NAJWYŻSZA IZBA KONTROLI

Delegatura w Lublinie

LLU.410.003.03.2019

Pan Marek Zawada
Samodzielny Publiczny Zakład Opieki Zdrowotnej
w Radzyniu Podlaskim
ul. Wisznicka 111
21-300 Radzyń Podlaski

WYSTĄPIENIE POKONTROLNE

Zmienione zgodnie z treścią uchwały nr KPK-KPO.443.118.2019
Komisji Rozstrzygającej w Najwyższej Izbie Kontroli z dnia 14 czerwca 2019 r.

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

NAJWYŻSZA IZBA KONTROLI
Delegatura w Lublinie
ul. Okopowa 7, 20-022 Lublin
T +48 81 461 31 20, F +48 81 461 31 11
llu@nik.gov.pl
Adres korespondencyjny: Skr. poczt. P-112, 20-001 Lublin 1

I. Dane identyfikacyjne

Jednostka kontrolowana

Samodzielny Publiczny Zakład Opieki Zdrowotnej w Radzyniu Podlaskim (dalej: *Szpital, ZOZ lub Placówka*), ul. Wisznicka 111, 21-300 Radzyń Podlaski

Kierownik jednostki kontrolowanej

Marek Zawada, Dyrektor Szpitala od 1 stycznia 2011 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

Kontrola objęła okres od 25 maja 2018 r. do dnia zakończenia czynności kontrolnych, tj. 12 kwietnia 2019 r. Badania kontrolne mogły dotyczyć działań sprzed tego okresu, jeśli mały 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 Lublinie

Kontroler

1. Małgorzata Dobrowolska, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LLU/39/2019 z 11.02.2019 r.
2. Marek Raczkowski, specjalista kontroli państwowej, upoważnienie do kontroli nr LLU/50/2019 z 18.03.2019 r.

(akta kontroli str.1-5)

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

Najwyższa Izba Kontroli ocenia negatywnie przygotowanie SP ZOZ w Radzyniu Podlaskim do wdrożenia niezbędnych regulacji dotyczących ochrony danych osobowych oraz sposób korzystania z dostępnych Placówce środków technicznych i organizacyjnych w celu prawidłowego przetwarzania i ochrony danych osobowych.

Uzasadnienie oceny ogólnej

Szpital nie wywiązał się z obowiązku aktualizacji wewnętrznych regulacji dotyczących przetwarzania danych osobowych uwzględniających przepisy RODO[3]. Dyrektor Szpitala powołał Inspektora Ochrony Danych[4] i zapewnił mu wykonywanie obowiązków w sposób niezależny, jednak zawiadomienie Prezesa Urzędu Ochrony Danych Osobowych we właściwej formie o jego wyznaczeniu nastąpiło z opóźnieniem wynoszącym sto dziewięć dni, a powołanie wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo nastąpiło dwa dni po upływie ustawowego terminu. Podczas zdalnego zgłaszania usterek dotyczących programów informatycznych, pomimo wprowadzonych technicznych zabezpieczeń platformy CGM i podpisanej umowy powierzenia przetwarzania danych osobowych z serwisem oprogramowania, w 10% przypadków, pracownicy nie zachowali zasady minimalizacji danych, o której mowa w art. 5 ust. 1 lit. c) RODO. Obowiązkowym

[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.
[3] Rozporządzenie 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 (Dz. Urz. UE L 119 z 4 maja 2016 r., str. 1).
[4] Dalej: IOD.

szkoleniem z zakresu ochrony danych osobowych objęto jedynie 60,3% personelu. Ponadto na dwóch oddziałach stwierdzono niewłaściwy sposób przechowywania dokumentacji medycznej (w punkcie pielęgniarskim i w dwóch gabinetach lekarskich). W pozostałym zakresie ochrony danych osobowych Szpital podejmował prawidłowe działania. IOD opracował rejestr czynności przetwarzania danych, przeprowadził analizę przetwarzania danych osobowych w Szpitalu i ocenił stopień zapewnienia ich bezpieczeństwa w stosunku do stwierdzonych ryzyk. Przyjęte przez Szpital rozwiązania podczas rejestracji pacjentów, wizyt w gabinetach specjalistycznych oraz hospitalizacji (m.in. stosowanie opasek na rękę zapewniających anonimowość pacjentów oraz przechowywanie kart gorączkowych znajdujących się przy łóżkach w osłonkach przysłaniających dane pacjentów[5]), zapewniały ochronę danych osobowych i medycznych pacjentów. Właściwie udostępniano dokumentację medyczną pacjentów oraz zawierano wymagane umowy powierzenia przetwarzania danych osobowych. Szpitalna serwerownia była zabezpieczona przed fizycznym dostępem, a jej wyposażenie w nowoczesny sprzęt zapewniało tworzenie kopii zapasowych i ochronę wewnętrznej sieci ZOZ.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[6] kontrolowanej działalności

OBSZAR

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

Opis stanu faktycznego

1.1. Dyrektor Szpitala, realizując wymóg określony w art. 8 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[7], z dniem 7 czerwca 2018 r. powołał Inspektora Danych Osobowych. W związku z odejściem z dniem 26 maja 2018 r. na emeryturę pracownika sprawującego dotychczas funkcję Administratora Bezpieczeństwa Informacji (dalej: ABI), funkcję IOD pełnił nowo zatrudniony pracownik. Natomiast powiadomienie Prezesa Urzędu Ochrony Danych Osobowych[8] o wyznaczeniu IOD, zawierające wszystkie elementy określone w art. 10 ust. 3 u.o.d.o., nastąpiło we właściwej formie[9] dopiero w dniu 8 października 2018 r., tj. z opóźnieniem wynoszącym sto dziewięć dni, co zostało opisane w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości*.

IOD ukończył studia magisterskie na kierunku finanse i bankowość w zakresie usług finansowych oraz studia licencjackie na kierunku ekonomia pracy i zarządzanie kadrami. Po podjęciu pracy, w dniach 18-19 czerwca 2018 r., IOD został skierowany na dwudniowy certyfikowany kurs inspektora danych osobowych pn. „RODO w placówce medycznej[10]". Dyrektor Szpitala wyjaśnił, że osoba pełniąca funkcję IOD została zatrudniona *ze względu na znajomość przepisów i tematyki ochrony danych osobowych nabytej wcześniej we własnym zakresie oraz doświadczenie w pracy administracyjno–biurowej. Zatrudnienie firmy zewnętrznej nie gwarantowałoby*

[5] Oprócz jednego przypadku.

[6] 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.

[7] Dz. U. z 2018 r. poz. 1000. Dalej: u.o.d.o.

[8] Dalej: Prezes UODO.

[9] Zawiadomienia sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP (art. 10 ust. 6 u.o.d.o.). W dniu 22 czerwca 2018 r. ADO przesłał zawiadomienie o wyznaczeniu nowego IDO w formie pisemnej.

[10] Szkolenie obejmowało omówienie przepisów RODO w specyfice funkcjonowania placówek medycznych oraz warsztaty z samodzielnego przeprowadzenia audytu oraz analizy ryzyka, wytyczenie planu wdrożenia RODO oraz opracowanie odpowiedniej polityki i dokumentacji i było skierowane m.in. dla osób przygotowujących się do zajmowania funkcji IOD w placówce medycznej.

natychmiastowej reakcji na incydenty. Merytoryczny zakres przedmiotowego szkolenia pozwolił przypuszczać, że pracownik sprawujący funkcję IOD posiadł wiedzę na temat prawa i praktyk w dziedzinie ochrony danych oraz nabył umiejętności wypełnienia zadań, o których mowa w art. 39 RODO.
Zgodnie z art. 37 ust. 7 RODO, dane IOD oraz sposób i formę kontaktu opublikowano na stronie internetowej Szpitala[11].

IOD zagwarantowano wykonywanie obowiązków w sposób niezależny, stosownie do art. 38 ust. 3 i ust. 4 RODO, poprzez bezpośrednią podległość Dyrektorowi Szpitala, co wynikało z § 52 regulaminu organizacyjnego Szpitala z dnia 24 sierpnia 2018 r. W zakresie obowiązków IOD wskazano m.in. określanie sposobów i celów przetwarzania danych. Osoba pełniąca funkcję IOD odpowiadała w Szpitalu również za utrzymanie kontaktów z podmiotami krajowego systemu bezpieczeństwa[12].

