NAJWYŻSZA IZBA KONTROLI
Delegatura w Szczecinie

LSZ. 410.002.01.2019

Pani
Krystyna Pieczyńska
Dyrektor
Zachodniopomorskiego Centrum Onkologii
71-730 Szczecin
ul. Strzałowska 22

WYSTĄPIENIE POKONTROLNE

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

NAJWYŻSZA IZBA KONTROLI
Delegatura w Szczecinie
ul. Jacka Odrowąża 1, 71-420 Szczecin
T +48 91 831 39 00, F +48 91 831 39 66
lsz@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Zachodniopomorskie Centrum Onkologii[1], 71-730 Szczecin ul. Strzałowska 22.
Kierownik jednostki kontrolowanej	Krystyna Pieczyńska, dyrektor ZCO od 1 września 2000 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. do 29 marca 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[2].
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Szczecinie.
Kontrolerzy	1. Leszek Smykowski, specjalista kontroli państwowej, upoważnienie do kontroli nr LSZ/46/2019 z 25 lutego 2019 r. 2. Tomasz Cyranka, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LSZ/49/2019 z 5 marca 2019 r.

(akta kontroli str. 1-5)

[1] Dalej: *Szpital* lub *ZCO*.
[2] Dz. U. z 2019 r. poz. 489. Ustawa zwana dalej: *ustawą o NIK*.

II. Ocena ogólna[3] kontrolowanej działalności

OCENA OGÓLNA

Szpital terminowo opracował wymaganą dokumentację oraz procedury związane z ochroną przetwarzanych danych osobowych, jednak dane osobowe nie były w pełni prawidłowo chronione i przetwarzane.

Uzasadnienie oceny ogólnej

W okresie od 25 maja 2018 r. do 29 marca 2019 r.[4] ZCO posiadał opracowaną i wdrożoną Politykę Bezpieczeństwa Ochrony Danych Osobowych[5], służącą zapewnieniu realizacji celów i zadań z zakresu ochrony danych osobowych, które uwzględniały przepisy RODO[6]. Ich aktualizacja i dostosowanie do tych regulacji nastąpiło przed wejściem w życie tego rozporządzenia.

Wywiązano się z obowiązku powołania Inspektora Ochrony Danych[7] i terminowego zgłoszenia tego faktu Prezesowi Urzędu Ochrony Danych Osobowych[8]. Przeprowadzono analizę procesów przetwarzania danych osobowych oraz ocenę skutków przetwarzania takich danych, mimo że nie była ona obligatoryjna. Pracowników Szpitala zapoznano z regulacjami dotyczącymi ochrony danych osobowych i zagadnieniami dotyczącymi ich bezpieczeństwa. Wszystkie nowozatrudnione osoby obejmowano szkoleniami indywidualnymi bądź grupowymi. Prowadzony rejestr czynności przetwarzania zawierał wszystkie wymagane elementy oraz został opracowany przed wejściem w życie przepisów RODO.

Personel ZCO posiadał adekwatne do wykonywanych obowiązków prawo dostępu do zbioru danych osobowych w zintegrowanym systemie informatycznym i zablokowano w nim konta byłych pracowników. Na bieżąco aktualizowano zakresy pisemnych upoważnień do przetwarzania danych osobowych oraz podejmowano odpowiednie działania w celu minimalizacji ryzyka utraty tych danych. Stwierdzono przypadek przechowywania na komputerze służbowym dokumentacji medycznej pacjentów, lecz była ona odpowiednio zabezpieczona przed dostępem osób niepowołanych. Wyeliminowano ryzyko dostępu osób nieuprawnionych do danych pacjentów zamieszczonych na tablicach z ruchem chorych, lecz nie zapewniono ich anonimowości na opaskach nadgarstkowych i kartach przyłóżkowych. Nie zawsze stosowano się do procedur wewnętrznych przyjętych przez Szpital. Dotyczyło to udostępniania dokumentacji medycznej pacjentów, zawierania umów powierzenia przetwarzania danych osobowych oraz przechowywania kopii zapasowych elektronicznych baz danych Szpitala w tym samym pomieszczeniu, w którym przechowywano dane produkcyjne. Wystąpił jeden przypadek przekazania w zgłoszeniu serwisowym nadmiarowych danych pacjenta, co nie było konieczne do naprawy usterki. Ponadto nie zaktualizowano rejestru umów powierzenia przetwarzania danych osobowych.

---

[3] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.

[4] Dalej: okres objęty kontrolą.

[5] Dalej: *Polityka RODO*.

[6] 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 (ogólne rozporządzenie o ochronie danych). Dz. Urz. UE L 119 z 2016 r., str. 1, ze zm.

[7] Dalej: *IOD*.

[8] Dalej: UODO.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[9] kontrolowanej działalności

OBSZAR

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

Opis stanu faktycznego

1.1. Szpital z dniem 22 maja 2018 r. wyznaczył IOD, wywiązując się tym samym z obowiązku określonego w art. 8 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[10] w związku z art. 37 RODO. Na to stanowisko powołany został w trybie art. 10 ust. 1 u.o.d.o. pracownik ZCO, pełniący dotychczas funkcję Administratora Bezpieczeństwa Informacji[11]. Szpital terminowo[12] wywiązał się z obowiązku zawiadomienia Prezesa UODO o przedłużeniu IOD jego uprawnień w trybie art. 10 ust. 2 u.o.d.o. Przekazane do Prezesa UODO zawiadomienie za pośrednictwem formularza elektronicznego zawierało wszystkie elementy określone art. 10 ust. 1 i 3 u.o.d.o., tj. m.in.: imię, nazwisko oraz adres poczty elektronicznej i numer telefonu IOD, nazwę oraz adres siedziby i numer identyfikacyjny REGON administratora danych osobowych. Zgodnie z wymogiem określonym w art. 37 ust. 7 RODO, dane IOD oraz sposób i formę kontaktu udostępniono na stronie internetowej Szpitala[13] oraz we wszystkich klauzulach informacyjnych Szpitala i klauzulach zgody podpisywanych przez pacjentów .

