznie powstania roszczenia odszkodowawczego. Podkreślamy, że cyberatak został skierowany przeciwko infrastrukturze zewnętrznego dostawcy oprogramowania MyDr, a nie bezpośrednio przeciwko systemom informatycznym Grupy Panda Med Holding.

VI. DODATKOWE INFORMACJE

25. Gdzie mogę znaleźć aktualne informacje dotyczące incydentu?

Informacje dotyczące naruszenia ochrony danych osobowych oraz zalecanych środków bezpieczeństwa udostępniamy za pośrednictwem oficjalnych kanałów komunikacji Grupy Panda Med Holding. Informacje dotyczące samego cyberataku oraz działań podjętych po stronie dostawcy oprogramowania dostępne są również w komunikacie MyDr „Informacja dla pacjentów", opublikowanym pod adresem:

https://pacjent.mydr.pl

W przypadku dodatkowych pytań zachęcamy do kontaktu z administratorem danych lub Inspektorem Ochrony Danych.

26. Czy nadal mogę umawiać wizyty i korzystać z usług placówek Grupy Panda Med Holding?

Tak. Zgodnie z informacjami przekazanymi przez dostawcę system MyDr EDM funkcjonuje prawidłowo, a incydent nie wpływa na możliwość bieżącego korzystania z systemu. W trosce o bezpieczeństwo danych osobowych pacjentów przy realizacji określonych czynności, w szczególności przy udostępnianiu dokumentacji medycznej lub przekazywaniu informacji o leczeniu, może być konieczne dodatkowe potwierdzenie tożsamości. Działania te służą ochronie Państwa prywatności oraz ograniczeniu ryzyka nieuprawnionego dostępu do informacji medycznych.