(akta kontroli, tom I str. 6-14, 17, 19, 21, 465, 467, 478-479, tom II str. 1-2, 86, 96)

Szpital został uznany za operatora usługi kluczowej[13], o którym mowa w art. 5 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[14], o czym został poinformowany w dniu 27 listopada 2018 r. Z dniem 1 marca 2018 r. w Szpitalu powołano zespół do spraw cyberbezpieczeństwa, którego członkiem został IOD. Zespół został powołany z dwudniowym opóźnieniem, co zostało opisane w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli tom I str. 165, 167, 169-175, 466, 467, 472, 478)

1.2. W Szpitalu obowiązywały: [1] *Polityka Bezpieczeństwa Danych Osobowych w SP ZOZ* (dalej: PBDO); [2] *Instrukcja zarządzania systemem informatycznym w SP ZOZ* (dalej: IZSI); [3] *Regulamin sieci komputerowej i korzystania ze stacji roboczych.* Zostały one wprowadzone w życie 11 kwietnia 2016 r. zarządzeniem Dyrektora Szpitala nr 14/2016 z 8 kwietnia 2016 r. i do 12 kwietnia 2019 r. nie zostały zaktualizowane. Jako podstawę prawną opracowania PBDO i IZSI podano przepisy ustawy o ochronie danych osobowych obowiązującej do dnia 25 maja 2018 r.[15] oraz rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. *w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych*[16], które przestało obowiązywać z dniem 25 maja 2019 r. Jednym z elementów Systemu Zarządzania Jakością (dalej: SZJ) w Szpitalu było stosowanie *Procedury udostępniania dokumentacji medycznej w SP ZOZ*, obowiązującej od dnia 24 stycznia 2018 r. Opisano w niej, w jaki sposób należy udostępniać dokumentację medyczną pacjentom oraz uprawnionym organom, a także zamieszczono wzory wniosku o udostępnienie oraz pokwitowanie wydania i upoważnienia pacjenta do wydania dokumentacji medycznej. W wymienionej powyżej dokumentacji nie zawarto uregulowań wynikających z wejścia w życie RODO oraz przepisów krajowych dotyczących ochrony danych osobowych, obowiązujących po 25 maja 2018 r. Szpital nie aktualizując PBDO oraz IZSI, powołał się na reorganizację oraz zmianę systemów i sprzętu IT. Zostało to szerzej opisane w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości*.

IOD opracował projekt *Polityki Ochrony Danych Osobowych (dalej: Projekt),* który do zakończenia kontroli nie został w Szpitalu wdrożony. W Projekcie IOD nie wskazał

---

[11] W dniu 13 lipca 2018 r.
[12] Zmiana warunków pracy IOD z dniem 5 grudnia 2018 r., podział czasu pracy na obie funkcje po ½ etatu.
[13] Pismo znak FZP.426.33.2018 z dnia 22 listopada 2018 r.
[14] Dz. U. poz. 1560. Dalej: ustawa o cyberbezpieczeństwie.
[15] Tj. ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 ze zm.), której część przepisów zostało uchylonych z dniem oraz (dalej: rozporządzenie w sprawie przetwarzania danych)
[16] Dz. U. z 2004 r., Nr 100, poz. 1024.

aktów prawnych, na podstawie których opracował ten dokument, zaznaczył jednak, iż stanowi ona zestaw wymogów, zasad i regulacji ochrony danych osobowych powołanych w celu zapewnienia oraz wykazania przetwarzania tych danych zgodnie z RODO. Załączniki do Projektu stanowiły: [1] wzory rejestrów: a) czynności przetwarzania danych osobowych, b) incydentów, c) naruszeń, d) upoważnień do przetwarzania danych osobowych, e) podmiotów, z którymi Szpital zawarł umowy powierzenia, f) przeszkolonych pracowników, [2] procedura zawiadamiania osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, [3] wzory: a) arkusza oceny ryzyka, b) oceny skutków, c) oświadczenia pracownika o zapoznaniu się z przepisami, d) upoważnienia pracownika do przetwarzania danych osobowych oraz e) wniosku o utworzenie konta w systemie informatycznym. W Projekcie wskazano obowiązki dokumentowania procesów, o których mowa w art. 32 i 33 RODO, nałożonych na ADO, nie określając sposobu realizacji tych procesów w ZOZ oraz ich dokumentowania. Projekt nie został udostępniony na wewnętrznej stronie internetowej Szpitala, natomiast zamieszczono tam m.in. prezentację PowerPoint przygotowaną i wykorzystywaną przez IOD przy prowadzeniu szkoleń w zakresie przepisów RODO oraz *Przewodnik po RODO w służbie zdrowia* opracowany przez Ministerstwo Cyfryzacji. PBDO nie przewidywała konieczności opracowania dodatkowych reguł i procedur uszczegóławiających ww. dokumenty. Dokumentacja została udostępniona na stronie intranetowej Szpitala.

(akta kontroli tom I str. 23-25, 72, 115, 124, 134, 167-168, 479, tom II str. 3-33)

1.3. Zgodnie z art. 30 ust. 1 RODO, w Szpitalu prowadzono rejestr czynności przetwarzania danych osobowych. Rejestr został opracowany w dniu 24 lipca 2018 r.[17] w wersji elektronicznej (Excel), na wzorze stanowiącym załącznik do Projektu i do dnia 12 kwietnia 2019 r. nie był aktualizowany. Liczył on 32 pozycje, zawierające wszystkie dane wymagane art. 30 ust. 1 RODO. Obowiązek opracowania rejestru istniał od 25 maja 2018 r., co opisano w dalszej części wystąpienia w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli tom I str. 181-201, 480, tom II str. 86, 96)

1.4. Stosownie do art. 32 RODO, na dzień 29 czerwca 2018 r. IOD przeprowadził ocenę ryzyka procesów przetwarzania danych osobowych pracowników oraz pacjentów Szpitala w ośmiu[18] komórkach organizacyjnych Szpitala, określając 15 ryzyk[19] mogących skutkować naruszeniem praw lub wolności osób, których te dane dotyczą. Dla każdego z ryzyk IOD ocenił poziom wystąpienia incydentu (w skali od zera do dwudziestu punktów), określony jako iloczyn prawdopodobieństwa wystąpienia ryzyka (w skali od zera do czterech punktów) i jego skutków (w skali od zera do pięciu punktów). W ocenie IOD największe ryzyka związane z przypadkowym udostępnieniem danych mogących przełożyć się na naruszenie dobrego imienia, dyskryminację czy stratę finansową pacjenta mogły zaistnieć podczas rejestracji i udzielania świadczeń lekarskich na SOR, w Centrum Zdrowia Psychicznego (dalej: CZP) oraz w oddziałach szpitalnych, a także podczas obsługi pracowników w księgowości i w kadrach. W celu zminimalizowania tych ryzyk, IOD zalecił m.in. wykonanie przegrodzeń pomiędzy stanowiskami w rejestracji ogólnej[20], zmianę lokalizacji rejestracji na SOR[21], uwrażliwienie pracowników CZP

[17] Data ostatniej modyfikacji pliku. IOD wyjaśnił, że rozpoczął pracę nad dokumentem 28 czerwca 2018 r.

[18] [1] kadry – w zakresie rekrutacji i obsługi pracowników, [2] rejestracja ogólna, [3] rejestracja i udzielenie świadczeń lekarskich na SOR, [4] przychodnie specjalistyczne (bez psychiatrii), [5] poradnia psychiatryczna, [6] księgowość, płace, [7] Dział Techniczny, [8] oddziały szpitalne.

[19] [1] dyskryminacja, [2] kradzież tożsamości, [3] oszustwo dotyczące tożsamości, [4] strata finansowa, [5] naruszenie dobrego imienia, [6] naruszenie poufności danych osobowych chronionych tajemnicą zawodową, przypadkowe lub niezgodne z prawem: [7] zniszczenie danych, [8] utrata danych, [9] zmodyfikowania danych, [10] nieuprawnione ujawnienie danych, [11] nieuprawniony dostęp do danych, [12] złamanie poufności, [13] złamanie dostępności, [14] złamanie integralności oraz [15] złamanie odporności.

[20] Wykonano w dniu 13 lipca 2018 r.

na konieczność zachowania dyskrecji oraz tajemnicy w przypadku powzięcia informacji chronionych podczas wykonywania obowiązków służbowych oraz zachowanie szczególnej ostrożności na oddziałach szpitala przy przetwarzaniu danych dotyczących stanu zdrowia pacjentów, mogących się przyczynić do ich dyskryminacji w miejscu pracy lub utraty zatrudnienia.

(akta kontroli tom I str. 235-242)

1.5. W Szpitalu nie została wykonana ocena skutków dla ochrony danych, o której mowa w art. 35 RODO, ponieważ nie rozpoczęto przetwarzania nowych kategorii danych osobowych, w szczególności z użyciem nowych narzędzi, a ZOZ nie wprowadził nowych rodzajów usług medycznych, które nie byłyby wykonywane wcześniej. Pojedyncza (bieżąca) ocena operacji wiążących się z wysokim ryzykiem jest fakultatywna, przy czym Grupa Robocza ds. Ochrony Danych[22] zalecała dokonanie oceny skutków dla ochrony danych dla operacji przetwarzania już trwających przed 25 maja 2018 r.[23] oraz w przypadkach, gdy nie jest jasne, czy taka ocena jest wymagana, ponieważ jest ona *przydatnym narzędziem, które może pomóc administratorom danych w zapewnieniu zgodności z prawem ochrony danych*. Dyrektor Szpitala wyjaśnił, że *ocena skutków dla ochrony danych osobowych jest integralną częścią analizy ryzyka i zostanie przeprowadzona przed zakończeniem projektu „Rozwój E-usług poprzez wdrożenie kompleksowego rozwiązania teleinformatycznego i aplikacyjnego[24]".*

(akta kontroli tom I str.166, 168, 471, 478)

1.6. Jednym z zadań IOD, w myśl art. 39 ust. 1 lit. b RODO, jest prowadzenie szkoleń personelu uczestniczącego w operacjach przetwarzania danych. Po wejściu w życie przepisów RODO, do dnia 20 lutego 2019 r., jedynie 255 z 486 (52%) pracowników Szpitala zostało objętych szkoleniem z zakresu ochrony danych osobowych, w formie warsztatów przeprowadzonych przez IOD, co opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości*. Szkolenia te obejmowały m.in. ogólną charakterystykę aktów prawnych w zakresie ochrony danych osobowych, omówienie obowiązku informacyjnego, zasady udostępniana i powierzana danych osobowych, omówienie praktyk związanych z ochroną danych osobowych[25].