(akta kontroli str. 6-19, 20-25, 26-40)

Wszystkie zadania IOD określone w art. 39 RODO wskazano w zarządzeniu Dyrektora[14] powołującym IOD. Osobie tej umożliwiono wykonywanie obowiązków w sposób niezależny, stosownie do art. 38 ust. 3 tego rozporządzenia. Samodzielne stanowisko IOD, podległe bezpośrednio Dyrektorowi Szpitala, zostało wyodrębnione w strukturze organizacyjnej ZCO 25 czerwca 2018 r., w związku ze zmianą regulaminu organizacyjnego[15]. Wraz z wprowadzeniem z dniem 5 kwietnia 2018 r. nowego regulaminu organizacyjnego wskazano zadania IOD, do których należało: [1] informowanie Dyrektora oraz pracowników o ich obowiązkach w zakresie ochrony danych osobowych; [2] monitorowanie przestrzegania wymienionych przepisów; [3] szkolenia personelu; [4] prowadzenie okresowych i systematycznych audytów; [5] udzielania wskazówek Dyrektorowi w przedmiocie wdrażania odpowiednich i skutecznych środków technicznych i organizacyjnych w celu ochrony danych osobowych; [6] identyfikowanie ryzyka związanego z przetwarzaniem danych osobowych, jego ocena i działanie pozwalające zminimalizować to ryzyko. Ponadto osoba będąca IOD była zatrudniona na stanowisku starszego specjalisty ds. technologii medycznej i informatyzacji w Sekcji Informatyki i Bezpieczeństwa Informacji. Jej zadania na tym stanowisku dotyczyły m.in. przygotowania, wdrożenia i funkcjonowania zintegrowanego systemu informatycznego zgodnie ze standardami bezpieczeństwa i jakości oraz stworzenie polityki bezpieczeństwa i wdrożenie jej w życie zgodnie z obowiązującymi przepisami. Zadania te nie powodowały konfliktu interesów z zadaniami IOD.

(akta kontroli str. 6-19, 20-25, 26-40)

---

[9] 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.

[10] Dz. U. poz. 1000, ze zm. Ustawa zwana dalej: *u.o.d.o.*

[11] Dalej: ABI.

[12] Dnia 27 sierpnia 2018 r.

[13] www.onkologia.szczecin.pl.

[14] zarządzenie nr 3/2018 Dyrektora ZCO z dnia 22 maja 2018 r. w sprawie powołania IOD.

[15] Regulamin wprowadzono zarządzeniem nr 2/2018 Dyrektora ZCO z dnia 5 kwietnia 2018 r. w sprawie Regulaminu Organizacyjnego ZCO.

Zgodnie z wymogami art. 37 ust. 5 RODO, osoba realizująca zadania IOD miała należyte przygotowanie i kwalifikacje zawodowe do pełnienia swojej funkcji[16].

(akta kontroli str. 26-40)

ZCO 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[17]. Nie prowadzono wobec ZCO postępowania administracyjnego w celu uznania za taki podmiot.

(akta kontroli str. 26-40, 927)

1.2. W okresie objętym kontrolą w Szpitalu obowiązywała, wprowadzona 21 maja 2018 r., Polityka RODO wraz z 19 załącznikami[18] oraz *Instrukcją zarządzania systemami informatycznymi i wykazami zabezpieczeń* oraz załączonymi do niej 10 procedurami[19], stanowiącymi integralną część Polityki. Opracowana dokumentacja oparta była o przepisy prawa obowiązujące od 25 maja 2018 r. Niektóre rozwiązania z ODO[20] sprzed 25 maja 2018 r. i ISO 27001:2014 były podstawą do opracowania np. nowej polityki kluczy, polityki haseł oraz wykonywania backupów.
Na dysku sieciowym, do którego dostęp posiadali wyłącznie pracownicy Szpitala, została zamieszczona dokumentacja ochrony danych osobowych. Przy opracowywaniu dokumentacji brali udział informatycy pomagający w zakresie zabezpieczeń systemów informatycznych. Przed zatwierdzeniem dokumentacji przez Dyrekcję ZCO, Polityka RODO była konsultowana z osobami, które bezpośrednio odpowiadały za jej prawidłowe funkcjonowanie. Po zatwierdzeniu dokumentacji opracowano materiały szkoleniowe dedykowane bezpośrednio dla pracowników Szpitala i przeprowadzono szkolenie z zakresu funkcjonowania i wymogów RODO.
Polityka RODO określała zasady postępowania w zakresie bezpieczeństwa ochrony danych osobowych. W Polityce RODO określono m.in. prawo do sprostowania danych (art. 16 RODO), prawo do usunięcia danych (art. 17 RODO), prawo do ograniczenia przetwarzania (art. 18 RODO), obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania (art. 19 RODO). Celem tej Polityki było zapewnienie właściwego przetwarzania danych, zbieranie ich dla oznaczonych, zgodnych z prawem celów, niepoddawanie danych osobowych dalszemu przetwarzaniu niezgodnemu z celami ich gromadzenia, przetwarzanie danych oraz przechowywanie ich w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż było to niezbędne do osiągniecia celu przetwarzania. Polityka odnosiła się do danych osobowych przetwarzanych w zbiorach tradycyjnych (forma papierowa) oraz w systemach informatycznych. Polityka określała również zadania i obowiązki IOD, do których należało m.in.:

---

[16] Od 22 grudnia 2010 r. pełnił w ZCO funkcję Administratora Bezpieczeństwa Informacji – posiadał wiedzę i wieloletnie doświadczenie w zakresie ochrony danych osobowych i polityki bezpieczeństwa informacji. Legitymował się wykształceniem wyższym technicznym. Odbył cykl szkoleń dotyczących zarządzania bezpieczeństwem informacji wg normy PN-ISO/IEC 27001:2007 oraz wg normy PN-ISO/IEC 27001:2014-12. Posiadał certyfikat ABI i IOD firmy AIMS Ziontek i wspólnicy ze szkoleń w dniach 29.09.2016 r. i 10.05.2018 r.

[17] Dz. U. z 2018 r. poz. 1560.

