NAJWYŻSZA IZBA KONTROLI
Delegatura w Krakowie

LKR.410.002.02.2019

Pan Stanisław Stępniewski
Dyrektor Wojewódzkiego Specjalistycznego
Szpitala Dziecięcego im. Św. Ludwika
w Krakowie,
ul.Strzelecka 2, 31-503 Kraków

WYSTĄPIENIE POKONTROLNE

P/19/063 „Wdrożenie przez podmioty lecznicze regulacji dotyczących ochrony danych osobowych”

NAJWYŻSZA IZBA KONTROLI
Delegatura w Krakowie
ul. Łobzowska 67, 30-038 Kraków
T +48 12 342 34 00, F +48 12 342 34 44
lkr@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana

Wojewódzki Specjalistyczny Szpital Dziecięcy im. Św. Ludwika w Krakowie, ul. Strzelecka 2, 31-503 Kraków (dalej: *Szpital*).

Kierownik jednostki kontrolowanej

Stanisław Stępniewski, dyrektor, od 1 czerwca 2005 r.

Zakres przedmiotowy kontroli

1. Opracowanie wymaganej dokumentacji oraz procedur związanych z ochroną przetwarzanych danych osobowych.
2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych.

Okres objęty kontrolą

Od 25 maja 2018 r. do dnia zakończenia czynności kontrolnych, tj. 9 kwietnia 2019 r. Badania kontrolne mogły dotyczyć działań sprzed tego okresu, jeśli miały związek z zagadnieniami będącymi przedmiotem kontroli.

Podstawa prawna podjęcia kontroli

Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[1]

Jednostka przeprowadzająca kontrolę

Najwyższa Izba Kontroli
Delegatura w Krakowie

Kontrolerzy

1. Zbigniew Polak, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LKR/12/2019 z 8 stycznia 2019 r. i nr LKR/66/2019 z 5 kwietnia 2019 r.
2. Małgorzata Korusiewicz, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LKR/13/2019 z 8 stycznia 2019 r.

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

W okresie objętym kontrolą w Szpitalu opracowano wymaganą dokumentację oraz procedury związane z ochroną przetwarzanych danych osobowych. Przyjęte rozwiązania techniczne i organizacyjne nie zapewniały jednak pełnej ochrony danych osobowych i nie eliminowały ryzyka nieuzasadnionego dostępu do danych przetwarzanych w systemach informatycznych Szpitala.

W Szpitalu w sposób prawidłowy sporządzono dokumentację związaną z ochroną danych osobowych, uwzględniającą przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (tzw. ogólne rozporządzenie o ochronie danych), w tym opracowano procedury wewnętrzne oraz dokonywano wymaganych przeglądów i aktualizacji opracowanej dokumentacji. Wprowadzono kompleksowy system zarządzania bezpieczeństwem informacji, zgodnie z § 20 ust. 1 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[3].

[1] Dz. U. z 2019 r. poz. 489, dalej: ustawa o NIK

[2] Najwyższa Izba Kontroli formułuje ocenę ogólną, jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej. W przypadku niniejszego wystąpienia zastosowano ocenę opisową.

[3] Dz. U. z 2017 r. poz. 2247. (zwane dalej: rozporządzeniem KRI).

W Szpitalu wyznaczono Inspektora Ochrony Danych (IOD) i poprzez przyjęte rozwiązania organizacyjne zagwarantowano mu status niezależności w sprawowaniu tej funkcji. Szpital właściwie zrealizował swoje obowiązki związane z przeprowadzeniem analizy procesów przetwarzania danych, dokonaniem oceny skutków przetwarzania danych osobowych i prowadzeniem rejestru czynności przetwarzania. Wprowadzone rozwiązania organizacyjne, zmierzające do zapewnienia ochrony danych osobowych pacjentów, gwarantowały poszanowanie ich prywatności. Personelowi szpitala zapewniono odpowiedni dostęp do danych medycznych.

W trakcie kontroli stwierdzono następujące nieprawidłowości:

1) nieprzeszkolono wszystkich pracowników Szpitala uczestniczących w przetwarzaniu danych osobowych. W szkoleniach związanych z wejściem w życie RODO oraz zagadnieniami dotyczącymi bezpieczeństwa danych wzięło udział 67,5% ww. pracowników;
2) czterem byłym pracownikom (na 21) nieodebrano bezzwłocznie możliwości dostępu do systemów informatycznych;
3) w dwóch przypadkach (na 60) Szpital przekazał firmie serwisowej w celu naprawy błędu systemowego dane medyczne i identyfikacyjne pacjentów.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[4] kontrolowanej działalności

OBSZAR

1. Opracowanie dokumentacji oraz procedur związanych z ochroną przetwarzanych danych osobowych

Opis stanu faktycznego

1.1. W Regulaminie Organizacyjnym Szpitala z 28 czerwca 2018 r.[5] wskazano stanowisko Inspektora Ochrony Danych (dalej: *IOD*), jako samodzielne stanowisko pracy. Wprowadzenie powyższego Regulaminu Organizacyjnego było związane ze zmianą nazwy stanowiska pracy z Administratora Bezpieczeństwa Informacji na Inspektora Ochrony Danych. Zmiana ta została pozytywnie zaopiniowana w dniu 26 czerwca 2018 r. przez Radę Społeczną Szpitala (Uchwała nr 8/2018).

Do zadań IOD należało m.in. informowanie o obowiązkach spoczywających na mocy ogólnego rozporządzenia o ochronie danych osobowych oraz innych przepisów Unii o ochronie danych i doradzanie w tej sprawie, monitorowanie przestrzegania obowiązujących w tym zakresie przepisów, podejmowanie działań zwiększających świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania danych, udzielanie zaleceń co do oceny skutków dla ochrony danych, współpraca z organem nadzorczym, pełnienie funkcji punktu kontaktowego oraz prowadzenie rejestru czynności. W Regulaminie dla IOD wskazano wszystkie zadania przewidziane w art. 39 RODO. Zadania te zostały również zawarte w obecnie obowiązującym Regulaminie z 19 grudnia 2018 r.[6]

IOD podlegał Dyrektorowi Szpitala. W myśl art. 8, art. 10 i art. 158 ust. 2 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[7], Szpital terminowo wywiązał się z obowiązku zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu na stanowisko IOD (28 sierpnia 2018 r. formularzem

[4] Oceny cząstkowe to oceny działalności w poszczególnych obszarach badań kontrolnych. Ocena cząstkowa może być sformułowana, jako ocena pozytywna, ocena negatywna albo ocena w formie opisowej. W przypadku niniejszego wystąpienia zastosowano ocenę opisową.

