SK&S Sołtysiński Kawecki Szlęzak

LEGAL ALERT
wrzesień 2026 r.

Cyberbezpieczeństwo dokumentacji medycznej - coraz większe wyzwanie dla sektora healthcare

SK&S

Incydent dotyczący systemu MyDr, a także niedawne cyberataki na podmioty działające w sektorze healthcare, w tym Exact Sciences, pokazują, że bezpieczeństwo informacji o zdrowiu pacjentów staje się jednym z kluczowych wyzwań dla podmiotów leczniczych i ich dostawców technologicznych.

W ostatnich miesiącach coraz częściej pojawiają się informacje o cyberincydentach dotyczących systemów wykorzystywanych w ochronie zdrowia. Ich przedmiotem są nie tylko dane osobowe pacjentów, ale również informacje dotyczące ich stanu zdrowia, historii leczenia, wyników badań czy korzystania ze świadczeń zdrowotnych. Przykładem jest incydent dotyczący MyDr – dostawcy systemu wykorzystywanego przez placówki medyczne do prowadzenia elektronicznej dokumentacji medycznej.

Podobny charakter miał niedawny incydent dotyczący Exact Sciences, amerykańskiej firmy zajmującej się diagnostyką onkologiczną. Abbott, który przejął Exact Sciences, potwierdził, że w wyniku cyberincydentu nieuprawniony dostęp uzyskano do części wewnętrznych systemów, a niektóre objęte incydentem pliki zawierały informacje dotyczące zdrowia.

Nie są to przy tym przypadki odosobnione. Tylko w ostatnim czasie podobne incydenty dotknęły również inne podmioty z sektora healthcare, w tym dostawców systemów wykorzystywanych do przechowywania danych pacjentów.

Dokumentacja medyczna – szczególny zasób wymagający ochrony

Skala i charakter tych incydentów zwracają uwagę na szczególny charakter dokumentacji medycznej. **Dokumentacja medyczna stanowi kluczowy element procesu udzielania świadczeń zdrowotnych**, a zapewnienie jej poufności i dostępności ma bezpośrednie znaczenie dla bezpieczeństwa pacjentów i ciągłości udzielania świadczeń.

Warto podkreślić, że podmiot udzielający świadczeń zdrowotnych ma ustawowy obowiązek prowadzić, przechowywać i udostępniać dokumentację medyczną oraz zapewnić ochronę danych w niej zawartych.

Cyberatak może tymczasem prowadzić nie tylko do nieuprawnionego ujawnienia informacji o pacjentach, lecz również do czasowej utraty dostępu do dokumentacji, jej uszkodzenia, a w konsekwencji zakłócenia funkcjonowania placówki medycznej.

SK&S

Ryzyko po stronie dostawców systemów

Szczególnego znaczenia nabiera to w sytuacji, gdy dokumentacja medyczna jest przechowywana lub przetwarzana z wykorzystaniem systemów dostarczanych przez podmioty zewnętrzne.

Incydent MyDr pokazuje, że bezpieczeństwo dokumentacji medycznej zależy w praktyce nie tylko od zabezpieczeń stosowanych przez sam podmiot leczniczy, ale również od bezpieczeństwa całego łańcucha technologicznego, z którego korzysta placówka.

Warto przy tym zwrócić uwagę, że na dostawców systemów informatycznych, którym podmiot leczniczy powierzył przetwarzanie danych osobowych pacjentów na podstawie umowy powierzenia przetwarzania danych, ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta nakłada wprost obowiązek zachowania w tajemnicy informacji związanych z pacjentem, uzyskanych w związku z realizacją tej umowy. Co istotne, realizacja umowy nie może przy tym powodować zakłócenia udzielania świadczeń zdrowotnych, w szczególności w zakresie zapewnienia, bez zbędnej zwłoki, dostępu do danych zawartych w dokumentacji medycznej.

Konsekwencje na gruncie RODO

Incydenty takie jak MyDr mają również istotne znaczenie z perspektywy ochrony danych osobowych. Nawet jeżeli naruszenie nastąpiło po stronie dostawcy systemu informatycznego działającego jako podmiot przetwarzający, podmioty lecznicze pozostają administratorami danych pacjentów i są odpowiedzialne za ocenę skutków incydentu na gruncie RODO. Oznacza to w szczególności konieczność samodzielnej oceny, czy naruszenie może powodować ryzyko dla praw i wolności osób, których dane dotyczą, a w konsekwencji czy zachodzi obowiązek zgłoszenia naruszenia organowi nadzorczemu oraz zawiadomienia pacjentów. Jednocześnie najnowsze stanowisko Prezesa UODO wskazuje, że administrator nie powinien pozostawać bierny w przypadku informacji o możliwym incydencie po stronie dostawcy i nie może poprzestać wyłącznie na jego komunikatach, lecz powinien aktywnie pozyskiwać informacje niezbędne do oceny skali i skutków zdarzenia. Warto przy tym pamiętać, że minimalizowanie ryzyka naruszeń powinno rozpoczynać się już na etapie wyboru dostawcy i obejmować odpowiednią weryfikację jego zdolności do zapewnienia bezpieczeństwa przetwarzanych danych. Szczególne znaczenie ma to w odniesieniu do danych dotyczących zdrowia, należących do szczególnych kategorii danych osobowych objętych podwyższonym poziomem ochrony.

SK&S

Warto zatem okresowo weryfikować nie tylko własne procedury bezpieczeństwa, lecz również:

- sposób zabezpieczenia dokumentacji przez dostawców systemów IT
- zasady wykonywania i przechowywania kopii zapasowych
- rozwiązania zapewniające dostęp do dokumentacji w przypadku niedostępności systemu
- postanowienia umowne dotyczące bezpieczeństwa informacji i odpowiedzialności dostawcy

Ostatnie incydenty pokazują, że cyberbezpieczeństwo dokumentacji medycznej nie jest wyłącznie zagadnieniem technicznym. Powinno być traktowane jako element systemu organizacji i bezpieczeństwa działalności podmiotu leczniczego oraz jako istotny element zarządzania ryzykiem związanym z korzystaniem z zewnętrznych dostawców technologii.

Zapraszamy do kontaktu!

JACEK MYSZKO

Partner, radca prawny
jacek.myszko@skslegal.pl

AGATA SZELIGA

Partner, radca prawny
agata.szeliga@skslegal.pl

AGNIESZKA JURCEWICZ-ANDROSZ

Starszy prawnik, adwokat
agnieszka.jurcewicz-androsz@skslegal.pl

EWELINA WOIKE-REGUŁA

Starszy prawnik, radca prawny
ewelina.woike-regula@skslegal.pl