[18] Rejestr czynności przetwarzania (zał. Nr 1), Wykaz aktywów (zał. Nr 2), Klauzule informacyjne (zał. Nr 3), Powierzenie danych (zał. Nr 4 i 5), Lista potencjalnych zagrożeń (zał. Nr 6), Lista zabezpieczeń (zał. Nr 7), Analiza ryzyka (zał. Nr 8), Wnioski o dostęp do zasobów ZCO (zał. Nr 9), Ewidencja osób upoważnionych do przetwarzania danych (zał. Nr 10), Raport z naruszenia, Rejestr naruszeń ODO (zał. Nr 11), Regulamin Ochrony Danych Osobowych (zał. Nr 12), Oświadczenia poufności (zał. Nr 13), Program szkolenia. Szkolenie – prezentacja. (zał. Nr 14 i 15), Plan postępowania z ryzykiem (zał. Nr 16), Procedura audytu (zał. Nr 17), Plan ciągłości działania (zał. Nr 18), Rejestr kamer i rejestratorów monitoringu wizyjnego CCTV (zał. Nr 19), Rejestr kategorii przetwarzania prowadzony przez ZCO – podmiot przetwarzający (zał. Nr 21).

[19] Zarzadzanie uprawnieniami użytkowników i administratorów (procedura 1), Polityka haseł (procedura 2), Tworzenie i przechowywanie kopii zapasowych (procedura 3), Polityka kluczy (procedura 4), Utylizacja nośników (procedura 5), Regulamin użytkownika komputerów przenośnych (procedura 6), Zabezpieczenie systemu informatycznego (procedura 7), Procedura wykonywania przeglądów i konserwacji (procedura 8), Monitoring wizyjny - CCTV (procedura 9), Bezpieczeństwo pacjenta (procedura 10).

[20] Ochrona danych osobowych, dalej: ODO.

sprawdzanie zgodności przetwarzania danych osobowych z obowiązującymi przepisami, aktualizacje dokumentacji bezpieczeństwa danych osobowych, zapoznanie osób upoważnionych do przetwarzania danych osobowych z obowiązującymi w Szpitalu zasadami oraz dokonywanie analizy stanu ochrony danych.
Polityka RODO była aktualizowana dwukrotnie. Dodano dwie nowe procedury: w czerwcu 2018 r. - procedurę Nr 10 z załącznikiem Nr 20 – Bezpieczeństwo pacjenta oraz w lutym 2019 r. – Monitoring wizyjny CCTV.

(akta kontroli str. 26-40, 41-419)

Zasady ochrony danych osobowych w ZCO określały również dodatkowe procedury wewnętrzne Szpitala. Obowiązek opracowania dodatkowych procedur wynikał z funkcjonowania w ZCO normy PN ISO 27001. Wdrożenie ISO 27001 nastąpiło 8 maja 2012 r., a ostatnią szóstą aktualizację przeprowadzono 9 kwietnia 2018 r. Procedury nadawania upoważnień i anulowania ich znajdowały się w procedurze *P 605 - Kontrola dostępu*, zawierającej stosowne instrukcje i formularze. Postępowanie w sytuacjach awaryjnych obejmowała instrukcja *I 505 – 004 Plan utrzymania lub odtworzenia działalności*, pochodząca z 2015 r. – ostatnia aktualizacja 5 kwietnia 2018 r. Aktualizacja obejmowała: plany awaryjne i odpowiedzialność, tryb postępowania (ocenę zagrożeń i zapewnienie awaryjnych rezerw i kopii zapasowych), zagrożenia (awarię w serwerowni, zniszczenie biur, brak poczty elektronicznej i Internetu, zawirusowanie, awarię sieci strukturalnej LAN). Ww. dokumentacja była aktualizowana zgodnie z wymogami w ISO – nie rzadziej niż co dwa lata.

Sposób zapoznania pracowników z Polityką RODO został opisany w pkt 1.6 wystąpienia.

(akta kontroli str. 26-40)

1.3. Zgodnie z obowiązkiem wynikającym z art. 30 ust. 3 RODO, w Szpitalu od 21 maja 2018 r. prowadzono rejestr czynności przetwarzania (wykaz zbiorów) w formie pisemnej, w tym elektronicznej (arkusz Excel). Ww. rejestr stanowił załącznik nr 1 do Polityki RODO. Rejestr czynności zawierał wszystkie elementy określone w art. 30 ust. 1 RODO tj. nazwy czynności przetwarzania, cel i kategorię osób i danych, które były przetwarzane, planowane terminy usunięcia poszczególnych kategorii danych, kategorie odbiorców, których dane osobowe zostały ujawnione oraz ogólny opis technicznych i organizacyjnych środków bezpieczeństwa stosowanych zgodnie z wymaganiami art. 32 ust. 1 RODO.

(akta kontroli str. 26-40, 71-83, 84-99)

1.4. W Szpitalu od 21 maja 2018 r. prowadzono analizę ryzyka, o której mowa w art. 32 RODO. W załączniku Nr 2 zestawiono aktywa w sześciu grupach wraz z możliwymi podaktywami dla każdej grupy. W załączniku Nr 6 zestawiono potencjalne zagrożenia dla aktywów. W załączniku Nr 7 zestawiono listę potencjalnych zabezpieczeń. W załączniku Nr 8 dokonano analizy ryzyka dla aktywów. W załączniku Nr 16 zestawiono zagrożenia i plan postępowania z istniejącym ryzykiem po wykonaniu analizy wg załącznika Nr 8. Cała analiza ryzyka wraz z opracowaniem planu postępowania była integralną częścią całej Polityki RODO i została opublikowana razem z tą polityką. W wyniku analizy wyodrębniono 51 możliwych do wystąpienia ryzyk w siedmiu grupach tematycznych m.in.: włamania, kradzieży, pożaru, zalania, awarii, uzyskania dostępu przez osobę nieupoważnioną, błędu i złośliwego działania użytkowników, używania prostych haseł, utraty danych z lokalnych dysków oraz braku kopii danych. Dla każdego z ryzyk określono prawdopodobieństwo i skutek oraz oszacowano jego wartość.

Największą wartość oszacowanego ryzyka na poziomie 6 punktów przypisano możliwości wystąpienia ataków na system komputerowy lub usługę sieciową w celu uniemożliwienia działania, kradzieży lub zagubieniu sprzętu i nośników poza jednostką, przegrzaniu lub wysokiej wilgotności w serwerowni lub archiwum, nieuprawnionemu kopiowaniu danych. W przypadku 24 ryzyk, których oszacowana wartość była na poziomie od 3 do 6 punktów[21] wskazano działania zapobiegawcze i korygujące. Rekomendowane działania, które zostały podjęte bezpośrednio przed wdrożeniem Polityki, dotyczyły m.in.: zapewnienia zabezpieczeń w postaci WAB, Firewall, mechanizmu captcha, systemu SIEM, testów penetracyjnych, szyfrowania laptopów i pendrive, klimatyzacji i monitoringu środowiskowego serwerowni i archiwum, blokowania portów USB, blokowania funkcji eksportu danych w programach i systemach Szpitala, rozliczanie operacji (sprawdzanie, czy każdy użytkownik programu / systemu posiada swój indywidualny login).