[5] Zarządzenie Dyrektora Szpitala nr 32/18.

[6] Zarządzenie Dyrektora Szpitala nr 60/18.

[7] Dz. U. poz. 1000, ze zm.

elektronicznym). Osoba ta do 24 maja 2018 r. była Administratorem Bezpieczeństwa Informacji. Przekazane zawiadomienie zawierało wszystkie elementy określone art. 10 ust. 3 ustawy o ochronie danych osobowych. Dane IOD oraz sposób i formę kontaktu udostępniono na stronie internetowej Szpitala – wymóg art. 37 ust. 7 RODO. IOD był zatrudniona w Szpitalu na 0,5 etatu. IOD zatrudniony był także na drugie 0,5 etatu, jako Specjalista ds. Administracyjnych. Szpital umożliwił, zatem IOD wykonywanie obowiązków w sposób niezależny, stosownie do art. 38 ust. 3 RODO. Spełniono, zatem wymóg wskazany w art. 38 ust. 6 RODO wskazujący, że IOD może wykonywać inne obowiązki, ale administrator lub podmiot przetwarzający zapewniają, aby takie zadania nie powodowały konfliktu interesów.

(akta kontroli str. 166, 207-212, 218-233)

Zgodnie z wymogami art. 37 ust. 5 RODO, IOD miał należyte przygotowanie i kwalifikacje zawodowe do pełnienia swojej funkcji. Wcześniej był Administratorem Bezpieczeństwa Informacji w kontrolowanym Szpitalu.
W 2017 r. ukończył kurs w zakresie obowiązków administratora bezpieczeństwa informacji i inspektora ochrony danych. W maju 2018 r. ukończyła kurs w zakresie obowiązków IOD w świetle RODO.

(akta kontroli str. 4)

Szpital nie został uznany za operatora usługi kluczowej, o którym mowa w art. 5 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[8], IOD nie był członkiem wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo, określonych w art. 14 tej ustawy.

(akta kontroli str. 14)

1.2. W Szpitalu obowiązywały następujące uregulowania wewnętrzne dotyczące ochrony danych osobowych, wynikające z przepisów RODO:

- Polityka Ochrony Danych Osobowych (dalej: PODO) z 18 maja 2018 r. m.in. z załącznikiem pn. Wykaz Zbiorów Danych Osobowych, tj. opis sposobu przepływu danych pomiędzy systemami oraz opis środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych. Załącznikami do PODO była informacja dla kontrahenta, wzór umowy powierzenia przetwarzania danych osobowych, wykaz zagrożeń, regulamin ochrony danych osobowych, wzór oświadczenia o poufności, rejestr czynności przetwarzania, procedura audytu, plan ciągłości działania. Postanowienia polityki obejmowały zarówno ochronę danych osobowych pracowników Szpitala, jak i danych pacjentów oraz określały sposoby zapewnienia bezpieczeństwa danych osobowych przetwarzanych w formie papierowej oraz w systemach elektronicznych. Akty prawne przywołane w opracowanej dokumentacji były aktualne.
- Instrukcja Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych opracowana na potrzeby RODO (dalej: IZSI) z 18 maja 2018 r. załącznikami: wzór ewidencji pobrań kluczy, dostępu do pomieszczeń podlegających szczególnej ochronie, regulamin użytkowania komputerów przenośnych, regulamin dostępu zdalnego poprzez VPN do sieci szpitalnej za pośrednictwem sprzętu prywatnego użytkownika, wykaz stanowisk i komórek organizacyjnych mający dostęp do programów i zasobów, wzór nadania i odebrania uprawnień w systemie informatycznym, upoważnienia do przetwarzania danych osobowych, instrukcja tworzenia kopii zapasowych, wzór zniszczenia uszkodzonych nośników komputerowych, ewidencja udostępniania danych, wzór protokołu usunięcia danych osobowych.

[8] Dz. U. poz. 1560. (zwana dalej: ustawą o cyberbezpieczeństwie).

Powyższe uregulowania zostały zatwierdzone przez Dyrektora Szpitala.

Po wejściu w życie RODO, IOD nie aktualizował PODO i IZSI. Opracowana dokumentacja nie wymagała aktualizacji z uwagi na zmiany w przepisach prawa, zmiany organizacyjne Szpitala lub wdrożenie nowych rozwiązań informatycznych.

(akta kontroli str.123-132, 142-159, 163-166, 206)

IOD wyjaśnił, że postanowienia PODO i IZSI zostały zamieszczone do zapoznania się przez personel w wewnętrznej sieci Szpitala. Dokumenty określające techniczne aspekty zabezpieczeń zostały udostępnione jedynie pracownikom służb informatycznych Szpitala, odpowiedzialnych za wdrożenie i stosowanie tych regulacji.

(akta kontroli str. 163-167)

W Szpitalu funkcjonowała Instrukcja udostępniania dokumentacji medycznej.

Została ona opisana na stronie internetowej[9] i opisywała, w jaki sposób należy udostępniać dokumentację medyczną pacjentom oraz jakie inne organy mają do niej dostęp, wraz ze sposobem udostępniania tej dokumentacji.

W dokumentach podstawowych nie określono konieczności opracowania dodatkowych reguł i procedur uszczegóławiających te dokumenty.

(akta kontroli str. 163-169)

1.3. Rejestr czynności przetwarzania był prowadzony w Szpitalu do 24 maja 2018 r. przez Administratora Bezpieczeństwa Informacji, a od 25 maja 2018 r. przez IOD (czym spełniono obowiązek wskazany w art. 30 RODO). Obok formy papierowej była również forma elektroniczna (excel) tego rejestru. Według stanu na 14 lutego 2019 r. liczył on 11 pozycji, zawierających wszystkie dane wymagane art. 30 ust. 1 RODO.

