

W kolskim szpitalu dane pacjentów powinny być już bezpieczne

BEZPIECZEŃSTWO INFORMACJI

Sławomir Wikariak
slawomir.wikariak@infor.pl

Szpital w Kole nie tylko nie zapewnił wystarczającej ochrony danych pacjentów, ale też nie reagował, choć już wiedział o możliwości wycieku – wynika z kontroli przeprowadzonej przez generalnego inspektora ochrony danych osobowych.

W czerwcu serwis Zaufana Trzecia Strona poinformował, że serwer Samodzielnego Publicznego Zakładu Opieki Medycznej w Kole jest całkowicie niezabezpieczony. Wystarczyło znać adres IP, by mieć niczym

nieskrępowany dostęp do przechowywanych na nim plików, w tym bazy danych osobowych 50 tys. pacjentów. Każdy mógł poznać ich imiona i nazwiska, adresy zamieszkania, numery PESEL i ubezpieczenia, a także grupę krwi. Ale to nie koniec. W jednym z plików zapisano dane dzieci wraz z informacjami na temat chorób zakaźnych, jakie przeszły. W innym katalogu były personalia 600 pracowników szpitala, a w kolejnym – numery ich rachunków bankowych.

Sprawą zainteresował się GODO. Jak wynika z przedstawionych przez niego wyników

kontroli, w szpitalu nie tylko zabrakło zabezpieczeń technicznych. Problemem był też brak komunikacji.

– Wobec tak poważnego wycieku natychmiastowa reakcja osób odpowiedzialnych za zarządzanie placówką jest niezbędna. Niestety, administrator bezpieczeństwa informacji oraz dyrektor szpitala zostali poinformowani o incydencie dopiero siedem dni po tym, jak wiadomość ta dotarła do pracownika szpitala. GODO zażądał w związku z tym wszczęcia postępowania dyscyplinarnego wobec osoby winnej opóźnienia, które uniemożliwiło szyb-

ką reakcję na wyciek – informuje Agnieszka Świątek-Druś, rzecznik prasowy GODO.

Serwis Zaufana Trzecia Strona natychmiast poinformował przedstawiciela szpitala o możliwym wycieku danych. Co prawda zostały one zabezpieczone, ale jeszcze przez kilka dni możliwy był dostęp do podglądu folderów.

Już podczas kontroli szpital podjął kroki, które mają go zabezpieczyć przed podobną sytuacją w przyszłości. Przeprowadził audyt systemów informatycznych, poprawił zabezpieczenia serwera, zwolnił pracowników odpowiedzialnych za błędy i zatrudnił no-

wych, zlecił wyspecjalizowanej firmie nadzór nad prawidłowym funkcjonowaniem sieci informatycznej oraz opracował procedurę reagowania na naruszenia danych osobowych. To ważne także w kontekście wchodzących od 25 maja 2018 r. nowych obowiązków. Zgodnie z unijnym rozporządzeniem administrator będzie musiał informować wszystkie osoby, których dane dotyczą, o naruszeniu zasad ich ochrony. ©P

PISALIŚMY O TYM

Informacje o chorych na otwartym serwerze – DGP nr 113/2017
www.praca.gazetaprawna.pl