Analizę procesów przetwarzania danych osobowych rozpoczęto od ustalenia wszystkich zbiorów danych osobowych. Następnie przeanalizowano jakie czynności są wykonywane na danych osobowych zawartych w tych zbiorach. Następnie pogrupowano je ze względu na powtarzające się procesy przetwarzania. Dla każdego procesu wskazano ryzyka i dokonano oceny poziomu zagrożenia. Uwzględniono wszystkie procesy występujące w ZCO.

(akta kontroli str. 26-40, 71-83, 100-103, 137-169)

1.5. W Szpitalu została wykonana ocena skutków dla ochrony danych[22], o której mowa w art. 35 RODO, mimo że jest fakultatywna. Również Grupa Robocza ds. Ochrony Danych[23] zdecydowanie zalecała dokonanie tej analizy dla operacji przetwarzania trwających przed 25 maja 2018 r.[24],w przypadkach, gdy nie było jasne, czy wymagana jest DPIA[25]. Analiza ta stanowiła element Polityki RODO przyjętej 21 maja 2018 r. DPIA zawierała elementy wymagane art. 35 ust. 7 RODO, w tym opis operacji przetwarzania i ocenę niezbędności oraz proporcjonalności. Dyrektor wyjaśnił, że *oceny skutków dla ochrony danych osobowych dokonano w maju 2018 r. Wyniki tej analizy przedstawiono w załączniku 8 i 16. W związku z tym, że w ZCO nie występuje ryzyko nieakceptowane (poziom 9) nie opracowano szczególnych procedur likwidacji zagrożeń. Z przedstawionych analiz ryzyka wynika, że występujące zagrożenia związane z dużymi możliwymi skutkami powinny być pod szczególną obserwacją i ich poziom prawdopodobieństwa wystąpienia powinien być zawsze poniżej 2. Często jest to związane z ponoszeniem dodatkowych kosztów finansowych na modernizację infrastruktury sieciowej czy związaną z przechowywaniem danych.*

(akta kontroli str. 26-40, 71-83, 151-169)

1.6. Jednym z zadań IOD, w myśl art. 39 ust. 1 lit. b RODO, jest prowadzenie szkoleń personelu uczestniczącego w operacjach przetwarzania danych. Kwestie przeprowadzania szkoleń zostały również określone w rozdziale 8 Polityki RODO,

---

[21] Poziom ryzyka akceptowalnego wynosił dziewięć punktów, maksymalne ryzyko stwierdzone w Szpitalu wyniosło sześć punktów.

[22] Dalej: *DPIA*.

[23] Grupa ta powołana została na mocy art. 29 dyrektywy 95/46/WE. Była ona niezależnym organem doradczym w zakresie ochrony danych i prywatności.

[24] 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 dostęp z dnia 4 marca 2019 r.

[25] Uznano bowiem, że jest ona *przydatnym narzędziem, które może pomóc administratorom danych w zapewnieniu zgodności z prawem ochrony danych*, chociaż Prezes UODO w komunikacie[25] – 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.

gdzie wskazano, że każda osoba przed dopuszczeniem do pracy z danymi osobowymi winna być poddana przeszkoleniu i zapoznaniu z przepisami RODO. Za przeprowadzanie szkoleń odpowiedzialny był IOD. W przypadku przeprowadzania szkoleń, odbywały się one zgodnie z planem i programem szkoleń określonym w zał. Nr 14 do Polityki RODO i w oparciu o materiały szkoleniowe określone w zał. Nr 15 do Polityki. Po przeszkoleniu uczestnicy szkoleń zobowiązani byli do potwierdzenia znajomości ww. zasad wypełnieniem oświadczenia poufności w formie określonej w zał. Nr 13. IOD realizując wymieniony obowiązek przeprowadził w okresie objętym kontrolą 27 grupowych szkoleń z zakresu RODO, w których wzięły udział łącznie 471 osoby. Szkolenia z RODO przeprowadzono w kilku grupach zawodowych rozpoczynając od osób mających bezpośredni kontakt z pacjentem. W dniu 28.05.2018 r. przeszkolono grupę statystyków, od 04 do 06.06.2018 r. szkolony był personel medyczny, w okresie 11 – 12.06.2018 r. administracja szpitala, a od 19.06. – 24.07.2018 r. szkoleni byli pracownicy, którzy nie mogli uczestniczyć w szkoleniach wcześniejszych. Szkolenia zostały przeprowadzone w oparciu o przygotowaną przez IOD prezentację uwzględniającą specyfikę pracy Szpitala ze szczególnym uwypukleniem bezpieczeństwa pacjenta, obiegu dokumentacji medycznej i wymogów w stosunku do personelu ZCO.

(akta kontroli str. 26-40, 71-83, 192-266, 494-537)

Szkolenia z ochrony danych osobowych były przeprowadzane od 2011 r., średnio co dwa lata – w 2011; 2013 i 2016 r. W 2011 r. szkolenie przeprowadzono z zasad ochrony danych osobowych i skutków wynikających z braku zapewnienia tej ochrony. W 2013 r. motywem przewodnim było bezpieczeństwo teleinformatyczne z uwzględnieniem zagrożeń i skutków wynikających z dostępu do Internetu. W 2016 r. szkolenie obejmowało ponownie ochronę danych osobowych z informacjami z bezpieczeństwa teleinformatycznego, przedstawiając zagrożenia i wprowadzone zabezpieczenia gwarantujące ciągłość pracy, integralność danych, dostęp do danych wraz z właściwymi uprawnieniami użytkowników. Pierwsze szkolenie w 2011 r. wynikało z powołania ABI i wprowadzenia polityki ochrony danych. Kolejne szkolenia wynikały z harmonogramu szkoleń – cyklu dwuletniego związanego z przeglądem dokumentacji ODO i ISO 27001. ABI (późniejszy IOD) realizując obowiązek szkoleń w zakresie bezpieczeństwa danych wskazany w § 20 ust. 2 pkt 6 rozporządzenia 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 przeprowadził[26] 33 grupowe szkolenia w 2016 r. z zakresu polityki bezpieczeństwa informatycznego, w których wzięły udział łącznie 476 osoby.