(akta kontroli str. 55-57, 163-164, 170, 238-239)

1.4. Stosownie do art. 32 RODO, w dniu 27 sierpnia 2018 r., IOD przeprowadził analizę procesów przetwarzania danych osobowych pacjentów Szpitala dla 16 ryzyk, przypisując im wartość punktową oceny prawdopodobieństwa wystąpienia ryzyka m.in. awaria sprzętowa/programowa serwera, utrata zasilania –, zawirusowanie, włamanie/wyciek informacji, awaria łącza internetowego, pożar, zalanie, ujawnianie danych osobowych w pomieszczeniach biurowych – 1 pkt. oraz awaria stacji roboczej, pomyłki informatyków i użytkowników, uzyskanie dostępu do serwerowni, wydanie kluczy nieodpowiedniej osobie, błąd, awaria oprogramowania, nieprzestrzeganie zasad ochrony danych przez użytkowników - 2 punkty.

Dla każdego z procesów przetwarzania danych wskazano ryzyka i dokonano określenia jego istotności.
W Szpitalu wprowadzono od 28 sierpnia 2018 r. Plan postępowania z ryzykiem i szansami, tj. rodzaj ryzyka, skutki, działania zapobiegawcze, działania minimalizujące ryzyko, osoby odpowiedzialne. Do 8 kwietnia 2019 r. dla 16 ryzyk zawartych w Planie podjęto działania minimalizujące dla 6 ryzyk (poz. 7,8,12,13,14,16 Planu).
Na przykład w przypadku awarii sprzętowej lub programowej serwera jako ryzyko ustalono brak możliwości pracy i utrata danych. Działaniem zapobiegawczym było m.in. tworzenie kopii zapasowych. Jako odpowiedzialnych za działania naprawcze wskazano informatyków Szpitala.

(akta kontroli str. 15-29, 238)

1.5. Stosownie do art. 35 RODO, w dniu 27 sierpnia 2018 r. w Szpitalu przeprowadzono ocenę skutków dla ochrony danych osobowych (dalej: DPIA).

[9] https://www.dzieciecyszpital.pl/pl/udostepnianie-dokumentacji-medycznej

Ocena zawierała część danych wymaganych art. 35 ust. 7 RODO. W DPIA brak było oceny, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów oraz oceny ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1. Ocena ta była fakultatywna i taka pojedyncza (bieżąca) ocena dotyczyć powinna operacji wiążących się z wysokim ryzykiem. Również Grupa Robocza Art. 29 ds. Ochrony Danych[10] zdecydowanie zalecała dokonanie DPIA dla operacji przetwarzania już trwających przed 25 maja 2018 r.[11] oraz w przypadkach, gdy nie jest jasne, czy wymagana jest DPIA. Uznano, bowiem, że jest ona „przydatnym narzędziem, które może pomóc administratorom danych w zapewnieniu zgodności z prawem ochrony danych", chociaż Prezes UODO w komunikacie[12] wydanym na podstawie art. 35 ust. 4 RODO wśród rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony, nie zawarł danych medycznych przetwarzanych w szpitalach, jako wymagających oceny skutków przetwarzania.

Wysokie ryzyko oszacowano w przypadku kradzieży danych oraz nieprzestrzegania zasad ochrony danych przez użytkowników. W celu wyeliminowania ryzyka zaproponowano wpływ na użytkowników poprzez szkolenie dotyczące ochrony danych osobowych. Po 25 maja 2018 r. nie rozpoczęto przetwarzania nowych kategorii danych.

(akta kontroli str. 21-28, 163-164, 167, 238)

1.6. Jednym z zadań IOD, w myśl art. 39 ust. 1 lit. b RODO było prowadzenie szkoleń personelu uczestniczącego w operacjach przetwarzania danych. Po wejściu w życie przepisów RODO 320 pracowników Szpitala (67,5 %) zostało objętych szkoleniem w formie czterech warsztatów, przeprowadzanych przez IOD w czerwcu 2018 r. Szkolenia te obejmowały m.in. zaznajomienie z przepisami RODO oraz przepisami rozporządzenia KRI. Tematy przedstawione na szkoleniach obejmowały m.in. zagrożenia bezpieczeństwa informacji, skutki naruszenia zasad bezpieczeństwa informacji i odpowiedzialności prawnej.

Pracownicy przetwarzający dane osobowe w Szpitalu, którzy z różnych przyczyn nie uczestniczyli w tych szkoleniach otrzymali materiały szkoleniowe drogą mailową z obowiązkiem zapoznania się z nimi.

(akta kontroli str. 31,163-164, 167-168,213-217, 238)

1.7. Po ukazaniu się (24 września 2018 r.) przewodnika „RODO w służbie zdrowia"[13] IOD rozesłał jego treść do pracowników Szpitala za pomocą poczty elektronicznej. Szpital nie zobowiązał się formalnie do przestrzegania regulacji zawartych w tym przewodniku.

(akta kontroli str. 163-164, 167)

---

[10] Grupa Robocza była niezależnym organem doradczym w zakresie ochrony danych i prywatności. Została ona powołana na mocy art. 29 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. UE L 281 z 1995 r., str. 31, ze zm.) i działała do 25 maja 2018 r.

[11] Dokument pt.: Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679 https://www.giodo.gov.pl/1520281/id_art/9957/j/pl

[12] Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 sierpnia 2018 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (M. P. poz. 827).

[13] Poradnik opracowany przez Grupę Roboczą ds. ds. Ochrony Danych Osobowych, utworzoną w Ministerstwie Cyfryzacji https://www.gov.pl/web/cyfryzacja/rodo-w-sluzbie-zdrowia-po-pierwsze-pacjent – dostęp z 4 grudnia 2018 r.

