Źródło: ©Blue Planet Studio – stock.adobe.com

Wdrożenie przez podmioty lecznicze regulacji dotyczących ochrony danych osobowych

Od 25 maja 2018 r. do 23 kwietnia 2019 r.

Najwyższa Izba Kontroli

Warszawa, listopad 2019 r.

01 Dlaczego podjęliśmy kontrolę?

- Rozporządzenie Ogólne o Ochronie Danych Osobowych (RODO) zmieniło zasady przetwarzania, wykorzystywania i przechowywania danych osobowych, zwiększając ich ochronę oraz nakładając nowe obowiązki na administratorów tych danych.
- Jednostki prowadzące działalność leczniczą w związku z wejściem w życie nowych przepisów obowiązane zostały do dokonania przeglądu stosowanych rozwiązań oraz sprawdzenia, czy spełniają one swoją rolę.

02 Dlaczego podjęliśmy kontrolę?

Specyfika danych osobowych i sposobu ich przetwarzania przez podmioty lecznicze

- Dane medyczne stanowią szczególną kategorię danych osobowych.
- Ujawnienie danych medycznych może mieć negatywne konsekwencje dla pacjentów.
- Coraz częstsze wykorzystanie systemów informatycznych do gromadzenia, przechowywania i przetwarzania danych osobowych.
- Doniesienia medialne o częstych działaniach cyberprzestępców zmierzających do nieuprawnionego wejścia w posiadanie danych medycznych.
- Wysokie administracyjne kary pieniężne za naruszenie przepisów przy przetwarzaniu danych osobowych.

03 Co kontrolowaliśmy?

Czy dane osobowe w podmiotach leczniczych są prawidłowo chronione i przetwarzane?

- Czy prawidłowo opracowano wymaganą dokumentację i procedury związane z ochroną przetwarzanych danych osobowych?
- Czy wdrożone rozwiązania zapewniają prawidłowe przetwarzanie i ochronę danych osobowych?

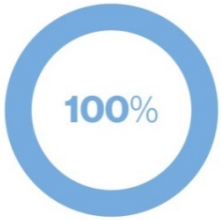
04 Kogo kontrolowaliśmy?

Kontrolę NIK przeprowadzono w 24 szpitalach z sześciu województw:

Źródło: Opracowanie własne NIK na podstawie wyników kontroli.

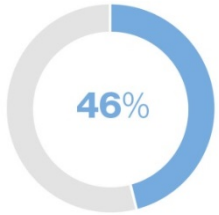
W każdym z województw skontrolowano dwa szpitale, dla których organem tworzącym jest marszałek województwa oraz dwa powiatowe lub miejskie.

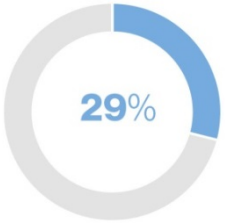
05 Stwierdzony stan – wymagania formalne związane z RODO



Powołano Inspektorów Ochrony Danych oraz zapewniono im wykonywanie obowiązków w sposób niezależny.

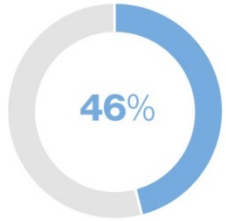
W prawie połowie szpitali wewnętrzna dokumentacja opisująca bezpieczeństwo przetwarzanych danych nie została terminowo zaktualizowana w związku z wejściem w życie RODO.

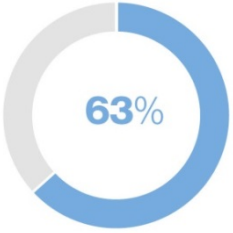




W siedmiu szpitalach nie założono w terminie rejestru czynności przetwarzania, wymaganego przepisami RODO.

W prawie połowie szpitali z opóźnieniem wykonano analizę ryzyk związanych z przetwarzaniem danych, która powinna być punktem wyjścia do przyjęcia właściwych środków do ochrony danych.