(akta kontroli str. 26-40, 461-493)

Analiza dokumentacji szkoleniowej wszystkich pracowników ZCO[27] wykazała, że:

- na 547 osób zatrudnionych w ZCO, szkoleń z zakresu przepisów RODO nie przeszło 29 pracowników (ok. 5% zatrudnionych);
- 139 pracowników (ok. 25% zatrudnionych) nie zostało przeszkolonych z zakresu bezpieczeństwa danych informatycznych;
- wszyscy przeszkoleni pracownicy złożyli oświadczenia poufności (stanowiące załącznik Nr 13 do Polityki RODO), w których m.in. stwierdzili, że zapoznano ich z przepisami dotyczącymi ochrony danych osobowych, zawartymi w RODO i u.o.d.o.

[26] Dz.U. z 2017 r. poz. 2247, zwane dalej: rozporządzeniem KRI.

[27] Wg stanu zatrudnienia na 1 marca 2019 r.

W sprawie szkoleń Dyrektor wyjaśnił, m.in., że *zgodnie z obowiązującymi procedurami zatrudnienia w ZCO, każda osoba przed podjęciem obowiązków służbowych jest szkolona w zakresie ochrony danych osobowych oraz z wybranych (dostosowanych do specyfiki zajmowanego stanowiska pracy) zagadnień bezpieczeństwa informatycznego obowiązującego w naszej placówce. Szkolenie przeprowadzane jest przez IOD i na potwierdzenie tego składany jest podpis pod tzw. kartą obiegową pracownika. Fakt ten ma odzwierciedlenie w teczce osoby zatrudnionej. Od maja 2018 r. fakt obycia indywidualnego szkolenia każdy pracownik potwierdza na dokumencie „oświadczenie poufności".*

Przedstawiono nazwiska 29 osób, które z powodu zwolnienia (chorobowe, macierzyński) lub z przyczyn losowych nie uczestniczyły w szkoleniach nt. zmian RODO organizowanych na przełomie lipca/sierpnia 2018 r. Każda z tych osób przechodziła indywidualne szkolenie przed dopuszczeniem do stanowiska pracy. Dla pracowników tych planowane jest szkolenie na przełomie maja/czerwca 2019 r.

Nazwiska 139 osób (…) dotyczą szkoleń organizowanych w lipcu/sierpniu 2016 r. Obejmują one pracowników, którzy nie podjęli jeszcze pracy w ZCO w tym terminie lub też nie mogli uczestniczyć w szkoleniach z powodu zwolnienia (chorobowe, urlop macierzyński) lub z przyczyn losowych. Zaznaczyć należy, że każda z tych osób przechodziła indywidualne szkolenie przed dopuszczeniem do stanowiska pracy. Dla tych pracowników, którzy nie byli uczestnikami szkoleń z lipca/sierpnia 2018 r. planowane jest również szkolenie na przełomie maja/czerwca 2019 r.

Analiza dokumentacji Szpitala wykazała, że wszyscy zatrudnieni w okresie objętym kontrolą pracownicy ZCO przed dopuszczeniem do pracy na swoim stanowisku poddani zostali indywidualnemu szkoleniu z zakresu ODO (lub RODO).

(akta kontroli str. 420-460, 912-926, 927)

1.7. Szpital nie zobowiązał się formalnie (np. poprzez deklarację stosowania) do przestrzegania regulacji zawartych w *Kodeksie postępowania dla sektora ochrony zdrowia*[28], dla którego wniosek o przyjęcie został 13 listopada 2018 r. przedłożony[29] Prezesowi UODO lub pozostałych opracowań związanych z ochroną danych osobowych, takich jak *Przewodnik po RODO w służbie zdrowia*[30] i *Wytyczne dotyczące inspektorów ochrony danych*[31].

(akta kontroli str. 927)

W powyższej sprawie Dyrektor wyjaśnił m.in., że *ZCO kieruje się kodeksem dobrych praktyk wynikających z opracowanych szczegółowych procedur związanych z polityką jakości. W Szpitalu funkcjonują łącznie 43 procedury obejmujące wszystkie aspekty pracy ZCO, które zaczęły obowiązywać od chwili wprowadzenia Zintegrowanego Systemu Zarządzania Jakością. Dodatkowo ZCO przechodzi co trzy lata proces akredytacyjny spełniając wszystkie wymogi w nim zawarte. Podczas ostatniej akredytacji w lipcu 2018 r. Szpital uzyskał wynik 86%.*

(akta kontroli str. 26-40)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

[28] Treść kodeksu została opublikowana na stronie internetowej: www.rodowzdrowiu.pl.

[29] Przez Polską Federację Szpitali – podmiot opracowujący ten dokument.

[30] Przewodnik został 24 września 2018 r. opublikowany na stronie internetowej Ministerstwa Cyfryzacji.

[31] Wytyczne zostały 10 maja 2018 r. opublikowane na stronie internetowej Urzędu Ochrony Danych Osobowych.

OCENA CZĄSTKOWA

Szpital wywiązał się z obowiązku opracowania dokumentacji oraz procedur dotyczących ochrony danych osobowych, które uwzględniały przepisy RODO. Ich aktualizacja i dostosowanie do regulacji nastąpiło przed wejściem w życie rozporządzenia. Wywiązano się z obowiązku powołania IOD i terminowego zgłoszenia tego faktu Prezesowi UODO. Przeprowadzono analizę procesów przetwarzania danych osobowych oraz ocenę skutków przetwarzania takich danych, mimo że nie była obligatoryjna. Pracowników Szpitala zapoznano z regulacjami dotyczącymi ochrony danych osobowych i zagadnieniami dotyczącymi ich bezpieczeństwa. Wszystkie nowozatrudnione osoby objęto szkoleniami. Prowadzony rejestr czynności przetwarzania zawierał wszystkie wymagane elementy oraz został opracowany przed wejściem w życie przepisów RODO.

OBSZAR

2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych.