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następującą nieprawidłowość:

Nieobjęcie wszystkich pracowników Szpitala zajmujących się przetwarzaniem danych osobowych pacjentów szkoleniami z zakresu bezpieczeństwa danych w związku z wejściem w życie RODO. Według stanu na 13 czerwca 2018 r. szkoleniami w zorganizowanej formie nie objęto 32,5% personelu Szpitala.

Jak wyjaśnił IOD: pracownicy przetwarzający dane osobowe w Szpitalu, którzy z różnych przyczyn nie uczestniczyli w szkoleniu otrzymali materiały szkoleniowe drogą mailową z obowiązkiem zapoznania się z nimi. Każdy pracownik podpisał oświadczenia o poufności (stanowi ono załącznik nr 11 do Polityki Ochrony Danych Osobowych) mówiące m.in., że osoba zapoznała się z przepisami dotyczącymi ochrony danych osobowych, w szczególności z RODO oraz odnośnymi wymaganiami „Regulaminu Ochrony Danych Osobowych".

W dokumentacji Szpitala brak było potwierdzeń pracowników na okoliczność zapoznania się z otrzymanymi materiałami szkoleniowymi.

Nieobjęcie szkoleniami wszystkich pracowników przed wejściem w życie przepisów RODO, tj. przed 25 maja 2018 r., NIK traktuje jako nieprawidłowość z uwagi na 25. miesięczne *vacatio legis* dla tego rozporządzenia. Tak długi okres czasu umożliwiał przeszkolenie wszystkich pracowników uczestniczących w procesach przetwarzania danych odpowiednio wcześniej.

(akta kontroli str. 31,163-164, 167-168,213-217, 238)

OCENA CZĄSTKOWA

Szpital wywiązał się z obowiązku opracowania i wdrożenia dokumentacji oraz procedur dotyczących ochrony danych osobowych. Powołano IOD oraz terminowo zgłoszono to do Prezesa UODO. Terminowo opracowano i właściwie prowadzono rejestr czynności przetwarzania danych osobowych, który zawierał wszystkie wymagane elementy, przeprowadzono analizę procesów przetwarzania danych osobowych pacjentów, wskazując dla każdego z nich ryzyka z określeniem ich istotności. Ponadto w Szpitalu wprowadzono *Plan postępowania z ryzykiem i szansami*, określając w nim rodzaje ryzyk, ich skutki, działania zapobiegawcze i minimalizujące ryzyko oraz osoby odpowiedzialne.

Zdaniem NIK za ryzyko dla bezpieczeństwa w zakresie ochrony danych, które może skutkować innymi nieprawidłowościami w przyszłości (jeżeli Szpital nie podejmie odpowiednich działań) należy uznać stwierdzoną nieprawidłowość, tj. nieobjęcie wszystkich pracowników Szpitala szkoleniami związanymi z wejściem w życie RODO. Osiągnięty w czerwcu 2018 r. wskaźnik 67,5% przeszkolonych pracowników, zdaniem NIK należy uznać za niesatysfakcjonujący. Systematyczny i cykliczny system szkoleń z zakresu ochrony danych osobowych, w tym RODO, dla personelu medycznego Szpitala, w szczególności tzw. szkoleń przypominających, sprzyjać będzie minimalizacji ryzyk przy przetwarzaniu ww. danych.

OBSZAR

2. Zapewnienie prawidłowego przetwarzania danych osobowych

Opis stanu faktycznego

2.1. Oględzinami objęto Rejestrację Szpitala, trzy oddziały szpitalne (Oddziały: Dzieci Starszych Reumatologia i Neurologia, Dzieci Starszych Gastrologia i Alergologia, Pulmonologii) oraz trzy gabinety lekarskie (Gabinety: Pulmonologiczny, Alergologiczny i Logopedyczny).

W celu właściwej ochrony danych osobowych w Szpitalu funkcjonowały poniżej wymienione rozwiązania:

- Przed okienkami rejestracji wyznaczona była linia, za którą oczekiwali kolejni pacjenci. W trakcie oględzin pacjenci niebędący bezpośrednio przy okienku rejestracji, nie wchodzili poza wyznaczoną linię.
- Nad okienkiem rejestracji znajdowała się informacja, że w związku z RODO Szpital zachowuje w tajemnicy dane osobowe, zatem pracownicy Szpitala nie wymawiali ich na głos i jednocześnie nie prosili o ich podawanie przez pacjentów, ale wymagane było okazanie dowodu osobistego w celu weryfikacji danych. Obok na tablicy informacyjnej znajdowała się informacja o przetwarzaniu danych, na której wskazano m.in. administratora, IOD, cele i podstawy przetwarzania danych, ich kategorie, odbiorców, okres przechowywania danych oraz prawo do dostępu, sprostowania, przenoszenia, wnoszenia skargi.
- W zasięgu wzroku pacjentów rejestrujących się na świadczenia medyczne nie znajdowały się dane osobowe innych pacjentów.
- Podczas przeprowadzonych oględzin rejestracji pacjentów do poradni specjalistycznych pacjent otrzymywał karteczkę z datą i planowaną godziną przyjęcia. Do poradni pacjenci byli proszeni przez lekarzy, bez używania danych osobowych (podawano imię pacjenta i godzinę planowanej wizyty).
- Dokumentację pacjentów przechowywano w dyżurkach pielęgniarskich i lekarskich oraz gabinetach poradni specjalistycznych we właściwy sposób (elektronicznie lub w zamykanej szufladzie).
- W dyżurkach pielęgniarskich na trzech objętych oględzinami oddziałach szpitalnych ruch chorych14 prowadzony był w miejscu niewidocznym dla osób postronnych (dane pacjentów były ukryte). Podręczna dokumentacja pielęgniarska przechowywana była w zamykanych szafkach. Podobne zamykane miejsca do przechowywania dokumentacji medycznej znajdowały się w gabinetach lekarskich oraz gabinetach poradni specjalistycznych.
- W salach chorych pacjenci (dzieci) posiadali na nadgarstkach opaski z unikalnym kodem (MIP) oraz imię i nazwisko. Były to wydruki ze specjalistycznej drukarki.
- Personel pielęgniarski i lekarski, w czasie oględzin nie opuszczał dyżurek i nie pozostawił uruchomionych komputerów.
- W Szpitalu od 2010 r. funkcjonował monitoring wizyjny, obejmujący korytarze szpitalne oraz tereny na zewnątrz wokół obiektów. Zapisane obrazy z monitoringu przechowywane były przez okres trzech dni (po jego upływie automatycznie kasowane i nadpisywane). W przypadku niepożądanego zajścia sporządzana była kopia zapasowa. Do podglądu zapisanych obrazów upoważnione były tylko osoby spośród pracowników Szpitala i współpracowników (świadczących usługi na rzecz Szpitala). W Szpitalu opracowany został Regulamin monitoringu. Po wejściu w życie przepisów RODO Szpital wprowadził do Regulaminu Pracy zapisy dotyczące monitoringu.