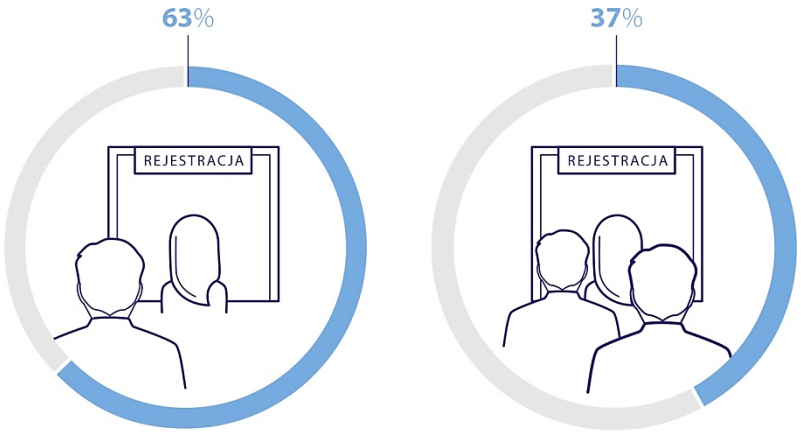




W blisko 2/3 skontrolowanych szpitali z zagadnień bezpieczeństwa danych osobowych przeszkolono mniej niż 95% załogi.

Stwierdzony stan – zapewnienie anonimowości pacjenta w procesie rejestracji w poradni i na oddziale

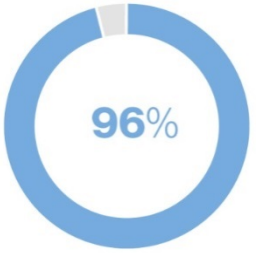
Udział szpitali zapewniających zachowanie prywatności podczas rejestracji



W ponad 1/3 skontrolowanych szpitali nie wprowadzono rozwiązań gwarantujących pacjentom zachowanie prywatności w procesie rejestracji.

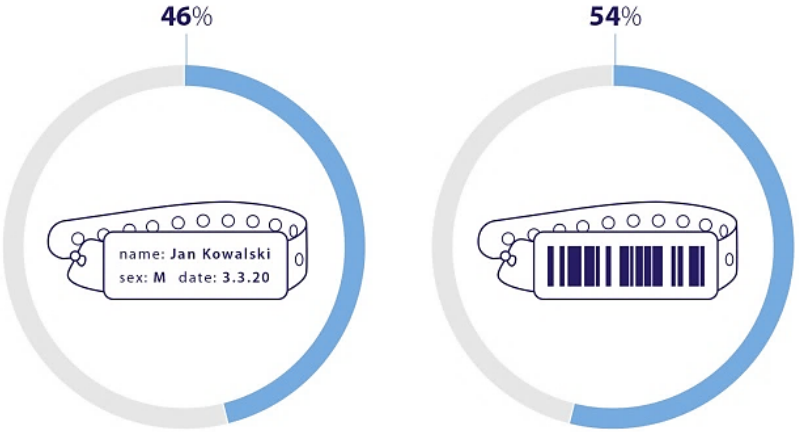
Źródło: Opracowanie własne NIK na podstawie wyników kontroli.

W 23 szpitalach pacjentom zapewniono anonimowość podczas wzywania do gabinetów poradni specjalistycznych.



Stwierdzony stan – zapewnienie anonimowości pacjenta w procesie rejestracji w poradni i na oddziale

Udział szpitali pod względem sposobów umieszczania danych na opaskach identyfikacyjnych pacjentów



W 46 % skontrolowanych szpitali na opaskach indentyfikacyjnych pacjentów umieszczano dane osobowe.