(akta kontroli tom I str. 166, 168, 202-207, 248-257, tom II str. 3-33)

Zgody na przetwarzanie danych osobowych, które zostały wydane pracownikom przeszkolonym z przepisów RODO, nie wskazywały podstawy prawnej, na jakiej zostały wydane, ani daty od kiedy i do kiedy obowiązywały. W upoważnieniach zawarto natomiast oświadczenie *o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych, w szczególności z RODO oraz z wydaną na jego podstawie przez ADO Polityką Ochrony Danych Osobowych,* która do dnia 12 kwietnia 2019 r. nie została ukończona, zatwierdzona i wdrożona, co opisano w dalszej części wystąpienia w sekcji *Stwierdzone nieprawidłowości*. Pracownicy, którzy nie zostali jeszcze przeszkoleni z przepisów RODO, posiadali upoważnienia do przetwarzania danych osobowych wydawane na podstawie art. 37 ustawy

[21] Wykonano w dniu 10 stycznia 2019 r.

[22] 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.

[23] Wytyczne dotyczące oceny skutków dla ochrony danych (https://www.giodo.gov.pl/1520281/id_art/9957/j/pl – dostęp z 18 marca 2019 r.).

[24] Realizowanego na podstawie umowy nr 9/2018/PN z dnia 25 października 2018 r. wprowadzającą m.in. usługę Activ Directory.

[25] Reguła czystego biurka, reguła czystego ekranu, zasada tworzenia bezpiecznego hasła, praca w internecie, zaznajomienie pracowników z instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych.

o ochronie danych osobowych z 29 sierpnia 1997 r. uchylonej z dniem 25 maja 2018 r., co opisano w dalszej części wystąpienia w sekcji *Stwierdzone nieprawidłowości*.

W związku z brakiem ewidencji pracowników upoważnionych do przetwarzania danych osobowych, ustalenie dokładnej liczy osób, którym wydano upoważnienia do przetwarzania danych osobowych, nie było możliwe. W toku kontroli IOD przedstawił listę 72 wydanych upoważnień personelowi kierowniczemu (kierownicy i zastępcy komórek organizacyjnych szpitala). Do 6 lutego 2019 r. obowiązek prowadzenia ewidencji wynikał z art. 39 ust. 1 ustawy o ochronie danych osobowych z 29 sierpnia 1997 r. oraz obowiązującej w Szpitalu Polityki bezpieczeństwa danych osobowych[26], co opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli tom I str. 502-513)

1.7. W Szpitalu nie stosowano kodeksu dobrych praktyk ani medycznego kodeksu branżowego. Natomiast obowiązywał kodeks etyki, wprowadzony zarządzeniem Dyrektora Szpitala z dnia 7 listopada 2011 r., który odnosił się m.in. do świadczenia usług medycznych. Ponadto, na wewnętrznej stronie internetowej Szpitala został opublikowany *Przewodnik po RODO dla służby zdrowia*, z którym personel mógł się zapoznać.

(akta kontroli tom I str. 165, 167, 176-179)

Stwierdzone nieprawidłowości

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

1. O wyznaczeniu IDO w dniu 7 czerwca 2018 r. Dyrektor Szpitala zawiadomił Prezesa Urzędu Ochrony Danych Osobowych dopiero w dniu 8 października 2018 r. tj. 109 dni po terminie wskazanym w art. 10 ust. 1 u.o.d.o., zgodnie z którym termin na dokonanie zawiadomienia wynosi 14 dni od dnia wyznaczenia IOD. Zgodnie z art. 10 ust. 6 u.o.d.o. zawiadomienie powinno być sporządzone w postaci elektronicznej i opatrzone kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.

   Dyrektor wyjaśnił, że *zawiadomienie zostało przesłane w dniu 22 czerwca 2018 r. w nieodpowiedniej, pisemnej formie.*

   (akta kontroli tom I str. 6, 174-175, 243-246, 465, 472, 478, 482-483)

2. W Szpitalu nie wprowadzono Polityki Bezpieczeństwa Informacji, o której mowa w § 2 pkt 15 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*[27], spełniającej wymogi § 20 ust. 1 tego rozporządzenia. W Szpitalu funkcjonowały PBDO, IZSI oraz regulamin sieci komputerowej i korzystania ze stacji roboczych, ale nie obejmowały one kompleksowo zagadnień związanych z zarządzaniem bezpieczeństwem informacji.

   Dyrektor wyjaśnił, że *ze względu na wielkość rozwiązań jakie stwarza dla ochrony danych osobowych modernizacja infrastruktury informatycznej, niemożliwe jest wprowadzenie jednej zasady właściwej dla różnych rozwiązań technicznych. Wprowadzenie regulacji wewnętrznych odnośnie użytkowania części sprzętu, byłoby działaniem pozornym. Osoby, które dysponują i obsługują*

[26] Załącznik nr 2 do PBDO.
[27] Dz. U. z 2017 r. poz. 2247. Rozporządzenie zwane dalej: rozporządzeniem KRI.

się nowym systemem informatycznym zostały przeszkolone w zakresie obsługi jak i bezpieczeństwa ochrony danych osobowych podczas szkoleń stanowiskowych.

(akta kontroli tom I str. 166, 168, 466, 475)

3. Do dnia 12 kwietnia 2019 r. nie zaktualizowano obowiązujących w Szpitalu regulacji wewnętrznych dotyczących ochrony danych osobowych, w celu dostosowania ich do przepisów RODO i ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. W Szpitalu obowiązywały PBDO i IZSI, które nie uwzględniały części wymogów przewidzianych w RODO oraz w przepisach krajowych obowiązujących od 25 maja 2018 r., w tym m.in. dotyczących powołania IOD w miejsce Administratora Bezpieczeństwa Informacji, prawa do sprostowania danych (art. 16 RODO), prawa do usunięcia danych (art. 17 RODO), prawa do ograniczenia przetwarzania (art. 18 RODO), obowiązku powiadamiania o sprostowaniu lub usunięciu danych osobowych, lub o ograniczeniu przetwarzania (art. 19 RODO), uwzględnianiu ochrony danych osobowych w fazie projektowania, domyślna ochrona danych (art. 25 RODO), rejestrowaniu czynności przetwarzania (art. 30 RODO), obowiązku zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu (art. 33 RODO), prowadzeniu oceny skutków dla ochrony danych osobowych (art. 35 RODO), statusu IOD w strukturach Szpitala (art. 38 RODO), co stanowiło naruszenie przepisu art. 24 ust. 1 i 2 RODO, zgodnie z którym do obowiązków administratora danych osobowych należy m.in. poddawanie w razie potrzeby przeglądom i aktualizacja przyjętych polityk ochrony danych i regulacji wewnętrznych w tym zakresie.

   Dyrektor Szpitala wyjaśnił, że: *ww. regulacje wewnętrzne nie zostały zaktualizowane w związku planowaną w 2018 r. modernizacją systemów informatycznych. Dopiero po zakończeniu projektu i konfiguracji wszystkich urządzeń będziemy w stanie określić jak będą zachodziły wszystkie procesy informatyczne w Szpitalu. Wdrożeniem odpowiednich polityk ochrony danych jest prowadzenie RCPD, rejestru umów powierzenia oraz naruszeń i incydentów oraz przeprowadzenie analizy ryzyka. Zasady przetwarzania i ochrony danych osobowych reguluje PBDO wprowadzona w dniu 11 kwietnia 2016 r. O wszystkich zmianach jakie zostały wprowadzone z momentem wejścia w życie nowej ustawy, a które mają znaczący wpływ na przetwarzanie oraz odpowiedzialność osób przetwarzających, pracownicy zostali powiadomieni za pomocą szkoleń umieszczonych na wewnętrznej stronie szpitala jak i podczas szkoleń stanowiskowych przeprowadzanych podczas modernizacji infrastruktury informatycznej.*

   (akta kontroli tom I str. 25, 72, 134, 165, 167-168, 471, 476)

4. Rejestr czynności przetwarzania danych osobowych, o którym mowa w art. 30 RODO, został opracowany z naruszeniem wymaganego terminu, tj. po 25 maja 2018 r. Powstał w wersji elektronicznej, a dzień ostatniej modyfikacji pliku nastąpił 24 lipca 2018 r.

   Dyrektor Szpitala wyjaśnił, że *odroczenie utworzenia rejestru czynności przetwarzania danych osobowych było związane z poszukiwaniem pracownika na stanowisko IOD. Niezwłocznie od chwili powzięcia informacji o zamiarze przejścia na emeryturę ABI (połowa kwietnia 2018 r.) rozpoczął poszukiwania osoby na stanowisko IOD na lokalnym rynku pracy oraz poprzez rozeznanie wśród dyrektorów innych podmiotów leczniczych. Z dniem 7 czerwca 2018 r. został zatrudniony pracownik na stanowisku IOD. W okresie od 25 maja 2018 r.*

do 20 czerwca 2018 r. czynności związane z ochroną danych osobowych były podejmowane przez ADO.