[14] Ruch chorych to lista pacjentów danego oddziału wraz z numerem sali, w których przebywają.

O zapisach tych pracownicy zostali mailowo poinformowani, regulamin został umieszczony na stronie intranetowej i tablicy ogłoszeń Szpitala.

(akta kontroli str. 78-95,168-169, 206, 213-224,234-235, 238)

2.2. Zarządzanie siecią odbywało się za pomocą usługi Active Directory, tj. zarządzane było centralnie przez administratora infrastruktury informatycznej Szpitala. Przeprowadzone oględziny tej usługi wykazały, że w panelu administratora dostęp personelu administracyjnego możliwy był jedynie po odpowiednim przeprowadzeniu autoryzacji użytkownika, tj. wprowadzeniu przez niego loginu i hasła.

Dane medyczne gromadzone były głównie w dwóch systemach informatycznych:

- HIS (Hospital Information System) – system informatyczny do obsługi Szpitala, którego głównym zadaniem jest obsługa pacjenta w poradniach i na oddziałach, tworzenie elektronicznej dokumentacji medycznej;
- EDM (Electronic Health Record) – Elektroniczna Dokumentacja Medyczna – system informatyczny przechowujący część lub całość dokumentacji medycznej indywidualnej i/lub zbiorczej w podmiocie leczniczym (w systemie tym przechowywana jest elektroniczna dokumentacja medyczna wytworzona wcześniej w systemie HIS).

(akta kontroli str. 89)

Upoważnienia do przetwarzania danych osobowych wydawane były także pracownikom administracyjnym (przetwarzanie danych osobowych pracowników Szpitala).

Personel działów administracyjnych Szpitala liczył 65 osób, z których 33 posiadało dostęp do systemu HIS. Byli to m.in. pracownicy Działu Dokumentacji i Statystyki, Rejestracji, Działu Planowania i Rozliczeń Świadczeń Medycznych, Działu Modernizacji i Rozwoju, Działu Marketingu, niektórzy pracownicy służby księgowo-finansowej i administracyjno-technicznej, Działu Informatyki. Nadane np. pracownikom Działu Modernizacji i Rozwoju, Działu Marketingu i Działu Administracyjno-Technicznego uprawnienia były im niezbędne i odpowiadały zakresom zadań i obowiązków realizowanych przez te osoby. Do systemu EDM nie były tworzone indywidualne konta. O tym czy użytkownik ma uprawnienia do dostępu do EDM decydowały uprawnienia przyznane w HIS. Na tej podstawie następował odczyt lub zapis w EDM. Do EDM użytkownicy nie logowali się bezpośrednio.

(akta kontroli str. 70-76, 238-247)

2.3. Wszystkie pielęgniarki i położne (130) zatrudnione w Szpitalu posiadały założone konta i dostęp do HIS (AMMS). Każda, z objętych badaniem 11 pielęgniarek, uruchamiała system operacyjny poprzez podanie loginu i hasła (spełniały wymagania przyjęte w PODO), brak było możliwości zainstalowania obcego oprogramowania oraz zawartości nośników poprzez port USB. Nie stwierdzono w lokalizacji Pulpit listy pacjentów lub plików tekstowych zwierających dane medyczne pacjentów.

Pielęgniarki pracowały w różnych Oddziałach Szpitala, dostęp nadawany był do grupy Oddziałów posiadających zbliżone specjalności medyczne. Nadane w systemie uprawnienia były adekwatne do wykonywanych przez pielgniarki zadań. Pielęgniarki te świadczyły prace we wszystkich oddziałach tej grupy.

Wyjątek stanowił Oddział Psychiatrii, gdzie dostęp miały tylko pielęgniarki tego Oddziału.

Poza lekarzami oraz pielęgniarkami i położnymi Szpital nie wydawał upoważnień do przetwarzania danych osobowych innym osobom (np. sanitariuszom, salowym lub

personelowi sprzątającemu). Ustalenia dokonano na grupie wszystkich pracowników, którym wydano takie upoważnienia.

(akta kontroli str. 75-77, 90-95, 238)

2.4. Od 25 maja 2018 r. do 26 lutego 2019 r. 29 osób zakończyło zatrudnienie w Szpitalu. Spośród nich, 21 w trakcie zatrudnienia miało przyznany dostęp do systemów informatycznych, w tym systemu AMMS.

Przeprowadzona analiza terminu odebrania uprawnień wszystkim 21 osobom wykazała, że: w dwóch przypadkach dostęp odebrano po upływie 67 i 101 dni po zakończeniu zatrudnienia, w dwóch przypadkach dostęp odebrano po upływie od 3 do 4 dni po zakończeniu zatrudnienia, w siedmiu przypadkach dostęp odebrano po upływie jednego dnia po zakończeniu zatrudnienia, w 10 przypadkach dostęp do systemu AMMS odebrano przed lub w dniu rozwiązania stosunku pracy.

(akta kontroli str. 69)

2.5. W okresie objętym kontrolą Szpital miał zawarte dwie umowy dotyczące świadczenia usług serwisu oprogramowania oraz pomocy technicznej tzw. help desk.

Spółka z Krakowa serwisowała m.in. systemy integracyjne z HIS, PACS. W dniu 17 września 2018 r. zawarła ze Szpitalem umowę na świadczenie usługi serwisu pogwarancyjnego i powierzenia przetwarzania danych osobowych. Zgłoszenia odbywały się za pomocą poczty e-mail oraz telefonu.