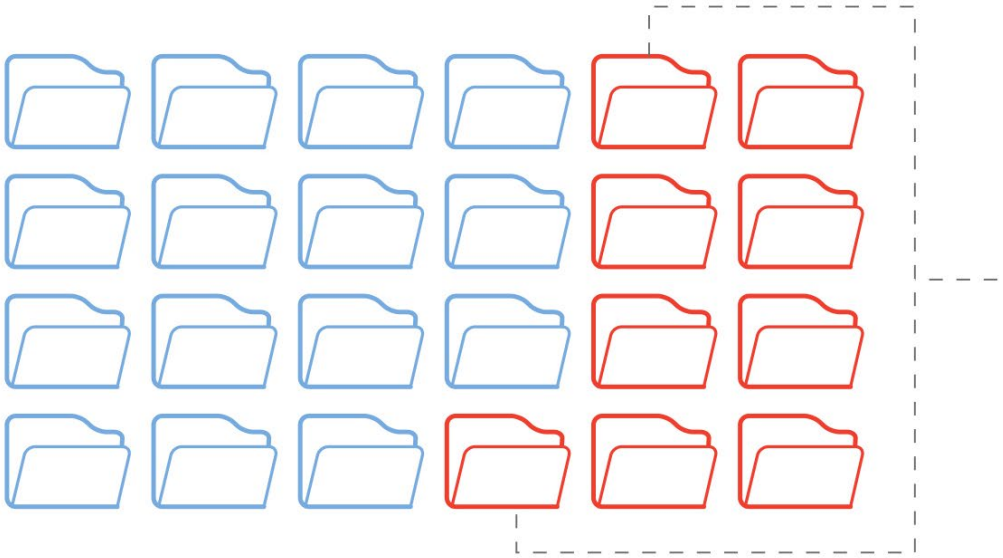
Udział szpitali pod względem kart gorączkowych przy łóżkach pacjentów

W większości szpitali (87%) na łóżkach pacjentów nie zamieszczano kart gorączkowych z widocznymi danymi pacjenta.

Źródło: Opracowanie własne NIK na podstawie wyników kontroli.

08 Stwierdzony stan – papierowa dokumentacja medyczna

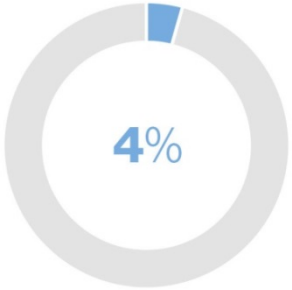
Sposób przechowywania papierowej dokumentacji medycznej
w dyżurkach pielęgniarskich oraz dyżurkach lekarskich



w **9/24 szpitalach**
dokumentacja medyczna
przechowywana była
w **niezamykanych szafkach**

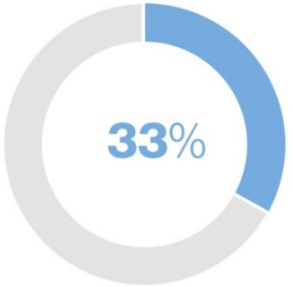
Źródło: Opracowanie własne NIK na podstawie wyników kontroli.

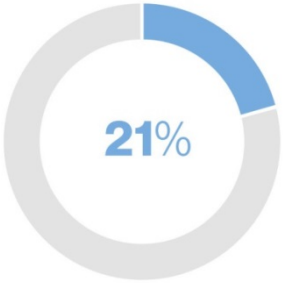
Stwierdzony stan – udzielanie uprawnień i wydawanie upoważnień personelowi



W jednym ze szpitali stwierdzono błędy w dostępie pracowników działów administracyjnych do danych osobowych i medycznych pacjentów.

W ośmiu szpitalach pielęgniarkom przyznano w systemie HIS uprawnienia dostępu do danych pacjentów z oddziałów lub poradni szpitala, na których nie świadczyły pracy.