Opis stanu faktycznego

2.1. Oględziny trzech[32] (z sześciu) funkcjonujących w Szpitalu rejestracji wykazały, że w celu ochrony danych osobowych pacjentów:

- Zapewniono, aby w obrębie wzroku pacjenta, znajdującego się przy oknie rejestracji, nie znajdowały się dokumenty zawierające dane osobowe innych pacjentów. Dokumenty osób już zarejestrowanych były na bieżąco przenoszone do gabinetów zabiegowych lub poradni Szpitala. Inne dokumenty medyczne dotyczące pacjenta nie były dostarczane na stanowiska osób rejestrujących. W rejestracjach nie zamontowano przesłon pomiędzy poszczególnymi stanowiskami. IOD wyjaśnił, że: *weryfikacja tożsamości pacjenta w rejestracji odbywała się poprzez okazanie przez niego dokumentu weryfikującego tożsamość, ograniczając ryzyko uzyskania danych osobowych przez osobę trzecią*. Pracownicy rejestracji od każdej rejestrującej się osoby żądali okazania dokumentu tożsamości, nie wypowiadali na głos informacji zawierających dane osobowe, przekazując jedynie dane dotyczące dalszego procesu postępowania po zarejestrowaniu się do danej poradni lub gabinetu.
- W jednej rejestracji[33], pomiędzy osobami przy okienku, a kolejnymi w kolejce, ustawione zostało drewniane przepierzenie, za którym stały kolejne oczekujące na rejestrację osoby. W dwóch rejestracjach[34] poza informacją o treści: *Przy okienku rejestracji może przebywać tylko jedna osoba,* zamieszczoną na każdym z okien rejestracji, nie wprowadzono innych rozwiązań zapewniających odstęp pomiędzy osobami przy okienku, a kolejnymi osobami w kolejce. Podczas oględzin nie stwierdzono osób stojących bezpośrednio za osobą przy okienku.
- Przy każdej rejestracji, umieszczono klauzule informacyjne (w formie wydruku). Ich treść była zgodna z treścią klauzuli stanowiącej załącznik do Polityki RODO, przyjętej 21 maja 2018 r.
- Przy okienkach wszystkich rejestracji zamieszczono informację dla pacjentów o konieczności okazania dowodu osobistego. Identyfikacja wszystkich pacjentów (rejestrujących się w trakcie prowadzonych oględzin) odbywała się na podstawie dowodów osobistych okazanych rejestratorce.

---

[32] Rejestracje: Poradni Ginekologii, Chirurgii Onkologicznej, Onkologii – Gabinet Profilaktyki Chorób Piersi i Diagnostyki Onkologicznej – pomieszczenie P18 wejście 8c, Przychodni Onkologii – Chemioterapii/Radioterapii/Dermatologii - pomieszczenie I1 wejście 8A i 8B oraz Diagnostyki Obrazowej – pomieszczenie R24.

[33] Rejestracja Poradni Ginekologii, Chirurgii Onkologicznej, Onkologii – Gabinet Profilaktyki Chorób Piersi i Diagnostyki Onkologicznej – pomieszczenie P18 wejście 8c

[34] Rejestracja Przychodni Onkologii – Chemioterapii/Radioterapii/Dermatologii - pomieszczenie I1 wejście 8A i 8B oraz Diagnostyki Obrazowej – pomieszczenie R24.

- Wszystkie monitory znajdujące się w rejestracjach były ustawione w sposób, który uniemożliwiał osobom rejestrującym się wgląd w treści na nich wyświetlane.
- W dwóch rejestracjach[35] pacjenci po zarejestrowaniu otrzymywali karteczki zawierające m.in. numer gabinetu, datę i godzinę wizyty, numer wskazujący na kolejność przyjęć. W jednej rejestracji[36] pacjenci otrzymywali specjalnie przygotowane numery (plastikowe tabliczki), zawierające nazwę badania oraz nazwę zakładu.

(akta kontroli str. 41-62, 543-545)

We wszystkich trzech objętych oględzinami gabinetach poradni specjalistycznych Szpitala[37] dokumentację pacjentów przechowywano we właściwy sposób. Pacjent wchodzący do gabinetu nie miał możliwości zapoznania się z danymi osobowymi innych osób oczekujących w kolejce lub tych, którzy odbyli już wizytę. W trakcie oględzin żaden gabinet nie został pozostawiony bez nadzoru. Oczekujący w kolejce samodzielnie ustalali kolejność (pytając osoby z kolejki o numerki). Do gabinetu wchodzili bez wezwania, po wyjściu aktualnie przebywającego w nim pacjenta.

(akta kontroli str. 41-62, 546-547)

Oględziny dyżurek pielęgniarskich, sal chorych oraz gabinetów lekarskich na trzech oddziałach szpitalnych[38] wykazały m.in., że:

- na oddziałach znajdowało się 80 sal chorych z 221 łóżkami;
- wszyscy zaobserwowani pacjenci w liczbie 154 nosili na nadgarstku opaski informacyjne zawierające widoczne następujące dane: imię i nazwisko pacjenta, pesel, kod kreskowy, nazwa szpitala, nazwa oddziału, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości;*
- za wyjątkiem pierwszego piętra jednego oddziału[39] na wszystkich trzech oddziałach przy łóżkach pacjentów zostały umieszczone karty zawierające widoczne imię i nazwisko pacjenta i lekarza (lub jego inicjały), w sposób umożliwiający odczytanie danych na nich zapisanych, bez konieczności ich wyjęcia z zawieszek, w których się znajdowały, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości*;
- ruch chorych[40] prowadzony był w dyżurkach pielęgniarskich w miejscach niewidocznych dla osób postronnych;
- w dyżurkach pielęgniarskich podręczna dokumentacja pielęgniarska przechowywana była prawidłowo;
- trzy dyżurki pielęgniarskie poddane oględzinom wyposażono w sześć komputerów, z których cztery były uruchomione – na trzech pracowały pielęgniarki, a przy jednym nie było nikogo z obsługi, zaś dostęp do systemu operacyjnego został zablokowany;
- w trzech poddanych oględzinom gabinetach lekarskich[41], znajdował się uruchomiony komputer, przy którym pracował lekarz, pozostałe komputery były wyłączone;

[35] Rejestracja Poradni Ginekologii, Chirurgii Onkologicznej, Onkologii – Gabinet Profilaktyki Chorób Piersi i Diagnostyki Onkologicznej – pomieszczenie P18 wejście 8c oraz Przychodni Onkologii – Chemioterapii/Radioterapii/Dermatologii - pomieszczenie I1 wejście 8A i 8B.