Spółka z Rzeszowa serwisowała pozostałe systemy. W dniu 25 maja 2018 r. Firma zawarła ze Szpitalem umowę powierzenia danych osobowych. Zgłoszenia odbywały się za pomocą przeznaczonego do tego celu portalu.

Badaniem objęto 60 zamkniętych zgłoszeń do Spółki z Rzeszowa zarejestrowanych od 28 września 2018 r. do 7 grudnia 2018 r. Oględziny zgłoszeń i przekazanych wraz z nimi załączników wykazały, że w dwóch przypadkach zgłoszenia Firmie z Rzeszowa przekazano dane osobowe i medyczne dwóch pacjentów.

(akta kontroli str. 172-205, 239)

2.6. Szpital zawarł 25 umów dotyczących powierzania przetwarzania danych osobowych pacjentów (23 umowy zawarte w okresie objętym kontrolą), m.in. ze szpitalami, podmiotami wykonującymi badania, kancelarią adwokacką, serwisem brokerskim, regionalnym centrum krwiodawstwa, pogotowiem ratunkowym,

Szczegółowym badaniem pod kątem wymagań określonych w art. 28 RODO objęto 6 umów, w których Szpital był podmiotem powierzającym przetwarzanie.

Umowy te zawierały wszystkie elementy zawarte w art. 28 RODO. Wskazany w tych umowach zakres danych osobowych powierzonych przez Szpital podmiotowi zewnętrznemu wynikał z rodzaju usług, które zgodnie z umowami miał na rzecz Szpitala realizować.

W badanym okresie Szpital, jako przetwarzający dane zawarł 15 umów.

(akta kontroli str. 32-54, 172-182, 239)

2.7. Na podstawie rejestru stwierdzonych przypadków naruszenia bezpieczeństwa danych osobowych w badanym okresie stwierdzono pięć takich przypadków, w tym trzy były związane z awarią dostawy prądu. W jednym przypadku kobieta wykonywała zdjęcia budynków Szpitala i pacjentów. Sprawę zgłoszono Policji. W drugim przypadku w dniu 26 lipca 2018 r. niezrównoważony psychicznie mężczyzna skradł z pomieszczenia Rejestracji trzy kartoteki pacjentów. Jedną kartotekę odnaleziono. Sprawę 26 lipca 2018 r. zgłoszono Policji. Kartotek nie odzyskano. Incydent ten został zgłoszony do Prezesa UODO terminowo, tj. 26 lipca 2018 r. i zawierał elementy wymagane przez art. 33 ust. 3 RODO.

W badanym okresie nie stwierdzono skarg związanych z przypadkami ujawnienia danych osobowych.

Szczegółowe procedury postępowania w przypadku wystąpienia przypadków naruszenia zasad stanowiły część polityki ochrony danych osobowych Szpitala.

(akta kontroli str. 58-68)

2.8. W Szpitalu obowiązywała instrukcja udostępniania dokumentacji medycznej, w której określono szczegółowe zasady w tym zakresie, a także wzór wniosku o udostępnienie oraz wzór rejestru wniosków o sporządzenie wyciągu, odpisu, kopii dokumentacji medycznej.

W badanym okresie osobom indywidualnym wydano dokumentacje 524 razy, a uprawnionym instytucjom 10 razy. Nie udostępniano dokumentacji medycznej instytucjom ubezpieczeniowym.

Badaniem objęto 30 spraw o udostępnienie dokumentacji medycznej osobom fizycznym innym niż pacjent, którego dokumentacja medyczna dotyczy. W każdym przypadku osoba, której udostępniono dokumentację medyczną posiadała upoważnienie pacjenta do dostępu lub była do tego uprawniona, jako opiekun osoby niepełnoletniej. W żadnym przypadku nie było podstaw, aby odmówić udostępnienia dokumentacji. Upoważnienia dla osób fizycznych będących opiekunami prawnym małoletnich pacjentów były weryfikowane poprzez sprawdzenie dowodu tożsamości.

(akta kontroli str. 159-162, 169, 239)

2.9. Regulacje wewnętrzne Szpitala dotyczące sposobu zabezpieczenia fizycznego posiadanej infrastruktury informatycznej (pomieszczenia serwerowni, punktów dostępowych, serwerów, wykonywanych kopii bezpieczeństwa, układów podtrzymywania napięcia) oraz regulacje dotyczące wprowadzenia w jednostce ochrony kryptograficznej (szyfrowania, pkt 4 ust. 5 IZSI) lub pseudonimizacji danych osobowych znajdowały się w PODO, IZSI, Regulaminie monitoringu i Instrukcji Odtwarzania Kopii Zapasowych.

Na stacjach roboczych zainstalowane było oprogramowanie antywirusowe. Oprogramowanie to było także wykorzystywane do kontroli pendrive. Każdy z użytkowników (sprawdzono na przykładzie 30 pracowników) posiadł swój własny login i hasło. Pracownicy logowali się do komputerów na swoje indywidualne konta. Po zalogowaniu do systemu operacyjnego uzyskiwali dostęp do swoich plików i katalogów na pulpicie. Zalogowanie się do HIS (AMMS) wymagało każdorazowo wprowadzenia loginu i hasła tożsamego jak do systemu operacyjnego. Użytkownicy nie logowali się bezpośrednio do systemu EDM (tylko za pośrednictwem AMMS).