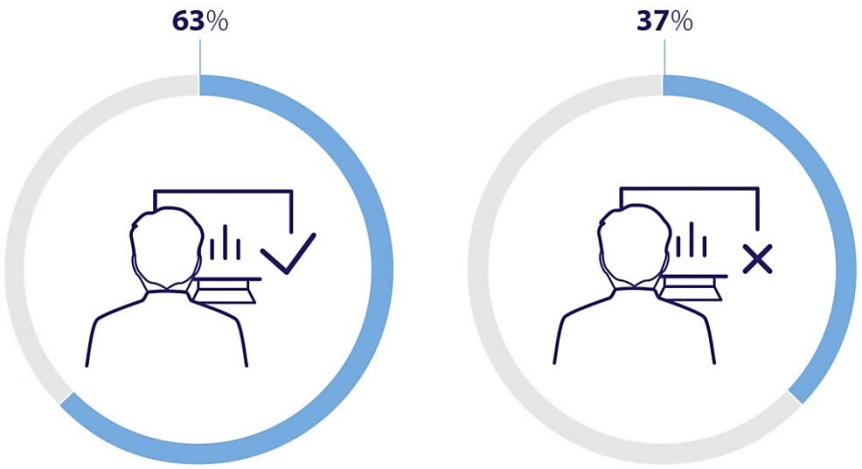




W pięciu szpitalach stwierdzono błędy formalne podczas udzielania uprawnień w systemach informatycznych oraz wydawania upoważnień.

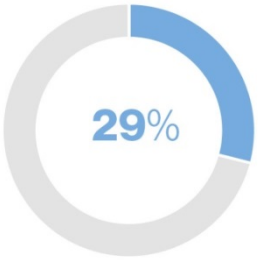
Stwierdzony stan – udzielanie uprawnień i wydawanie upoważnień personelowi

Udział szpitali terminowo odbierających uprawnienia w systemach informatycznych pracownikom kończącym zatrudnienie



Byłym pracownikom 15 szpitali nie odbierano niezwłocznie dostępu do systemów informatycznych wraz z końcem ich pracy.

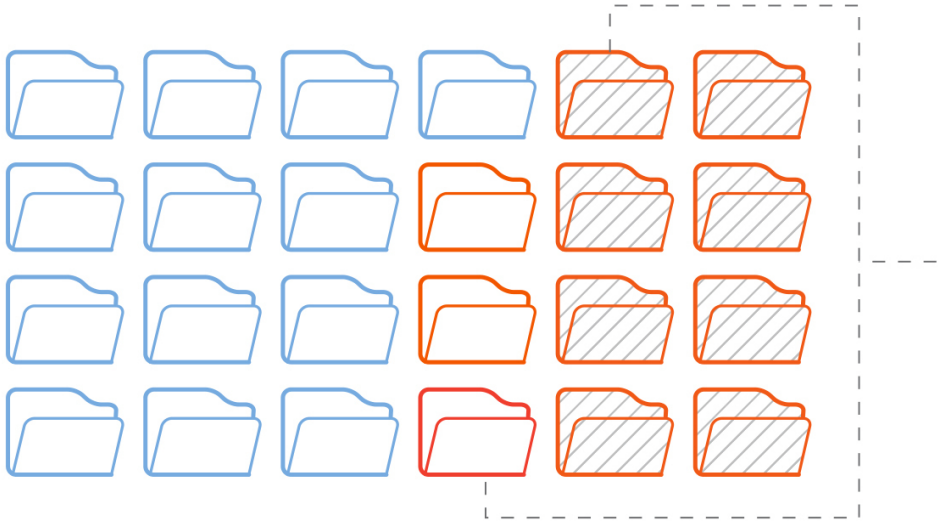
Źródło: Opracowanie własne NIK na podstawie wyników kontroli.



W siedmiu szpitalach salowym i sanitariuszom wydawano upoważnienia do przetwarzania danych osobowych, chociaż nie należą oni do personelu medycznego i dostęp do tego rodzaju danych nie jest niezbędny do wykonywania przez nich zadań służbowych.