(akta kontroli tom I str. 166, 168, 181-201, 461-462, 472, 480, tom II str. 86, 96)

5. Dyrektor Szpitala wyznaczył zespół ds. cyberbezpieczeństwa, o którym mowa w art. 14 ustawy o cyberbezpieczeństwie z dwudniowym opóźnieniem w stosunku do wymogu ustawy. Szpital otrzymał decyzję w sprawie uznania go za operatora usługi kluczowej w dniu 27 listopada 2018 r. Zgodnie z art. 16 pkt 1 ustawy powołanie zespołu powinno nastąpić w terminie trzech miesięcy od daty otrzymania decyzji o uznaniu go za operatora usługi kluczowej, tj. do dnia 27 lutego 2019 r. Zarządzenie dyrektora o powołaniu zespołu zostało wydane w dniu 1 marca 2019 r.

   Dyrektor wyjaśnił, że *w dniu 27 listopada 2018 r. był nieobecny w pracy, i że jest to niedopatrzenie IOD.*

   (akta kontroli tom I str. 165, 167, 169-173, 472, 478)

6. Inspektor ochrony danych nie wywiązał się w pełni z wynikającego z art. 39 ust. 1 lit. b RODO obowiązku prowadzenia szkoleń dla personelu uczestniczącego w operacjach przetwarzania danych. Po wejściu w życie przepisów RODO, do dnia 12 kwietnia 2019 r. przeszkolonych zostało jedynie 293 z 486 pracowników Szpitala (tj. 60,3%). Obowiązek zapewnienia szkoleń osobom zaangażowanym w proces przetwarzania informacji, z uwzględnieniem zagrożenia jej bezpieczeństwa, skutków naruszenia zasad bezpieczeństwa, konsekwencji prawnych i środków zapewniających jej bezpieczeństwo wynika również z § 20 ust. 2 pkt 6 rozporządzenia KRI.

   Dyrektor Szpitala wyjaśnił, że *wszyscy pracownicy SP ZOZ są przeszkoleni w zakresie ochrony danych osobowych jeszcze przez ABI. W chwili wejścia w życie RODO ustalono, że ponownemu szkoleniu będzie podległ cały personel Szpitala. Ze względu na charakter pracy nie było możliwości sprawnego przeszkolenia wszystkich pracowników jednocześnie lub w dużych grupach. Szkolenia prowadzone były sukcesywnie, w miarę możliwości, na wszystkich oddziałach. Szkolenia musiały być przeprowadzane wśród poszczególnych grup, przy uwzględnieniu charakteru, rodzaju oraz ryzyka jakie wiąże się z przetwarzaniem – inne jest na oddziale dziecięcym, a inne na oddziale neurologii. Ponadto wszyscy pracownicy Szpitala mają możliwość zapoznania się z PBDO, jak i zasadami przetwarzania danych osobowych za pomocą wewnętrznej strony internetowej, na której zostało udostępnione również szkolenie dla pracowników, z którymi wszyscy są zobowiązani się zapoznać.*

   (akta kontroli tom I str. 5, 166, 168, 202-207, 461-464, 466-468)

7. Szpital nie dysponował ewidencją osób upoważnionych do przetwarzania danych osobowych, w związku z czym nie było możliwe określenie dokładnej liczby wydanych upoważnień w tym zakresie. Obowiązek prowadzenia takiej ewidencji do dnia 25 maja 2018 r. wynikał z art. 39 ust. 1 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r., wynikał również z regulacji wewnętrznych Szpitala (tj. z załącznika nr 2 do PBDO).

   Dyrektor wyjaśnił, że *w dokumentach zgromadzonych przez ABI znajdują się upoważnienia do przetwarzania danych w oryginale, natomiast nie jest w stanie odnaleźć ewidencji i nie posiada wiedzy czy była prowadzona. Upoważnienia wydawane na podstawie art. 37 ustawy o ochronie danych osobowych z 1997 r. były udzielane do 10 października 2018 r. IOD posiada ewidencję upoważnień wydanych kierownikom jednostek organizacyjnych Szpitala do przetwarzania i udzielania upoważnień podległym pracownikom. W zmodernizowanym systemie informatycznym ewidencja osób upoważnionych do przetwarzania danych*

osobowych będzie prowadzona w formie elektronicznej w programie kadrowym, w celu zapewnienia pełnej rozliczalności.

(akta kontroli tom I str. 477, 486-489)

8. Pracownicy Szpitala, którzy nie zostali przeszkoleni z RODO, posiadali upoważnienia do przetwarzania danych osobowych wydawane na podstawie nieobowiązującego art. 37 ustawy o ochronie danych osobowych z 1997 r., uchylonej z dniem 25 maja 2018 r. Natomiast w upoważnieniach do przetwarzania danych osobowych wydanych po 10 października 2018 r. zawarto oświadczenia o zapoznaniu się pracowników z Polityką Ochrony Danych Osobowych, która do dnia 12 kwietnia 2019 r. nie została, zatwierdzona i wdrożona.

   Dyrektor wyjaśnił, że *kwestia wydania nowych upoważnień została przeoczona. Szpital jest w trakcie aktualizacji wszystkich dokumentów związanych z RODO*, natomiast odnośnie do oświadczeń o zapoznaniu się z nieobowiązująca jeszcze PODO, Dyrektor wyjaśnił, że *było to niedopatrzenie IOD, które zostanie usunięte wraz z wydaniem nowych upoważnień personelowi przetwarzającemu dane osobowe.*

   (akta kontroli tom I str. 471, 477)

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli ocenia negatywnie przygotowanie Szpitala do obowiązujących od maja 2018 r. rozwiązań w zakresie ochrony danych osobowych. Placówka nie wywiązała się z obowiązku opracowania dokumentacji oraz procedur wewnętrznych uwzględniających przepisy RODO. Szkoleniami z zakresu ochrony danych osobowych objęto jedynie 60,3% personelu. Umożliwiono IOD wykonywanie obowiązków w sposób niezależny poprzez bezpośrednią podległość Dyrektorowi Szpitala, jednak informacja o jego powołaniu została przekazana do Prezesa Urzędu Ochrony Danych osobowych z opóźnieniem wynoszącym sto dziewięć dni, a powołanie wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo nastąpiło z dwudniowym opóźnieniem. IOD wywiązał się z obowiązku prowadzenia rejestru czynności przetwarzania danych osobowych oraz przeprowadził analizę przetwarzania danych osobowych w Szpitalu i właściwie ocenił stopień zapewnienia ich bezpieczeństwa w stosunku do stwierdzonych ryzyk. Mimo braku przeszkolenia całej kadry, niezbędne informacje dotyczące zmian w obowiązujących przepisach, udostępniono na stronie intranetowej Szpitala z jednoczesnym poleceniem przez Dyrektora zapoznania się z nimi przez pracowników.

OBSZAR

2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych

Opis stanu faktycznego

2.1. Na podstawie przeprowadzonych oględzin trzech rejestracji[28] Szpitala stwierdzono, że w celu właściwej ochrony danych osobowych funkcjonowały poniżej wymienione rozwiązania:

- przed każdym okienkiem rejestracji była wyznaczona linia, oddzielająca osoby oczekujące w kolejce od osoby rejestrującej się, w odległości ok. 2 m od okienka,
- trzy okienka rejestracji ogólnej usytuowane w jednej linii były od siebie oddzielone przegrodami z pleksi,
- w obrębie wzroku pacjentów rejestrujących się nie znajdowały się dane osobowe innych pacjentów (przygotowane karty pacjentów były układane niezapisaną stroną do góry lub były odkładane poza obręb stanowiska),

[28] Rejestracja ogólna, rejestracja poradni pediatrycznej oraz rejestracja poradni psychiatrycznej.

- na szybie każdego z okienek rejestracji znajdowała się informacja, że przy okienku może przebywać tylko jedna osoba oraz, że podczas rejestracji należy okazać dokument tożsamości (dowód osobisty, paszport lub dowód osobisty, paszport, prawo jazdy, albo książeczkę zdrowia dziecka lub legitymację szkolną dla osób, które nie ukończyły 18 roku życia)[29],
- w każdej z rejestracji znajdowała się informacja[30] o przetwarzaniu danych, na której wskazano m.in. administratora, dane IOD, cele i podstawy przetwarzania danych, ich kategorie, odbiorców, okres przechowywania danych oraz prawo do dostępu, sprostowania, przenoszenia, wnoszenia skargi,
- rejestracja pacjentów odbywała się na podstawie skierowań do poradni specjalistycznych oraz dowodu osobistego,
- w przypadku rejestracji bezpośrednio przed wizytą pacjenci kierowani byli przez rejestratorkę pod gabinet, gdzie sami pilnowali kolejności wejścia (kolejność pokrywała się z kolejnością rejestracji),
- podczas rejestracji na termin odległy, pacjent otrzymywał karteczkę z nazwiskiem lekarza, datą i planowaną godziną przyjęcia oraz numerem gabinetu oraz nazwą poradni,
- rejestracja pacjentów w poradni pediatrycznej odbywała się najczęściej telefonicznie: pacjent proszony był o podanie imienia, nazwiska i roku urodzenia, a przy rejestracji osobistej opiekun dziecka proszony był o zapisanie ww. danych na karteczce, która po zarejestrowaniu pacjenta była niszczona,
- karty pacjentów w rejestracjach przechowywane były w metalowych szafkach z szufladami zamykanymi na klucz, ponadto w rejestracji ogólnej karty przechowywano w otwartych regałach przesuwnych, natomiast wejście do rejestracji nie było możliwe z zewnątrz pomieszczenia (w drzwiach zamontowana była nieruchoma gałka zamiast klamki).