(akta kontroli str. 90-95, 123-158)

W wyniku oględzin stwierdzono, że pomieszczenie serwerowni nie było oznakowane i posiadało 12,6 m² powierzchni użytkowej. Serwerownia służyła do przechowywania/przetwarzania danych medycznych oraz zapewnienia połączenia z internetem. Zabezpieczeniem dostępu do serwerowni były drzwi stalowe, przeciwwłamaniowe, przeciwpożarowe, zamykane na zwykły zamek. Przed otwarciem drzwi wymagane było wpisanie kodu. Każde wejście do serwerowni było odnotowywane w zeszycie przy pobraniu kluczy przez upoważnionych informatyków z portierni. W serwerowni działała instalacja alarmowa. W serwerowni zainstalowano klimatyzację nadmiarową, czujniki temperatury i system przeciwpożarowy i antywłamaniowy. W pomieszczeniu znajdowała się gaśnica. Urządzenia serwerowni podłączone były do układu podtrzymywania napięcia UPS. Na zewnątrz pomieszczenia znajdowała się kamera monitoringu. Serwery znajdowały się w dwóch specjalnych szafach (na podwyższeniu nad podłogą). Stan okablowania nie nosił oznak uszkodzenia. W okolicach sufitu pomieszczenia serwerowni przebiegały rury centralnego ogrzewania. W przypadku awarii instalacji centralnego ogrzewania może to być potencjalnym zagrożeniem zalania serwerowni.

W pomieszczeniu nie znajdowały się urządzenia komputerowe wycofane z użytku, materiały łatwopalne (meble, dokumentacja).
W Szpitalu prowadzony był remont starego budynku. Na okres remontu tymczasowo funkcjonowała jedna serwerownia. Zagospodarowanie i uruchomienie pomieszczenia drugiej serwerowni przewidywane było na koniec 2019 r.

(akta kontroli str. 5-6)

W wyjaśnieniu Główny Specjalista ds. Sieci Informatycznych Szpitala podał, że kopia bezpieczeństwa była wykonywana raz w tygodniu, jako kopia całości danych baz oraclowych HIS i EDM, zgromadzonych na serwerach (z wyłączeniem obrazów DICOM i EEG). Natomiast każdego dnia wielokrotnie wykonywano kopie archivelog. Kopie zapasowe były przechowywane w pomieszczeniu Działu Informatycznego w zamykanej na klucz szafie. Pomieszczenie było zabezpieczone instalacją alarmową. W każdym tygodniu przed zmianą nośników było wykonywane sprawdzenie czy zaplanowane zadanie zostało wykonane i czy nie zwróciło błędu. Dodatkowo dla wszystkich baz oraclowych było wykonywane sprawdzenie czy dane w serwerze zapasowym odtworzyły się poprawnie. W Szpitalu użytkowano 7 sztuk komputerów przenośnych. Cztery komputery użytkowane przez pracowników administracyjnych posiadały szyfrowanie dysku. Pozostałe trzy komputery przenośne nie posiadały szyfrowania dysku. W wyjaśnieniu IOD podał, że komputery te nie zawierały danych chronionych, umożliwiały tylko dostęp do tych danych zlokalizowanych na serwerach po skutecznym uwierzytelnieniu się. Komputery te zostały zaszyfrowane.

(akta kontroli str. 30, 234-235, 239)

W Szpitalu w badanym okresie przeprowadzono dwa audyty, tj. 21 grudnia 2018 r. w zakresie bezpieczeństwa informacji oraz od 12 listopada do 12 grudnia 2018 r. w zakresie zgodności przetwarzania danych.
Audyt dotyczący bezpieczeństwa informacji dotyczył sprawdzenia zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia, utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmujących ich rodzaj i konfiguracje, przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących ryzyko, podejmowania działań zapewniających posiadanie stosownych uprawnień, zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji, zapewnienia ochrony przetwarzanych informacji, ustanowienia podstawowych zasad gwarantujących bezpieczna pracę przy przetwarzaniu danych, odpowiedni poziom bezpieczeństwa informacji w umowach serwisowych, ustalenia zasad postepowania z informacjami zapewniających minimalizacje wystąpienia ryzyka, zapewnienia poziomu bezpieczeństwa w systemach informatycznych, zgłaszania incydentów naruszenia bezpieczeństwa informacji. Nie stwierdzono niezgodności. Zalecono działania doskonalące, m.in. przeprowadzenie kontroli uprawnień dwa razy do roku oraz przypomniano o konieczności zgłaszania zmian w przepisach.
Na podstawie oględzin 30 komputerów użytkowanych przez pracowników przetwarzający dane osobowe stwierdzono, że użytkownicy ci (lekarze, pielęgniarki i pracownicy administracyjni) mieli uprawnienia do dostępu danych osobowych w systemie HIS. Każdy użytkownik posługiwał się własnym loginem i hasłem do dostępu do systemu operacyjnego i AMMS (hasła posiadały odpowiednią długość i podlegały okresowej zmianie – raz na miesiąc). Ustalenia oględzin były zgodne z ustaleniami audytu.
W przypadku audytu dotyczącego badania zgodności przetwarzania danych osobowych Szpitala dokonał sprawdzenia aspektów prawnych i organizacyjnych zabezpieczenia, realizacji praw osób, analizy ryzyka, oceny skutków, zabezpieczeń

organizacyjnych, fizycznych, technicznych, informatycznych oraz zewnętrznych. Nie stwierdzono niezgodności.

(akta kontroli str. 96-122, 218-224)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

1. Konta użytkowników czterech (na 21 przypadków) byłych pracowników Szpitala w systemie AMMS zostały zablokowane po upływie odpowiednio: 101, 67, 4 i 3 dni po dacie rozwiązania z nimi stosunku pracy.

   Stanowiło to naruszenie § 20 ust. 2 pkt 5 rozporządzenia KRI, zgodnie, z którym należy podejmować działania polegające na bezzwłocznej zmianie uprawnień w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji.

   W wyjaśnieniu IOD podał, że przyczyną braku bezzwłocznego zablokowania kont użytkowników po rozwiązaniu stosunku pracy była nieprawidłowa komunikacja pomiędzy służbami Szpitala. Procedura nadawania uprawnień do przetwarzania danych nie posiadała wskazania, że uprawnienia te winny być odebrane w dniu rozwiązania stosunku pracy.

   (akta kontroli str. 69, 216)

   Zdaniem NIK, mając na uwadze § 20 ust. 2 pkt 5 rozporządzenia KRI, zasadne jest zapewnienie prawidłowego obiegu informacji pomiędzy służbami Szpitala.