Stwierdzony stan – przekazywanie danych pacjentów na zewnątrz szpitala

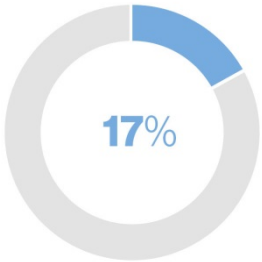
Proceder przesyłania danych osobowych i medycznych pacjentów w zgłoszeniach serwisowych dokonanych w okresie objętym kontrolą



w **11/24 szpitalach** w zgłoszeniach do serwisanta problemów technicznych z medycznymi systemami informatycznymi **przekazano na zewnątrz szpitala dane osobowe pacjenta**

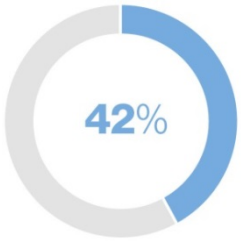
w tym w **8/24 szpitalach** wśród przekazanych danych znalazły się **informacje medyczne o pacjentach**

Źródło: Opracowanie własne NIK na podstawie wyników kontroli.



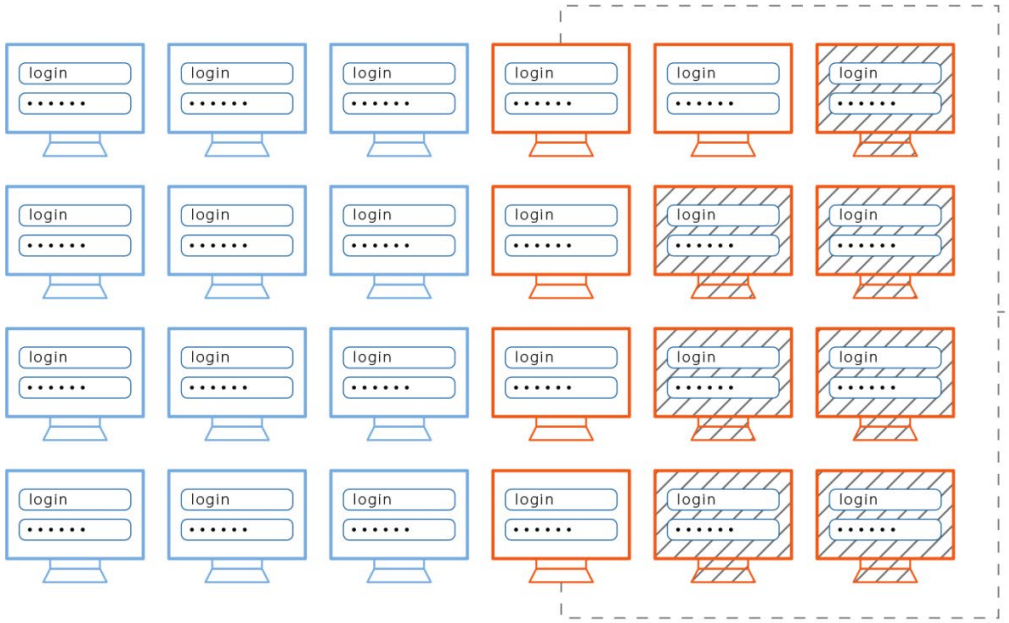
W czterech szpitalach stwierdzono przypadki niewłaściwego udostępniania dokumentacji medycznej; w dwóch z nich udostępniono ją osobom innym niż pacjent, chociaż nie posiadały one stosownego upoważnienia.

Stwierdzony stan – bezpieczeństwo danych w postaci elektronicznej



W 10 z 24 szpitali część pracowników posiadała uprawnienia administratora systemu operacyjnego, chociaż nie wykonywali zadań związanych z administrowaniem systemami.

Posługiwanie się tym samym loginem i hasłem do systemu operacyjnego

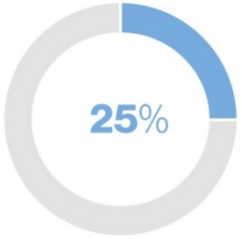


w **12/24 szpitalach**
tym samym loginem i hasłem do systemu Windows posługiwało się kilkudziesięciu pracowników

w tym w **7/24 szpitalach**
pracownicy logujący się mogli dokonywać dowolnych i nieograniczonych działań na komputerach