W trakcie oględzin zaobserwowano trzy przypadki przekroczenia linii oddzielającej przez pacjentów aktualnie nieobsługiwanych. W każdym przypadku rejestratorka zwróciła interesantowi uwagę i prosiła o oddalenie się od okienka za wyznaczoną linię.

(akta kontroli tom I str. 296-301, 310-320)

We wszystkich trzech objętych oględzinami gabinetach poradni specjalistycznych Szpitala[31] karty pacjentów były ułożone w stosach danymi osobowymi w stronę biurka, co uniemożliwiało odczyt tych danych przez pacjentów odbywających wizytę. W dwóch gabinetach lekarzowi przyjmującemu asystowały pielęgniarki. Nie stwierdzono przypadku pozostawienia gabinetu lekarskiego bez nadzoru. Wywoływanie pacjentów wszystkich trzech poradni odbywało się w sposób zapewniający anonimowość, według kolejności przyjścia lub zanonimizowanej listy[32] wywieszonej na drzwiach gabinetu, zawierającej początkowe litery nazwiska, imienia oraz przewidywaną godzinę wizyty. W przypadku konieczności wezwania pacjenta posługiwano się słowami: *następny proszę*.

(akta kontroli tom I str. 298, 302-304, 306)

Oględziny dyżurek pielęgniarskich, sal chorych oraz gabinetów lekarskich na trzech oddziałach szpitalnych[33] wykazały m.in., że:

- na oddziałach znajdowały się 36 sale chorych, dysponujące 95 łóżkami,

[29] Dotyczyło poradni pediatrycznej.
[30] W rejestracji ogólnej na tablicy informacyjnej, w pozostałych rejestracjach na szybie okienka.
[31] Oględzinami objęto trzy poradnię okulistyczną, endokrynologiczną oraz chirurgii ogólnej.
[32] W poradni chirurgii ogólnej.
[33] Oględziny przeprowadzono na Oddziale Chorób Wewnętrznych i Kardiologii z pododdziałem Pulmonologii (dalej Oddział Wewnętrzny), Oddziale Urazowo Ortopedycznym i Oddziale Chirurgii.

- 76 z 78 zaobserwowanych pacjentów miało na nadgarstku odręcznie wypisane opaski ze skróconą nazwą oddziału oraz numerem identyfikacyjnym pacjenta (dalej: numer ID)[34]: jedna opaska została przypadkowo zerwana przez pacjentkę i przed zakończeniem oględzin ponownie założona, brak drugiej opaski dotyczył pacjenta czekającego na wypis ze Szpitala,
- na jednym oddziale[35] nie umieszczano kart chorych przy łóżkach pacjentów, a na dwóch pozostałych karty te były umieszczone w sposób uniemożliwiający odczytanie przez osoby postronne danych na nich zapisanych (były umieszczone w osłonkach),
- na Oddziale Chirurgii stwierdzono jeden przypadek pozostawienia karty przy łóżku pacjenta bez osłonki, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości*,
- ruch chorych[36] prowadzony był w pomieszczeniach, w których nie przebywali pacjenci (tablice były zlokalizowane za drzwiami, we wnęce, na filarze usytuowanym równolegle do płaszczyzny drzwi wejściowych),
- na dwóch oddziałach[37], podręczna dokumentacja pielęgniarska przechowywana była w zamykanych na klucz szafkach, w zamykanych na klucz pokojach socjalnych usytuowanych za dyżurką pielęgniarską (wydzieloną we wnęce korytarza),
- na jednym oddziale dokumentację pielęgniarską przechowywano w otwartej szafce z przegródkami, w punkcie pielęgniarskim usytuowanym we wnęce korytarza, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości*,
- dyżurki pielęgniarskie były wyposażone w pięć komputerów, z których dwa były uruchomione i pracowały na nich pielęgniarki, w trakcie oględzin jedna z pielęgniarek opuściła stanowisk, ale dostęp do systemu operacyjnego na tym urządzeniu został przez nią zablokowany,
- na oddziałach znajdowały się cztery gabinety lekarskie, z czego jeden był zamknięty, trzy poddane oględzinom gabinety wyposażone były w 13 komputerów, z których siedem było uruchomionych – lekarze pracowali na sześciu z nich, a użytkownik jednego komputera był wylogowany,
- dokumentacja medyczna pacjentów w jednym gabinecie lekarskim była przechowywana w szafie aktowej zamykanej na klucz, a w dwóch[38] gromadzono ją na otwartych półkach z przegródkami, nieposiadającymi możliwości zamknięcia, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości*,

Szpital nie został wyposażony w specjalistyczne drukarki i skanery służące do tworzenia i odczytu danych na opaskach. W dokumentacji pielęgniarskiej i medycznej, obok danych osobowych pacjentów znajdował się ich numer ID. Na oddziałach, na których karty pacjenta znajdowały się w osłonkach zakrywających dane medyczne i osobowe, przy łóżkach, pacjenci wyrażali pisemnie na to zgodę (w uwagach historii choroby). Jeżeli pacjent nie wyraził pisemnej zgody, jego karta nie była przechowywana przy łóżku. W trakcie przeprowadzonych oględzin nie stwierdzono przypadku pozostawienia punktów pielęgniarskich[39], gabinetów lekarskich i pomieszczeń, w których wywieszony był ruch chorych, bez nadzoru.

---

[34] Numer nadawany w systemie informatycznym w momencie rejestracji pacjenta na SOR.
[35] Oddział Wewnętrzny.
[36] Ruch chorych to lista pacjentów danego oddziału wraz z numerem sali, w których przebywają pacjenci.
[37] Oddział Wewnętrzny i Oddział Chirurgii.
[38] Oddział Wewnętrzny i Oddział Urazowo Ortopedyczny.
[39] Dotyczy Oddziału Urazowo Ortopedycznego, na Oddziale Wewnętrznym i Chirurgii w punktach pielęgniarskich nie przechowywano dokumentów zawierających dane osobowe, a stacje robocze pozostawały wyłączone lub wylogowane.

(akta kontroli tom I str. 276-295)

Szpital był objęty monitoringiem wizyjnym, na który składały się z trzy[40] rejestratory obsługujące łącznie 24 kamery. W dniu 21 marca 2019 r., podczas oględzin NIK, na komputerze Administratora Systemu Informatycznego (dalej: ASI) odczytano obraz z dziewięciu kamer zainstalowanych w Centrum Zdrowia Psychicznego, natomiast na komputerze Zastępcy Kierownika Działu Metodyczno – Organizacyjnego - osiem kamer obejmujących SOR, wejście do wind na parterze budynku głównego, pracownię tomografii komputerowej oraz korytarz przed pracownią fizjoterapii. Jeden z rejestratorów, który obsługiwał trzy[41] kamery zewnętrzne oraz cztery[42] wewnętrzne był zepsuty. Informacje na temat celu zainstalowania i zasad funkcjonowania monitoringu wizyjnego w Szpitalu, w tym wykorzystania oraz udostępniania nagrań organom w wyniku prowadzonego przez nie postępowania, zostały zamieszczone IZSI[43].

(akta kontroli tom I str. 307-309)

2.2. Personel działów administracyjnych[44] Szpitala, według stanu na dzień 22 marca 2019 r., liczył 26 osób[45]. Analiza uprawnień tych osób wykazała, że nie posiadały one dostępu do danych medycznych w systemach informatycznych, ani upoważnień do przetwarzania danych osobowych w tych systemach. Wśród 15 pracowników średniego personelu niemedycznego, 11 osób[46] z Działu Statystyki Medycznej oraz trzech informatyków posiadało zarówno upoważniania do przetwarzania danych osobowych, jak aktywne konta w systemie HIS, co odpowiadało realizowanym przez nich obowiązkom Jeden z informatyków nie posiadał ani upoważnienia, ani konta z dostępem do systemu.

(akta kontroli tom I str. 395-397, 501, tom II str. 77-79, 84-85)

2.3. Na próbie upoważnień do sytemu informatycznego do obsługi danych medycznych HIS wydanych dla 30 (z 210) pielęgniarek i położnych zatrudnionych w Szpitalu stwierdzono, że 28 z nich posiadało dostęp w systemie HIS wyłącznie do pacjentów z oddziału, na którym wykonywały przydzielone obowiązki służbowe, natomiast dwie pielęgniarki pracujące w Szpitalnym Oddziale Ratunkowym, ze względu na charakter pracy[47], posiadały dostęp w tym systemie do pacjentów ze wszystkich oddziałów Szpitala. Dyrektor wyjaśnił, że *przyjęcia do Szpitala odbywają się przez SOR*, *dlatego w takim przypadku, by przyjąć pacjenta na oddział należy mieć do niego uprawnienia.* W Szpitalu nie było osób zatrudnionych na stanowisku salowych. Wszystkie pielęgniarki i położne miały upoważnienia do przetwarzania danych osobowych.