2. Pacjenci (dzieci) posiadali na nadgarstkach opaski z unikalnym kodem (MIP) oraz imię i nazwisko. Opaski były zwrócone na zewnątrz, przykryte rękawkami koszulki dziecka. Rodzice przy przyjęciu dziecka do Szpitala podpisywali zgodę na używanie imienia i nazwiska dziecka. Zgoda ta nie była obligatoryjna. Szpital nie posiadał wewnętrznej procedury w tym zakresie.

   Zgodnie z art. 36 ust. 5 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej[15] opaska zawierać powinna informacje zapisane w sposób uniemożliwiający identyfikację pacjenta przez osoby nieuprawnione.

   W wyjaśnieniu Dyrektor Szpitala podał, że opaski na nadgarstkach pacjentów z imionami i nazwiskami pacjentów umieszczane były w celu ochrony życia i zdrowia. Ułatwiały one personelowi medycznemu niezwłoczną identyfikację pacjenta i pozwalały uniknąć pomyłki i narażenia pacjenta na utratę zdrowia lub życia. W planach Szpitala było wprowadzenie elektronicznej dokumentacji medycznej i zakupienie tabletów medycznych z dostępem do systemu AMMS, które umożliwią identyfikację pacjenta po unikalnym kodzie MIP (nadawany w chwili przyjęcia do Szpitala). Koszt tabletów i czytników dla całego Szpitala wynosiłby około 240 tys. zł. Dodatkowo do budynku Szpitala należy doprowadzić sieć WiFi. W chwili obecnej Szpital jest w trakcie generalnego remontu i brak jest środków finansowych potrzebnych na zakup takiego sprzętu elektronicznego. Aby uniknąć możliwości identyfikacji pacjenta przez osoby nieupoważnione, Szpital wprowadził umieszczanie opasek z imieniem i nazwiskiem pacjenta na nadgarstkach treścią do spodu.

   (akta kontroli str. 78-83, 218-224,236-238)

   Zdaniem NIK, wprawdzie występowaly przeszkody finansowe oraz ograniczone zostało ryzyko możliwości identyfikacji pacjenta przez osoby nieupoważnione, poprzez umieszczanie jego imienia i nazwiska na wewnętrznej stronie opaski, to

[15] Dz. U. z 2018 r. poz. 2190, ze zm.

jednak mając na uwadze treść cytowanego wyżej aktykułu brak jest podstaw do stosowania tego typu praktyk.

3. W dwóch przypadkach (na 60), zgłaszając firmie serwisowej błąd systemowy, Szpital przekazał dane osobowe i medyczne dwóch pacjentów.

   W zgłoszeniu z 30 października 2018 r. zostały przekazane wyniki tomografii komputerowej głowy pacjenta w związku z odrzuceniem rozliczenia przez NFZ. W zgłoszeniu z 7 listopada 2018 r. w związku z błędem generacji dokumentu zostały przekazane wyniki badania mikrobiologicznego pacjenta.

   Stanowiło to naruszenie zasady określonej w art. 5 ust. 1 lit. c RODO, tj. zapewnienia, aby przetwarzanie danych osobowych było adekwatne i ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych").
   W wyjaśnieniu IOD podał, że przesłanie wyników badania ww. pacjentów było niezbędne z uwagi na konieczność analizy błędu konkretnego przypadku – konkretnego pacjenta. Podanie danych pacjentów usprawniło rozwiązanie błędów systemowych. Było to konieczne z uwagi na rodzaj awarii, a dane były przesyłane szyfrowaną stroną z zabezpieczeniem.

   (akta kontroli str. 183-205, 215)

   NIK zwraca jednak uwagę, że system AMMS przypisuje każdemu pacjentowi indywidualny identyfikator, numer ID pacjenta. Realizując zasadę minimalizacji danych, w zgłoszeniach serwisowych należało posługiwać się tym numerem w celu wskazania błędu dotyczącego konkretnego pacjenta.

OCENA CZĄSTKOWA

W ocenie NIK wdrożone w Szpitalu rozwiązania techniczne i organizacyjne nie zapewniały w pełni prawidłowego przetwarzania i ochrony danych osobowych.

W okresie objętym kontrolą Szpital w sposób prawidłowy zawarł umowy powierzenia przetwarzania danych, które zawierały wymagane przez RODO postanowienia. Właściwie dokumentowano naruszenia ochrony danych osobowych oraz podejmowano odpowiednie działania w tym zakresie. Prawidłowo udostępniano dokumentację medyczną pacjentów oraz podejmowano odpowiednie działania w celu minimalizacji ryzyka utraty danych osobowych w wyniku awarii, błędów lub nieuprawnionej modyfikacji.

Tym niemniej potencjalne ryzyka dla prawidłowego przetwarzania i ochrony danych osobowych wynikały z trzech stwierdzonych nieprawidłowości, tj.:

- opóźnień w odbieraniu byłym pracownikom Szpitala dostępu do systemów informatycznych (cztery przypadki na 21),
- stosowanie na opaskach danych umożliwiających identyfikację pacjenta,
- przekazania dostawcy oprogramowania danych osobowych i medycznych pacjentów (dwa przypadki na 60).

IV. Wnioski

W związku ze stwierdzonymi nieprawidłowościami, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK, przedstawia następujące wnioski:

Wnioski

1) zapewnienie personelowi uczestniczącemu w operacjach przetwarzania danych szkoleń w zakresie adekwatnym do wykonywanych zadań;
2) bieżące odbieranie uprawnień do systemu HIS (AMMS) dla osób, które przestały być pracownikami;
3) wyeliminowane ze stosowanych opasek danych umożliwiających identyfikację pacjentów przez osoby nieuprawnione;

4) dokonywanie zgłoszeń serwisowych w sposób zapewniający ochronę danych osobowych i medycznych pacjentów.

V. Pozostałe informacje i pouczenia

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden dla kierownika jednostki kontrolowanej, drugi do akt kontroli.

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 ustawy o NIK kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do dyrektora Delegatury NIK w Krakowie. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Obowiązek poinformowania NIK o sposobie wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 21 dni od otrzymania wystąpienia pokontrolnego, o sposobie wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Kraków, kwietnia 2019 r.

Kontroler

Zbigniew Polak
główny specjalista kontroli państwowej