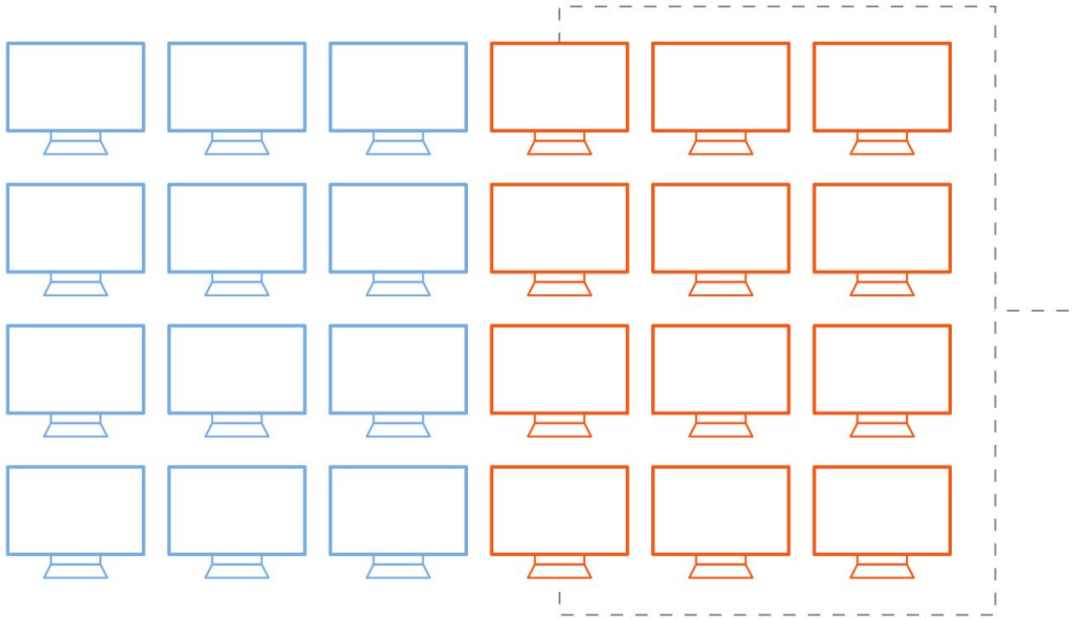
Źródło: Opracowanie własne NIK na podstawie wyników kontroli.

Stwierdzony stan – bezpieczeństwo danych w postaci elektronicznej



W sześciu szpitalach część komputerów nie posiadała zainstalowanego programu antywirusowego lub baza sygnatur wirusów w takim programie była nieaktualna.