[36] Rejestracja 3 Diagnostyki Obrazowej – pomieszczenie R24.

[37] Oględzinami objęto: gabinet Poradni Radioterapii pok. P61, Profilaktyki Chorób Piersi i Diagnostyki Onkologicznej pok. P31, Chemioterapii pok. P57.

[38] Oględzinom poddano Oddziały: Kliniczny Radioterapii, Onkologii Klinicznej i Chirurgii Onkologicznej.

[39] Oddział Chirurgii Onkologicznej.

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

– dokumentacja medyczna pacjentów, którzy mieli zostać przyjęci danego dnia w gabinetach lekarskich, leżała na blacie biurka (lub w koszyku, w którym została dostarczona) stroną tytułową skierowaną do dołu. Dokumentacja medyczna pozostałych pacjentów nie była przechowywana w gabinetach lekarskich. W trakcie oględzin dyżurek pielęgniarskich i gabinetów lekarskich nie pozostawiono otwartych i bez nadzoru.

(akta kontroli str. 41-62, 68, 538-542)

Podczas oględzin stwierdzono, że na trzech oddziałach zamontowano osiemnaście kamer, z tego siedem nagrywało obraz, ustawionych w sposób uniemożliwiający odczytywanie danych z dokumentacji medycznej. Łącznie w pozostałych budynkach (wewnątrz i na zewnątrz) funkcjonował monitoring wizyjny składający się z 136 kamer związanych z ochroną mienia, 15 kamer związanych z leczeniem i 9 kamer związanych z leczeniem – napromieniowaniem. Informacja o monitoringu (zawierająca m.in. dane ADO, kontakt do IOD, informację o celu stosowania monitoringu i czternastodniowym czasie przechowywania nagrań) znajdowała się przy drzwiach wejściowych do pomieszczeń ZCO. Zgodnie z postanowieniami Polityki RODO - Procedura 9 – Monitoring w ZCO[42], zapisy monitoringu przechowywane były przez okres do jednego miesiąca, a dostęp do niego miał dyrektor ZCO, dyrektor ds. administracyjno-eksploatacyjnych, IOD oraz administratorzy Systemu Monitoringu Wizyjnego CCTV – łącznie 5 osób. Dokument *Regulamin monitoringu wizyjnego (CCTV)* czas przechowywania nagrań określał na nie dłużej niż dziewięćdziesiąt dni. Dostęp do podglądu obrazu posiadało 149 osób.

Regulamin monitoringu wizyjnego został sporządzony wraz z opracowaniem Polityki RODO dla Szpitala. Jak wyjaśnił IOD *Regulamin monitoringu wizyjnego (CCTV) jest elementem procedury nr 9, która została opracowana w związku z wejściem w życie RODO. W maju 2018 r. opublikowano ustawę o ochronie danych osobowych, która w artykułach 111 i 122 umożliwiła prawne funkcjonowanie monitoringu wizyjnego (CCTV). Dlatego wcześniej nie było wytycznych prawnych przygotowania regulaminu funkcjonowania monitoringu. Monitoring wizyjny funkcjonuje w ZCO od ponad 10 lat*".

(akta kontroli str. 41-62, 548-553)

2.2. Według stanu na 11 marca 2019 r. personel działów administracyjnych[43] Szpitala liczył 95 osób. Analiza uprawnień 30 osób z tej grupy w systemach Eskulap; Aria; Cato; Patomorfolg; Syngo.Via; Syngo.Plaza[44] wykazała, że 14 osób miało dostęp do HIS/EDM, z czego po jednej osobie z działów: Archiwum, Informatyki i Bezpieczeństwa Informacji, Obsługi Pacjenta i Ewidencji Świadczeń, Kierownictwa, samodzielnego stanowiska pracy (specjalista ds. epidemiologii) i Zakładu Diagnostyki Laboratoryjnej, po dwie osoby z Działu Rozliczeń i Analiz oraz po trzy osoby z Działu Żywienia i Zachodniopomorskiego Rejestru Nowotworów Złośliwych i odpowiadały one zakresom zadań i obowiązków realizowanych przez tych pracowników. Szesnaście osób nie posiadało dostępu do systemów HIS/EDM, co również wynikało z ich zakresów obowiązków.

---

[41] Nr 08 na Oddziale Kliniczny Radioterapii, nr OD112 na Oddziale Onkologii Klinicznej i gabinet lekarski na Oddziale Chirurgii Onkologicznej.

[42] Polityka RODO - Procedura 9 – Monitoring w ZCO.

[43] Działy i inne stanowiska: Księgowości, Apteka, Archiwum, Administracyjno – Gospodarczy, Informatyki i Bezpieczeństwa Informacji, Obsługi Pacjenta i Ewidencji Świadczeń, Rozliczeń i Analiz, Spraw Pracowniczych i Organizacyjnych, Techniczny, Żywienia, Kierownictwo, Samodzielne stanowiska pracy, Zachodniopomorski Rejestr Nowotworów Złośliwych, Zakład Diagnostyki Laboratoryjnej.

[44] Systemy typu HIS/EDM (Hospital Information System) – rodzaj oprogramowania do obsługi ruchu pacjentów wewnątrz podmiotu leczniczego, EDM- Elektroniczna Dokumentacja Medyczna (Electronic Health Record) – system informatyczny przechowujący część lub całość dokumentacji medycznej indywidualnej i/lub zbiorczej w podmiocie leczniczym.

(akta kontroli str. 41-62, 580-609)

2.3. Analiza uprawnień w systemach ESKULAP i CATO, przeprowadzona na próbie 30 pielęgniarek i położnych (ze 141) zatrudnionych w Szpitalu[45] wykazała, że dostęp został nadany na oddział/poradnię gdzie wykonywały swoje obowiązki.

(akta kontroli str. 554-579, 927)

Do przetwarzania danych osobowych nie upoważniono żadnej z osób zatrudnionych na stanowiskach: sanitariuszy, salowych lub personelu sprzątającego.