Pracownicy personelu niższego Szpitala, do których zaliczały się osoby sprzątające z oddziałów szpitalnych (50 osób) oraz SOR (pięć osób), do obowiązków których należał m.in. transport pacjentów na badania i na oddziały szpitalne, nie posiadali założonych kont w systemie HIS i nie zostali upoważnieni do przetwarzania danych

[40] Na rejestracji SOR, w pokoju pielęgniarek Oddziału Psychiatrycznego, w rejestracji ogólnej.
[41] Wejście główne do budynku oraz wejście do Podstawowej Opieki Zdrowotnej (dalej: POZ) i Pomocy Nocnej i Świątecznej.
[42] W holu głównym, w poczekalni POZ oraz pracowni RTG.
[43] W pkt 17 IZSI. Pracownicy podpisali na upoważnieniach wydanych na podstawie przepisu art. 37 u.o.d.o. z 1997 r. oświadczenia o zapoznaniu się z PBOD i IZSI.
[44] Z wyłączeniem Dyrektora Szpitala, Zastępcy Dyrektora Szpitala, ASI, Zastępcy Kierownika Działu Metodyczno – Odganizacyjnego.
[45] W Dziale Finansowo-Ekonomicznym – 10; Dziale Techniczno-Eksploatacyjnym – 5; Sekcji Zamówień Publicznych – 2; Dziale Zatrudnienia – 2; Dziale Logistyki i Higieny Oddziałów – 1; na stanowiskach samodzielnych – 6;
[46] Z wyjątkiem jednej osoby, która przebywała na urlopie bezpłatnym od dnia 1 stycznia 2019 r. i posiadała nieaktywne konto w systemie HIS.
[47] Pielęgniarki pracujące na Szpitalnym Oddziale Ratunkowym.

osobowych[48]. IOD wyjaśnił, że *cały personel sprzątający został przez niego przeszkolony w zakresie przepisów RODO, natomiast nikt z tych osób nie otrzymał upoważnienia do przetwarzania danych osobowych.*

System HIS w Szpitalu umożliwiał przesyłanie zleceń na wykonanie badań pomiędzy komórkami oraz pozwalał na dostęp do danych pacjenta.

(akta kontroli tom I str. 166, 208, 398-417, 499-500, tom II str. 73, 87, 96)

2.4. Od 25 maja 2018 r. do 12 kwietnia 2019 r. zatrudnienie w Szpitalu zakończyło 18 osób, spośród których dziewięć w trakcie zatrudnienia posiadało aktywne konto w usłudze Active Directory i programie CLININET. Konta tych osób Administrator Systemów Informatycznych zablokował w dniu rozwiązania z nimi stosunku pracy. Data ostatniego logowania tych osób do systemu nie była w żadnym przypadku późniejsza niż data rozwiązania z nimi stosunku pracy.

(akta kontroli tom I str. 321-323)

2.5. Od 2010 r., dla posiadanego oprogramowania HIS i EDM, Szpital miał uruchomioną usługę zdalnego zgłaszania usterek. Błędy w działaniu programów do obsługi ZOZ były zgłaszane online za pośrednictwem Administratora Sieci Komputerowej lub Zastępcy Kierownika Działu Metodyczno – Organizacyjnego, którzy otrzymywali przedmiotowe informacje bezpośrednio od użytkowników osobiście lub telefonicznie. W okresie od 5 czerwca 2018 r. do 15 lutego 2019 r. przez Portal CGM dostawca oprogramowania otrzymał 100 zgłoszeń, które objęto szczegółowym badaniem. ASI wyjaśnił, że *możliwość zdalnego zgłaszania usterek funkcjonuje w Szpitalu od 2010 r. Od czerwca 2018 r. firma CGM zmieniła platformę do zgłaszania usterek, w związku z czym Placówka nie miała dostępu do wcześniejszych zgłoszeń.* W trzynastu przypadkach stwierdzono przesłanie w treści zgłoszeń lub w załącznikach (zrzuty ekranu) takich danych jak: personalia pacjenta, data urodzenia, numer PESEL, adres, rodzaj zleconych badań lub opis procesu leczenia, co opisano poniżej, w sekcji „*Stwierdzone nieprawidłowości*". W innych sytuacjach, w zgłoszeniu usterki posiłkowano się numerem ID pacjenta – indywidualnym numerem przypisywanym pacjentowi w systemie. W związku z obsługą serwisową programów HIS, EDM oraz płacowo – kadrowego, Szpital miał zawarte umowy powierzenia przetwarzania danych osobowych.

(akta kontroli tom I str. 209-223, 324-394, 448-450)

2.6. W okresie od dnia 15 maja 2018 r. do dnia 11 października 2018 r. Szpital zawarł 20 umów powierzenia danych osobowych, z czego w 11 przypadkach wystąpił jako podmiot powierzający przetwarzanie danych, a w 9 jako procesor[49].

Szczegółowym badaniem objęto pięć umów[50] (cztery umowy dotyczące nadzoru autorskiego oraz usług serwisowych systemów informatycznych HIS i kadrowo – płacowego oraz jedną dotyczącą odczytów danych o skali narażenia na promieniowanie jonizujące). Analiza umów wykazała, że zawierały one, adekwatnie do ich treści, wymagane w art. 28 ust. 3 RODO postanowienia, m.in. zawierały cel i zakres przetwarzanych danych osobowych oraz zapisy o: przetwarzaniu danych osobowych przez procesora wyłącznie na udokumentowane polecenie ADO, zobowiązaniu osób upoważnionych do zachowania tajemnicy, zapewnieniu przez procesora wszelkich środków technicznych i organizacyjnych w celu ochrony danych, przestrzeganiu warunków korzystania z usług innego podmiotu przetwarzającego za zgodą ADO na dalsze

[48] Weryfikację przeprowadzono na podstawie 436 upoważnień do przetwarzania danych osobowych wydanych na podstawie art. 37 u.o.d.o. z 1997 r.

[49] Podmiot przetwarzający dane na podstawie umowy powierzenia danych osobowych.

[50] Zawartych w 2018 r. w dniach: 25 maja (2 umowy), 1 sierpnia, 18 lipca i 4 września.

powierzenie, usunięciu lub zwrocie ADO wszelkich danych osobowych po zakończeniu świadczenia usług, umożliwieniu ADO lub audytorowi upoważnionemu przez ADO przeprowadzenie audytów, w tym inspekcji.

(akta kontroli tom I str. 494-496, tom II str. 34-71)

2.7. IOD prowadził rejestr incydentów i naruszeń, w którym odnotował 12 zdarzeń, z czego jedno zostało zakwalifikowane przez niego jako naruszenie. Dotyczyło ono ataku hakerskiego, do którego doszło w dniu 17 czerwca 2018 r. ADO, stosownie do zapisów art. 33 ust. 1 RODO, dokonał zgłoszenia niniejszego naruszenia Prezesowi UODO w dniu 20 czerwca 2018 r., tj. w ciągu 72-godzin od jego stwierdzenia. Atak hakerski miał miejsce w Dziale Księgowości i został ujawniony w związku ze zgłoszeniem usterki o problemach z działaniem systemu. W wyniku zdarzenia doszło do naruszenia danych podstawowych[51] oraz danych szczególnej kategorii[52] dotyczących pracowników, użytkowników, studentów, klientów, dzieci oraz osób o szczególnych potrzebach (np. osoby starsze, niepełnosprawne itp.). Dyrektor Szpitala wyjaśnił, że *w wyniku ataku wirusa nie doszło do kradzieży danych osobowych. Zostały one zaszyfrowane na jednym serwerze. Po usunięciu wirusa przywrócono dane z kopii zapasowej.*
Zastosowane przez IOD środki zaradcze wprowadzone w 11 pozostałych przypadkach, polegających m.in. na udaremnionych próbach wyrzucenia list pacjentów z numerami PESEL, poleceniu niszczenia nieaktualnych skierowań przez personel sprzątający czy wywieszeniu na drzwiach poradni specjalistycznej listy pacjentów z pełnym imieniem i nazwiskiem, zakończyły się wyeliminowaniem potencjalnych zagrożeń.

