Medexpress, 2019-11-14 07:45

NIK o danych osobowych pacjentów w szpitalach

Fot.NIK

W ocenie NIK niewłaściwe zabezpieczenie i przechowywanie dokumentacji medycznej przez personel medyczny wynika z rutyny.

- W ponad połowie skontrolowanych szpitali doszło do naruszeń ochrony danych osobowych, z czego w sześciu sytuacja była na tyle poważna, że konieczne było powiadomienie Prezesa Urzędu Ochrony Danych Osobowych.
- W Szpitalu Specjalistycznym im. Ludwika Rydygiera w Krakowie Sp. z o.o. jeden z pacjentów niechcący zabrał dokumentację medyczną innego pacjenta jednej z poradni.
- W Wojewódzkim Specjalistycznym Szpitalu Dziecięcym im. Św. Ludwika w Krakowie mężczyzna z zaburzeniami psychicznymi ukradł z pomieszczenia rejestracji trzy kartoteki pacjentów - dwóch z nich nie odnaleziono.
- W 9 z 24 skontrolowanych szpitali papierowa dokumentacja pacjentów na oddziałach szpitalnych przechowywana była w niezamykanych szafkach lub na półkach.
- W dwóch skontrolowanych szpitalach kopie dokumentacji zostały udostępnione osobom, których pacjent nie upoważnił.
- W siedmiu skontrolowanych szpitalach do przetwarzania danych osobowych, w tym medycznych, upoważnieni byli pracownicy obsługi, np. salowe i sanitariusze.

Prywatność pacjenta

Ważna jest również kwestia prawa pacjenta do zachowania prywatności w newralgicznych momentach pobytu w szpitalu, np. podczas rejestracji do poradni, oczekiwania na wizytę i wezwania do gabinetu, w trakcie pobytu na oddziale szpitalnym.

W 9 z 24 skontrolowanych szpitali pacjentom nie zagwarantowano prawa do prywatności w trakcie rejestracji.

Odległość pomiędzy okienkami rejestracji była zbyt mała lub nie wyznaczono strefy oddzielającej pacjentów obsługiwanych od oczekujących w kolejce. W tych sytuacjach osoby postronne mogły usłyszeć treści rozmów pomiędzy pacjentem a personelem szpitala, dotyczących np. stanu zdrowia pacjenta, w tym szczegóły związane z dolegliwościami i procesem leczenia.
Dużo bardziej dyskretnie wzywano pacjentów do gabinetów lekarskich. Najczęściej posługiwano się komunikatem: „proszę kolejną osobę” lub podawano imię pacjenta i godzinę wizyty, ewentualnie numer, który pacjent otrzymał podczas rejestracji.

We wszystkich objętych kontrolą szpitalach pacjentom umieszczano na nadgarstkach opaski ze znakami identyfikacyjnymi.

Innym niepokojącym zjawiskiem było przekazywanie danych osobowych pacjentów firmom informatycznym serwisującym szpitalne systemy podczas zgłaszania usterek oprogramowania.

W ¾ szpitali nie wdrożono odpowiednich środków zabezpieczających dane osobowe i medyczne

pacjentów przechowywane w postaci elektronicznej.

Stosowanie odpowiedniej ochrony antywirusowej posiadanych komputerów powinno być podstawowym elementem właściwej ich ochrony. W trzech szpitalach część komputerów nie miała zainstalowanego takiego programu, a w czterech programy antywirusowe nie miały aktualnej bazy sygnatur wirusów, przez co ich skuteczność była ograniczona.

W połowie skontrolowanych szpitali kontrolerzy NIK stwierdzili zaniechania, które w sposób szczególny wpływały na obniżenie bezpieczeństwa danych przechowywanych w formie elektronicznej.

Zawiódł też system szkoleń. Tylko w 9 szpitalach szkoleniami z zakresu ochrony danych osobowych objęto prawie cały personel (co najmniej 95%).

Wnioski NIK

do Prezesa Urzędu Ochrony Danych Osobowych o:

- przeprowadzanie systemowych kontroli przestrzegania zasad ochrony danych osobowych w jednostkach z sektora ochrony zdrowia oraz
- niezwłoczne zakończenie działań związanych z przyjęciem Kodeksu postępowania dla sektora ochrony zdrowia i wprowadzenie regulacji dotyczących certyfikacji, o której mowa w art. 42 RODO.

do organów założycielskich szpitali o:

- nadzorowanie zagadnień związanych z ochroną danych osobowych pacjentów w podległych podmiotach leczniczych.

do kierowników podmiotów leczniczych o:

- analizowanie ryzyka dotyczącego ochrony danych osobowych, zgodnie z aktualną wiedzą techniczną, a następnie stosowanie rozwiązań adekwatnych do ustalonych zagrożeń,
- regularne szkolenie osób uczestniczących w procesach przetwarzania informacji, ze szczególnym uwzględnieniem zagrożeń bezpieczeństwa informacji, skutków naruszenia zasad bezpieczeństwa informacji, odpowiedzialności prawnej oraz stosowania środków zapewniających bezpieczeństwo informacji,
- nadawanie pracownikom uprawnień w systemach operacyjnych komputerów oraz systemach HIS w stopniu adekwatnym do realizowanych przez nich zadań,
- wprowadzenie zindywidualizowanej autoryzacji dostępu do posiadanych zasobów informatycznych,
- przechowywanie kopii bezpieczeństwa posiadanych zasobów informacyjnych w innym miejscu niż dane produkcyjne,
- zapewnienie zabezpieczeń fizycznych infrastruktury informatycznej, uniemożliwiających dostęp osób nieuprawnionych oraz zapewniających ochronę przed skutkami zdarzeń losowych (np. pożar, powódź, wichura),
- zapewnienie, aby osoby, które uzyskują dostęp do danych osobowych, posiadały stosowne upoważnienia administratora danych osobowych w tym zakresie,
- przekazywanie firmom świadczącym usługi serwisowe jedynie danych niezbędnych do usunięcia usterek oprogramowania.

Źródło: NIK