Rzecznik alarmuje: dane pacjentów muszą być lepiej chronione

Kategoria: Aktualności
Opublikowano: środa, 15, lipiec 2026 11:48
Tomasz Smaś
Odsłony: 172

Dane medyczne to wyjątkowo wrażliwe informacje, których odpowiednia ochrona powinna być priorytetem dla placówek przetwarzających te dane. Działania Rzecznika Praw Pacjenta oraz wydana decyzja w tej sprawie są jednoznaczne i wskazują na obowiązki placówek leczniczych.

Z uwagi na zakres przetwarzanych danych osobowych każdy podmiot leczniczy może stać się celem ataku cyberprzestępców. Sam fakt wystąpienia takiego ataku nie przesądza automatycznie o naruszeniu praw pacjenta. Podmioty lecznicze mają jednak obowiązek odpowiedniego zabezpieczenia danych medycznych pacjentów i stosowania odpowiednich, aktualnych i rekomendowanych mechanizmów zabezpieczających dostęp do elementów systemów teleinformatycznych. Działanie bez należytej staranności w tym zakresie może już naruszać zbiorowe prawa pacjentów. W badanej sprawie Rzecznik Praw Pacjenta ustalił istotne uchybienia w tym zakresie, tj.:

- zaniechanie wdrożenia centralnego zarządzania usługą poczty elektronicznej oraz pozostawienie użytkownikom uprawnień do tworzenia autonomicznych reguł przekierowań, przez co podmiot leczniczy ustanowił rażące odstępstwo od powszechnie uznanych standardów bezpieczeństwa teleinformatycznego;
- zezwolenie na niekontrolowany dostęp zdalny do sieci wewnętrznej ze sprzętu prywatnego;
- brak weryfikacji i egzekwowania stosowania zabezpieczeń kryptograficznych w korespondencji mailowej.

- *Podmioty lecznicze zobowiązane są do stosowania właściwych zasad ochrony dostępu do danych pacjentów i dokumentacji medycznej, w szczególności mechanizmów zabezpieczających dostęp do elementów systemów teleinformatycznych podmiotu leczniczego* – podkreśla Rzecznik Praw Pacjenta Bartłomiej Chmielowiec.

Rzecznik, po uprzednim przeprowadzeniu postępowania w sprawie stosowania praktyk naruszających zbiorowe prawa pacjenta, wydał decyzję uznającą stosowanie praktyk przez jeden z zakładów opieki zdrowotnej, w związku z uzyskaniem przez osoby nieuprawnione dostępu do danych pacjentów. Zakres wycieku danych był znaczący i dotyczył szerokiego zbioru danych o pacjentach podmiotu leczniczego takich jak: numer PESEL, imię i nazwisko, adres, data od, data do, czy zgon, rozpoznanie zasadnicze, rozpoznanie współistniejące, numer prawa wykonywania zawodu lekarza, kod komórki. Z ustaleń wynika, że do zdarzenia doszło na skutek założenia filtra, przekierowującego wiadomości ze skrzynek pocztowych zakładu opieki zdrowotnej na niepowołany adres e-mail.

Zgodnie z art. 24 ust. 1 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, w celu realizacji prawa, o którym mowa w art. 23 ust. 1, podmiot udzielający świadczeń zdrowotnych jest obowiązany prowadzić, przechowywać i udostępniać dokumentację medyczną w sposób określony w niniejszym rozdziale oraz w ustawie z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, a także zapewnić ochronę danych zawartych w tej dokumentacji.

Należy wskazać, że dokumentacja medyczna zawiera dane szczególnych kategorii w rozumieniu art. 9 ust. 1 RODO, w tym dane dotyczące zdrowia pacjentów. Z uwagi na szczególnie wrażliwy charakter tych informacji administrator danych zobowiązany jest do zapewnienia podwyższonego poziomu ochrony, obejmującego zarówno rozwiązania organizacyjne, jak i techniczne. Do danych osobowych dotyczących zdrowia należy zaliczyć wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą. Dane zawarte w dokumentacji medycznej przetwarzanej w systemach

teleinformatycznych podmiotu leczniczego należą do szczególnej kategorii danych chronionych. Wszelkie zestawienia, zawierające nawet samą informację o korzystaniu ze świadczeń zdrowotnych w podmiocie leczniczym, które są przechowywane w skrzynce odbiorczej podmiotu leczniczego, również stanowią szczególną kategorię tych danych.

Podmioty lecznicze powinny m.in.: każdoczasowo stosować szyfrowanie wiadomości mailowych zawierających poufne dane pacjentów, szyfrować pliki zawierające dane pacjentów, posiadać zabezpieczenia w dostępie do skrzynek mailowych, zablokować możliwość podłączania zewnętrznych nośników danych do sprzętu służbowego i prywatnego, ograniczyć możliwość logowania się do prywatnych skrzynek pocztowych ze sprzętu służbowego, stosować mechanizm weryfikacji tożsamości uprawnionych do dostępu do skrzynki mailowej, wykonywać pracę zdalną tylko na urządzeniach mobilnych przeznaczonych do użytku służbowego oraz nawiązywać połączenia z siecią firmową za pośrednictwem urządzeń zaakceptowanych przez administratora, stworzyć procedury i zabezpieczenia w przypadku wykonywania pracy zdalnej, prowadzić analizy ryzyka, wprowadzić i respektować zasady ochronne, co do sposobu tworzenia haseł, wprowadzić politykę zarządzania serwerem pocztowym oraz blokadę automatycznego przekierowywania wiadomości na zewnątrz domeny organizacji.

Rzecznik Praw Pacjenta Bartłomiej Chmielowiec wskazuje: - *Od podmiotów leczniczych wymagana jest podwyższona staranność, nie tylko w procesie bieżącej ochrony danych pacjentów, ale także w procesie przewidywania możliwych scenariuszy naruszenia dostępu do danych*.

Stwierdzone przez Rzecznika Praw Pacjenta nieprawidłowości i uznanie praktyki za naruszającą zbiorowe prawa pacjentów nie wynika z samego faktu, że zakład opieki zdrowotnej stał się celem zewnętrznego ataku informatycznego, lecz z uwagi na całość wadliwego procesu ochrony dostępu do systemów teleinformatycznych w zakładzie opieki zdrowotnej w zakresie braku stosowania mechanizmów zabezpieczających dostęp do elementów systemów teleinformatycznych szpitala przed osobami nieuprawnionymi, w tym dostęp do skrzynek poczty elektronicznej Szpitala.

Rzecznik nakazał wyeliminowanie ww. nieprawidłowości i obecnie oczekuje na stanowisko podmiotu leczniczego.

Źródło: RPP