(akta kontroli tom I str. 258-274, 514-515, tom II str. 86, 96)

2.8. W okresie od 25 maja 2018 r. do 26 marca 2019 r. dokumentację medyczną pacjentów udostępniono 10 firmom ubezpieczeniowym oraz 338 osobom innym niż pacjenci. Na próbie wszystkich spraw (10) dotyczących wydania dokumentacji firmom ubezpieczeniowym oraz 30 losowo wybranych spraw dotyczących udostępnienia dokumentacji medycznej osobom prywatnym innym niż pacjenci stwierdzono, że podmioty występujące z wnioskiem o udostępnienie dokumentacji medycznej posiadały każdorazowo pisemne upoważnienie pacjenta w tym zakresie, co było zgodne z PBDO oraz art. 26 ust. 1 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta[53]

(akta kontroli tom I str. 423-426)

2.9. W trakcie oględzin 30 komputerów (po 10 użytkowanych przez pielęgniarki, lekarzy oraz pracowników administracyjnych), służących do przetwarzania danych osobowych stwierdzono, że Szpital wprowadził rozwiązania minimalizujące ryzyko utraty lub nieuprawnionej modyfikacji danych osobowych za pośrednictwem tych urządzeń. W 20 przypadkach dotyczących lekarzy oraz pracowników administracyjnych dostęp do poszczególnych systemów informatycznych możliwy był po wprowadzeniu indywidualnego loginu i hasła użytkownika. Nie stwierdzono przypadków wykorzystywania tych samych danych autoryzacyjnych (loginu i hasła) przez kilku użytkowników. We wszystkich przypadkach hasła posiadały liczbę znaków nie mniejszą niż wymagana PBDO. Na ww. 20 komputerach objętych oględzinami uniemożliwiono ich użytkownikom instalowanie oprogramowania, a program antywirusowy posiadał aktualną bazę sygnatur wirusów. Porty USB zostały zabezpieczone przed możliwością podłączenia do nich nośników pamięci.

[51] Dane identyfikacyjne, PESEL, dane kontaktowe, ekonomiczne i finansowe, lokalizacyjne.
[52] Dane dotyczące zdrowia oraz przynależności do związków zawodowych.
[53] Dz. U. z 2017 r. poz. 1318, ze zm.

W pozostałych 10 przypadkach (dotyczących komputerów użytkowanych przez pielęgniarki i położne) pracownicy wykorzystywali w pracy terminale, służące do zalogowania się w systemie HIS. Terminal wymagał podania loginu i hasła, a hasło posiadało odpowiednią liczbę znaków. Porty USB zostały zabezpieczone przed możliwością podłączenia do nich nośników pamięci.

(akta kontroli tom I str. 427-447)

Serwerownia Szpitala była zlokalizowana w wydzielonym pożarowo pomieszczeniu, bez okien oraz wyposażona w dwa klimatyzatory, czujkę pożarową oraz gaśnicę. Drzwi do serwerowni były zamykane na klucz i objęte kontrolą dostępu na kartę. Trzy ustawione na podłodze podniesionej szafy RACK służyły do przetwarzania i przechowywania danych medycznych oraz zapewnienia do połączenia z internetem. Serwerownia była wyposażona w urządzenie do tworzenia kopii zapasowych (backup) oraz UPS podpięty pod centralny UPS i agregat prądotwórczy (zlokalizowany w innym budynku).

W Szpitalu wykorzystywano osiem komputerów przenośnych. ASI wyjaśnił, że *nie mają ochrony kryptograficznej, gdyż nie są one wynoszone poza Placówkę.*

(akta kontroli tom I str. 418-422)

Stosowane w Szpitalu oprogramowania do przetwarzania danych osobowych zainstalowane były na maszynach wirtualnych, na klastrze HA[54] wysokiej dostępności VMware[55]. Przestrzeń dyskowa na macierzy była odporna na awarię dysku, wyposażona w dwa niezależne kontrolery i dwa zasilacze – wszystko podpięte było pod zasilacz UPS. Backup był wykonywany codziennie – przechowywany na dedykowanym urządzeniu dyskowym, a także na taśmach LTO i nośnikach DVD poza serwerownią, w innej części budynku. Informacje o zapisaniu taśmy otrzymywał ASI na poczcie elektronicznej. Przechowywane były taśmy z zapisem całościowym[56]. Sieć wewnętrzna była chroniona przez dwa redundantne UTM-y[57]. Poczta elektroniczna przechowywana była na serwerach Szpitala. Nie dokonywano sprawdzenia poprawności zapisu tworzonych kopii zapasowych, ponieważ ZOZ nie posiadał odpowiednich narzędzi[58].

(akta kontroli tom I str. 208, 448-450)

Stwierdzone nieprawidłowości

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

1. Podjęte przez Szpital działania nie we wszystkich obszarach zapewniały odpowiednią ochronę prywatności pacjentów oraz danych zawartych w dokumentacji medycznej:
   a) Na Oddziale Chirurgii, w trakcie przeprowadzonych w dniu 5 marca 2019 r., oględzin, stwierdzono jeden przypadek zawieszenia przy łóżku pacjenta karty z danymi dotyczącymi stanu zdrowia pacjenta bez osłonki.
   b) Podręczna dokumentacja pielęgniarska na Oddziale Urazowo Ortopedycznym oraz dokumentacja medyczna w dwóch gabinetach lekarskich na Oddziałach Wewnętrznym oraz Urazowo Ortopedycznym, przechowywana była w otwartych szafkach, przy czym w przypadku dokumentacji pielęgniarskiej, szafki te zlokalizowane były w punkcie pielęgniarskim usytuowanym w niezamykanej wnęce na korytarzu Oddziału.

[54] Klaster HV (High Availability) – fizyczny serwer.

[55] W przypadku awarii fizycznego serwera zapewniona jest ciągłość działania systemów, ponieważ maszyny wirtualne automatycznie migrują (przenoszą się) na inny serwer fizyczny w klastrze (np. w zespole trzech klastrów.

[56] Z danymi zgranymi z całego tygodnia.

[57] Ochrona pomiędzy siecią Szpitala, a siecią zewnętrzną (Fiewall), redundantny – nadmiarowy, w razie awarii jeden, w sposób nieodczuwalny dla użytkownika, może przenieść obsługę drugiego.

[58] ABI otrzymywał informacje na e-mail o tym, że tworzenie kopii zapasowej zakończyło się sukcesem.

Powyższe sytuacje stwarzały ryzyko ujawnienia danych medycznych pacjenta osobom nieuprawnionym. Zgodnie z art. 24 ust. 1 RODO, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z tym rozporządzeniem. Jednocześnie, w myśl motywu 39 preambuły oraz art. 5 ust. 1 lit. f. RODO, dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich, niedozwolonym lub niezgodnym z prawem przetwarzaniem. W myśl art. 13 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta[59] (dalej: u.o.p.p.), pacjent ma prawo do zachowania w tajemnicy przez osoby wykonujące zawód medyczny informacji z nim związanych, uzyskanych w związku wykonywaniem tego zawodu.

Pielęgniarka Odcinkowa na Oddziale Chirurgii odnośnie zawieszenia karty pacjenta bez osłonki wyjaśniła, że *pacjent ten został przyjęty nadprogramowo.* IOD podał natomiast, że *dotyczyło to Oddziału urazowego i pacjenci są poddawani operacjom i zabiegom chirurgicznym, w wyniku których bardzo często nie ma z nimi kontaktu. Dlatego niezbędne jest, aby identyfikacja była natychmiastowa. Jest to jeden z dwóch oddziałów w Szpitalu, gdzie karty gorączkowe są zawieszone przy łóżkach pacjentów.* Dyrektor Szpitala wyjaśnił, że *był to pacjent nadprogramowy, dla którego, w chwili przyjęcia, nie było możliwości odpowiedniego zabezpieczenia karty gorączkowej. Oddziały, na których umieszczane są karty przy łóżkach pacjentów zostaną zaopatrzone w osłony rezerwowe, w celu uniknięcia w przyszłości takich incydentów.*

Pielęgniarka Oddziałowa na Oddziale Urazowo-Ortopedycznym wyjaśniła, *że w punkcie pielęgniarskim odbywa się stały dyżur pielęgniarski.* Dyrektor Szpitala wyjaśnił, że *w miarę możliwości finansowych Szpitala Oddział zostanie wyremontowany i obejmie swym zakresem również przebudowę punktu pielęgniarskiego, który uwzględni potrzebę zabezpieczenia dokumentacji. Problem ten został ujęty przez IOD w analizie ryzyka bez sprecyzowania konkretnych uchybień. Do czasu wyremontowania Oddziału personel dokłada wszelkich starań, aby dokumentacja nie była pozostawiona bez nadzoru – przynajmniej jedna osoba musi przebywać w pobliżu dokumentacji.*

Pielęgniarka Oddziałowa na Oddziale Wewnętrznym wyjaśniła, że *w przypadku konieczności opuszczenia gabinetu przez wszystkich lekarzy, pomieszczenie jest zamykane, a klucz przekazywany dyżurującej w gabinecie zabiegowym pielęgniarce.* Kierownik Oddziału Urazowo Ortopedycznego *poinformował, że w przypadku konieczności opuszczenia gabinetu przez wszystkich lekarzy, pomieszczenie jest zamykane na klucz, którym dysponuje każdy lekarz oraz jeden, który przechowują pielęgniarki.* Dyrektor Szpitala wyjaśnił, że *mimo braku szafek zamykanych, dokumentacja znajduje się pod stałym nadzorem lekarzy. W momencie, gdy w gabinecie nikt nie przebywa pomieszczenie zamykane jest na klucz.*

(akta kontroli tom I str. 277, 280, 285, 287-290, 292, 473-474, 487, 490)

2. W 13 (ze 100) zgłoszeniach usterek oprogramowania przekazanych dostawcy oprogramowania od dnia 6 czerwca 2018 r. do dnia do 15 lutego 2019 r., za pośrednictwem platformy CGM, zamieszczono dane personalne 15 pacjentów: imię, nazwisko, datę urodzenia, adres, nr PESEL, informacje o stanie zdrowia, co było niezgodne z wynikająca z art. 5 ust. 1 lit. c) RODO zasadą