Użytkowanie systemów operacyjnych bez wsparcia producenta

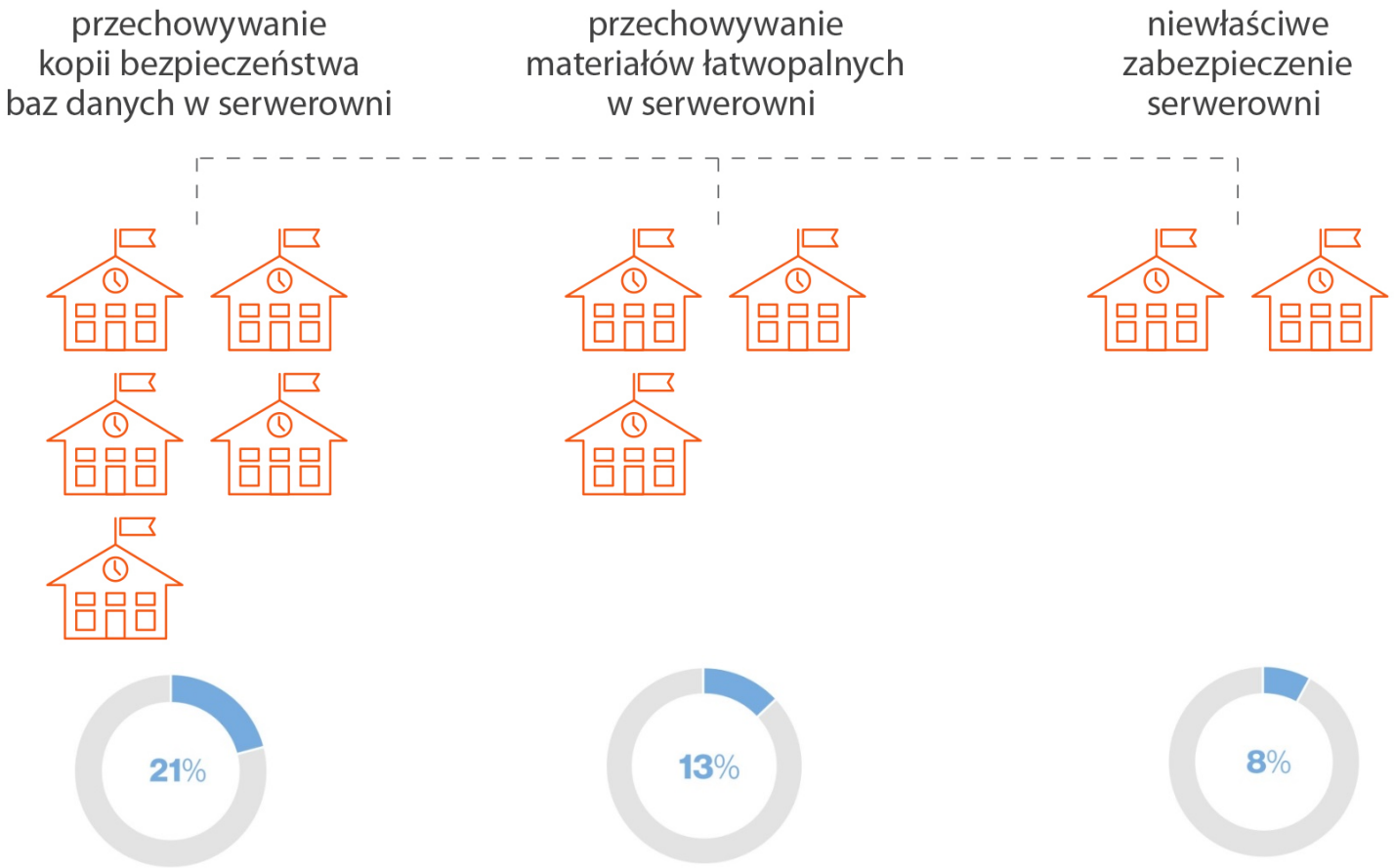


w **12/24 szpitalach** posługiwano się przestarzałymi systemami operacyjnymi Windows XP i Windows Vista

Źródło: Opracowanie własne NIK na podstawie wyników kontroli.

Stwierdzony stan – bezpieczeństwo serwerowni i kopii zapasowych baz danych

Przechowywanie kopii bezpieczeństwa baz danych



Źródło: Opracowanie własne NIK na podstawie wyników kontroli.

Ocena ogólna (1)

Niemal w żadnym ze skontrolowanych podmiotów leczniczych dane osobowe pacjentów nie były prawidłowo chronione i przetwarzane po wejściu w życie przepisów RODO. W konsekwencji kierownicy tych podmiotów i Inspektorzy Ochrony Danych nie zapewnili pacjentom pełnego zabezpieczenia ich danych. Personel medyczny i administracyjny postępował rutynowo, według schematów wypracowanych przed wejściem w życie nowych uregulowań.

Ocena ogólna (2)

Szesnaście z 24 skontrolowanych podmiotów leczniczych (67%) nie było właściwie przygotowanych do wejścia w życie RODO.
Dokumenty i procedury związane z wejściem w życie RODO zostały w nich bowiem wdrożone z opóźnieniem lub do zakończenia kontroli NIK ich nie wprowadzono:

- w dziewięciu szpitalach analiza ryzyka procesów przetwarzania danych osobowych, która powinna poprzedzić przyjęcie właściwych środków do ochrony danych osobowych, została przeprowadzona po upływie od 35 do 201 dni od dnia wejścia w życie RODO, a w dwóch kolejnych wykonano ją dopiero w trakcie kontroli NIK;
- w siedmiu podmiotach leczniczych wewnętrzną dokumentację, opisującą stosowane środki techniczne i organizacyjne związane z zapewnieniem bezpieczeństwa danych osobowych zaktualizowano po upływie od 37 do 263 dni od wejścia w życie RODO, a w czterech jej nie uaktualniono;
- w siedmiu szpitalach rejestr czynności przetwarzania założono od 12 do 263 dni od wejścia w życie RODO, a w jednym go nie opracowano.