[59] Dz. U. z 2017, poz. 1318 ze zm.

adekwatności i minimalizacji danych. Ww. zgłoszenia[60] dotyczyły m.in. (1) wielokrotnego powtórzenia tych samych informacji na wydruku karty informacyjnej, (2) komunikatu o błędzie w związku z korzystaniem z różnych funkcjonalności programu, (3) dodatkowych uprawnień użytkownika systemu, (4) braku przesłania wyników badań pacjenta, (5) możliwości edycji danych opisowych po wypisie pacjenta, (6) braku zgodności wzoru raportu lekarskiego z aktualnym rozporządzeniem, (7) niepełnego wydruku karty kwalifikacyjnej, (8) braku pacjenta w module laboratoryjnym, (9) braku automatycznego czyszczenia danych po wprowadzeniu następnego pacjenta, (10) błędnego wydruku upoważnienia do uzyskiwania danych na temat stanu zdrowia pacjenta. Trzy[61] przypadki zamieszczenia na zrzutach ekranu informacji o stanie zdrowia siedmiu pacjentów zostały udostępnione przez pracowników firmy serwisującej HIS i dotyczyły a) błędu raportu statystyki przeprowadzonych badań przez pracownię RTG, b) braku możliwości zidentyfikowania pacjenta oraz c) błędnego numeru PESEL dla tego samego nr ID pacjenta.

ASI oraz Zastępca Kierownika Działu Metodyczno – Organizacyjnego wyjaśnili, że *Szpital podpisał umowę powierzenia danych z firmą serwisującą, która udostępniła portal do zdalnego zgłaszania usterek. Połączenie do portalu jest bezpieczne (szyfrowane), a dostęp do danych na portalu odbywa się poprzez logowanie za pomocą indywidualnego loginu i hasła.* ASI wyjaśnił również, że *załączenie przez niego danych osobowych, w przypadkach: (1), (2), (3), (4), (5), (6), (9) było niezbędne z następujących powodów: (1) pełna karta informacyjna danego pacjenta pozwoliła poprawnie zidentyfikować i naprawić problem, Brakowało również trybów wypisu, które ten pacjent miał wpisane, dlatego też musiał być on wskazany. Zamazanie jakichkolwiek informacji mogło wprowadzić w błąd osobę realizującą zgłoszenie, ponieważ dotyczyło ono wyświetlania różnych informacji, a zamazanie ich zaburzyłoby schemat karty i tego jak jest prezentowana w systemie, (2) problem dotyczył pacjenta przebywającego na oddziale, więc podanie konkretnego przykładu było niezbędne w celu zweryfikowania czy dana osoba ma wpisane wszystkie niezbędne informacje w danym pobycie, (3) problem nie występował u wszystkich pacjentów, tylko u tych, którzy mieli wpisane uprawnienia dodatkowe (wymagane przez NFZ), więc był zmuszony wskazać konkretny pobyt i konkretną osobę, (4) problem dotyczył konkretnych pacjentów przebywających w tym czasie w Szpitalu, dlatego niezbędne było załączenie wszystkich danych, (5) problem nie dotyczył wszystkich pacjentów, więc należało wskazać przykładowego pacjenta, aby odtworzyć problem, (6) brakowało pól ilość przyjęć i odmów, więc dane pacjentów były konieczne do ustalenia czy dana osoba była przyjęta czy wypisana w celu zaczytania do raportu odpowiednich wartości, (9) problem dotyczył pacjenta przebywającego na oddziale, nie wszyscy pacjenci występujący w systemie mieli wypełniony formularz, więc musiałem wskazać przykład.* Zastępca Kierownika wyjaśnił, że *załączenie przez niego danych osobowych, w przypadkach: (7), (8), (10), (11) było niezbędne z następujących powodów: (7) wydruk karty miał na celu zobrazować graficznie problem jaki wystąpił u konkretnego pacjenta na danym stanowisku komputerowym, czasami dochodzi do sytuacji, ze po stronie firmy CGM wydruk ma inną postać i wtedy wiemy, że problem dotyczy konkretnego komputera, a nie błędnie działającego systemu, (8) zgłoszenie dotyczyło problemu badań diagnostycznych, nie wiem, jak identyfikują poszczególne osoby aparaty laboratoryjne, więc aby nie było*

[60] (1) Nr zgłoszenia 806324985, (2) Nr zgłoszenia 806295922, (3) Nr zgłoszenia 806229649, (4) Nr zgłoszenia 806190871, (5) Nr zgłoszenia 806025091, (6) Nr zgłoszenia 805794636, (7) Nr zgłoszenia 806002471, (8) Nr zgłoszenia 805992111, (9) Nr zgłoszenia 805875899, (10) Nr zgłoszenia 806049804.

[61] Zgłoszenia, w których serwis zamieścił zrzuty ekranu a) nr 805496595, b) nr 805605202 i c) 805683501.

wątpliwości posłużyłem się nr PESEL, (10) zgłoszenie było długo realizowane przez firmę CGM, w trakcie jednej z rozmów telefonicznych zostałem poproszony o graficzne przedstawienie naszych oczekiwań, jak ma wyglądać wydruk, jakie dane i w jakim miejscu mają się pojawiać, aby szybciej zrealizować zgłoszenie.

Dyrektor Szpitala wyjaśnił, że *podtrzymuje stanowisko ASI oraz Zastępcy Kierownika.*

W innych sytuacjach, w zgłoszeniu usterki nie podawano danych osobowych lub posiłkowano się numerem ID pacjenta i było to wystarczające do obsługi zgłoszenia.

(akta kontroli tom I str. 329-394, 451-460, 470-471, 476, tom II str. 87-91, 97-98)

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli negatywnie ocenia ujawnienie danych osobowych pacjentów podczas zgłaszania usterek w systemie informatycznym Szpitala. Pomimo wdrożonych zabezpieczeń (technicznych oraz prawnych), podczas zdalnego zgłaszania usterek dotyczących pracy systemu HIS, w 10% przypadków, pracownicy Szpitala nie zapewnili minimalizacji danych, co było niezgodne z art. 5 ust. 1 lit. c) RODO. Ponadto na dwóch oddziałach stwierdzono też niewłaściwy sposób przechowywania dokumentacji medycznej (w punkcie pielęgniarskim i w dwóch gabinetach lekarskich). Zapewniono natomiast pacjentom dyskrecję podczas rejestracji oraz wywoływania do gabinetów w poradniach specjalistycznych, wprowadzone oznaczenia na opaskach na rękę pacjentów oddziałów szpitalnych zapewniały im anonimowość. Karty gorączkowe przy łóżkach pacjentów (z jednym wyjątkiem) znajdowały się w osłonkach przykrywających dane pacjentów. Personel administracyjny Szpitala nie posiadał dostępu do danych medycznych, a uprawnienia do systemu HIS służącego do przetwarzania danych medycznych nadane 30 pielęgniarkom i położnym, 11 osobom z działu statystyki medycznej oraz trzem informatykom były adekwatne do realizowanych przez nie obowiązków. Dokumentację medyczną udostępniono podmiotom posiadającym stosowne upoważnienia. Szpitalna serwerownia była zabezpieczona przed nieuprawnionym dostępem, a jej wyposażenie w nowoczesny sprzęt zapewniało tworzenie kopii zapasowych i ochronę wewnętrznej sieci.

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. Bieżące aktualizowanie regulacji wewnętrznych dotyczących ochrony danych osobowych oraz bezpieczeństwa informacji i wydanych upoważnień do przetwarzania danych osobowych.
2. Przeprowadzenie szkoleń dotyczących ochrony danych osobowych oraz szkoleń uwzględniających zagadnienia z zakresu bezpieczeństwa informacji określone w § 20 ust. 2 pkt 6 rozporządzenia KRI dla wszystkich pracowników zaangażowanych w proces przetwarzania informacji.
3. Wdrożenie polityki bezpieczeństwa informacji spełniającej wymogi § 20 ust. 1 rozporządzenia KRI.
4. Niepodawanie w zgłoszeniach serwisowych danych osobowych i medycznych pacjentów.
5. Prowadzenie ewidencji pracowników upoważnionych do przetwarzania danych osobowych zgodnie z obowiązującymi w tym zakresie regulacjami wewnętrznymi, w celu zachowania zasady rozliczalności.
6. Wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających ochronę danych osobowych oraz minimalizację ryzyka

ujawnienia informacji osobom postronnym na salach chorych, podczas przechowywania papierowej dokumentacji medycznej pacjentów w dyżurkach pielęgniarskich i gabinetach lekarskich na oddziałach Szpitala.

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 Lublinie. 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 wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 21 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.

Lublin, 19 kwietnia 2019 r.

Kontrolerzy
Małgorzata Dobrowolska
Główny specjalista kontroli państwowej

/-/

.....
podpis

Dyrektor
Delegatury Najwyższej Izby Kontroli
w Lublinie
Edward Lis

/-/

.....
Podpis

Marek Raczkowski
Specjalista kontroli państwowej

/-/

.....
podpis

Zmian w wystąpieniu pokontrolnym dokonał:

Dyrektor
Delegatury Najwyższej Izby Kontroli
w Lublinie
Edward Lis

.....
Podpis