Ocena ogólna (3)

Jedną z głównych przyczyn wymienionych nieprawidłowości była nieznajomość zagadnień bezpieczeństwa danych osobowych.
Tylko w dziewięciu szpitalach szkoleniami w tym zakresie objęto prawie cały personel (co najmniej 95%).
W rezultacie w podmiotach tych stwierdzono najmniej istotnych nieprawidłowości dotyczących ochrony danych osobowych pacjentów.
Jedynie w trzech szpitalach (12,5%) przyjęte rozwiązania organizacyjne i techniczne stworzyły odpowiednie warunki do rejestracji na wizyty do lekarza, identyfikacji pacjenta na oddziale i przechowywania jego dokumentacji medycznej. W pozostałych nie zapewniono skutecznej ochrony danych osobowych i medycznych pacjentów przed ujawnieniem osobom postronnym.

Ocena ogólna (4)

Nie przestrzegano też ustalonej w RODO zasady ograniczania dostępu do danych osobowych do zakresu niezbędnego do osiągnięcia celu ich przetwarzania. W rezultacie średnio co 11 pielęgniarka posiadała przyznane w systemie informatycznym uprawnienia do danych medycznych pacjentów leczonych na innych oddziałach szpitala, a byłym pracownikom personelu medycznego 15 podmiotów leczniczych (62,5%) nie odebrano niezwłocznie dostępu do systemów informatycznych. Z kolei 11 szpitali (45,8%) w nieuprawniony sposób przekazało dane osobowe pacjentów podmiotom serwisującym systemy informatyczne. Prawidłowo natomiast przyznawano dostęp do systemu HIS pracownikom działów administracyjnych. Był on odpowiedni i niezbędny do wykonywania obowiązków służbowych.
W 18 szpitalach (75%) nie przestrzegano wymogów dotyczących nadawania właściwych uprawnień do administrowania systemami informatycznymi, ochrony przed złośliwym oprogramowaniem oraz odpowiedniej autoryzacji. W pięciu (20,8%) zaś kopie bezpieczeństwa danych przechowywano w niewłaściwym miejscu. Nie gwarantowało to zabezpieczenia zasobów elektronicznych przed nieuprawnionym dostępem, przejęciem i zniszczeniem.

Wnioski – do Prezesa Urzędu Ochrony Danych Osobowych

- Przeprowadzanie systemowych kontroli przestrzegania zasad ochrony danych osobowych w jednostkach z sektora ochrony zdrowia, z uwagi na przetwarzanie przez te podmioty szczególnych kategorii danych osobowych.
- Niezwłoczne zakończenie działań związanych z przyjęciem *Kodeksu postępowania dla sektora ochrony zdrowia* oraz wprowadzenie regulacji dotyczących certyfikacji, o której mowa w art. 42 RODO.

Wnioski – do organów założycielskich szpitali

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

Wnioski – do kierowników podmiotów leczniczych

- Analizowanie ryzyka dotyczącego ochrony danych osobowych, uwzględniającego aktualny stan wiedzy technicznej, a następnie stosowanie rozwiązań adekwatnych do ustalonych zagrożeń.
- Przeprowadzanie regularnych szkoleń 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.

Wnioski – do kierowników podmiotów leczniczych

- 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 upoważniania ADO w tym zakresie.
- Przekazywanie firmom świadczącym usługi serwisowe jedynie danych osobowych niezbędnych do usunięcia usterek oprogramowania.

Źródło: ©Blue Planet Studio – stock.adobe.com

Najwyższa Izba Kontroli

Delegatura w Białymstoku