(akta kontroli str. 41-62, 927)

2.4. Od 25 maja 2018 r. do 31 grudnia 2018 r. Szpital rozwiązał stosunek pracy z 32 osobami. Spośród nich, 15 w trakcie zatrudnienia miało przyznany dostęp do systemów informatycznych (konto w Active Directory[46]). W dniu oględzin konta 13 osób były wyłączone[47]. Ostatnie logowanie tych osób miało miejsce przed datą zaprzestania świadczenia pracy. Dwie osoby zostały ponownie zatrudnione w Szpitalu i ich konta były aktywne. Wyłączenie konta w AD blokowało danej osobie dostęp do systemów informatycznych ZCO, ponieważ wszystkie stacje zarządzane były domenowo. Polityka RODO Szpitala zobowiązywała użytkowników do ochrony hasła.

(akta kontroli str. 610-618, 928-929)

2.5. W myśl postanowień umów serwisowych, które obowiązywały w okresie objętym kontrolą[48], Szpital obowiązany był do zgłaszania błędów w działaniu systemów HIS/EDM poprzez Help Desk (tylko ESKULAP – pod adresem https://helpdesk.nexuspolska.pl), telefonicznie na infolinię lub pocztą internetową na wskazane w umowie adresy. W okresie od 25 maja 2018 r. do 15 marca 2019 r. miały miejsce zgłoszenia awarii do programów HIS/EDM: ESKULAP – 89 razy, ARIA – 10 razy, CATO – nie było zgłoszeń, PATOMORFOLOG – jeden raz, SYNGO.VIA i PLAZA - nie było zgłoszeń.

- Oględziny sposobu przekazania 51 (ze 100) zgłoszeń serwisowych[49], związanych z błędami lub wadliwym działaniem systemu informatycznego ESKULAP (47 zgłoszeń), ARIA (trzy zgłoszenia) i PATOMORFOLOG (jedno zgłoszenie) wykazały m.in., że: [1] dostęp do archiwalnych zgłoszeń w systemie ESKULAP możliwy był po dokonaniu autoryzacji (wpisaniu loginu i hasła) w serwisie internetowym do tego wykorzystywanym; [2] pozostałe zgłoszenia zrealizowano drogą mailową; [3] w jednym przypadku, w zgłoszeniu o nr 50877 z 31 grudnia 2018 r. dotyczącym systemu ESKULAP przekazano dane medyczne pacjenta Szpitala (imię i nazwisko, PESEL i nazwę choroby) – jak wyjaśnił IOD w tym przypadku „*Niezbędne zatem okazało się wskazanie konkretnego przykładu, którego problem dotyczy, z odpowiednią ilością informacji do przetworzenia, aby producent systemu mógł przeanalizować błędy w działaniu aplikacji. Wpisanie zanonimizowanych danych spowodowałoby brak odniesienia do konkretnego przypadku*". Z podmiotem, któremu przekazano dane 21 maja 2018 r., została zawarta *umowa powierzenia przetwarzania*

[45] Dane wg. stanu na 11 marca 2019 r.

[46] Active Directory to oprogramowanie przechowujące m.in. dane o koncie użytkownika (zablokowanie konta uniemożliwiało dostęp do zasobów informatycznych Szpitala), dalej: AD.

[47] W Active Directory nie można ustalić kiedy dane konto zostało zablokowane.

[48] Umowy z firmami: Nexus Polska (ESKULAP) – w zakresie oprogramowania wszystkich modułów wraz z bazą danych, Varian (ARIA) – w zakresie sprzętu i całego oprogramowania, Siemens (SYNGO.PLAZA i .VIA) - w zakresie sprzętu i całego oprogramowania, Silversoft (Patomorfolog) - w zakresie oprogramowania i bazy danych.

[49] Zgłoszenia te Szpital przekazał od 25 maja 2018 r. do 15 marca 2019 r.

danych osobowych. Zobowiązywała ona podmiot do ochrony przekazanych mu danych osobowych pacjenta.

(akta kontroli str. 41-62, 619-628)

Szpital nie posiadał informacji dotyczących wywiązania się przez dostawcę nowo wdrożonego oprogramowania z obowiązku przeprowadzenia testów akceptacyjnych, zgodnie z art. 21 ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[50]. Jak wyjaśnił IOD *„Nowo wdrażane oprogramowanie Eskulap NT nie będzie podlegało obowiązkowi wynikającemu z art. 21 ust. 1 ww. ustawy, ponieważ nie jest realizowana wymiana informacji za pomocą implementowanego systemu z podmiotami niebędącymi podmiotami publicznymi, co wynika z § 5 ust. 3 rozporządzenia Ministra Nauki i Informatyzacji z dnia 19 października 2005 r. w sprawie testów akceptacyjnych oraz badania oprogramowania interfejsowego i weryfikacji tego badania (Dz.U. Nr 217, poz. 1836). W ZCO nie przeprowadzono badania poprawności wdrożenia rozwiązań w oprogramowaniu interfejsowym przy wykorzystaniu testów akceptacyjnych udostępnionych przez podmiot publiczny. Zgodnie z art. 13 ust. 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, testy akceptacyjne oprogramowania szpitalnego i publikacja w BIP-ie zestawienia stosowanych w oprogramowaniu formatów danych oraz protokołów komunikacyjnych i szyfrujących nie są wymagane w sytuacji wymiany danych pomiędzy Szpitalem a podmiotami publicznymi."*

(akta kontroli str. 41-62, 927)

2.6. W okresie objętym kontrolą ZCO zawarł 27 umów dotyczących powierzenia przetwarzania danych osobowych, z tego 23 umowy dotyczące przetwarzania danych osobowych pacjentów. Z 23 umów dotyczących przetwarzania danych osobowych pacjentów Szpital zawarł 18 umów, w których wystąpił jako podmiot powierzający przetwarzanie danych oraz pięć umów, gdzie wskazano go jako podmiot przetwarzający dane osobowe pacjentów. Przesłanki, dla których ZCO jako ADO, zawarł umowy powierzenia przetwarzania danych pacjentów dotyczyły: zewnętrznego serwisu maszyn i urządzeń oraz oprogramowania, zlecania badań diagnostyki obrazowej i laboratoryjnej na zewnątrz z powodu braku możliwości wykonania tego we własnym zakresie oraz wykonywania usług hotelowych i transportowych przez firmy zewnętrzne.

(akta kontroli str. 41-62, 71-83, 112-136)

Analiza 16 z 27 umów dotyczących powierzenia danych osobowych wykazała, że w przypadku 12 podmiotów ZCO zawarł umowy powierzenia przetwarzania danych osobowych (zgodnie ze wzorem w formie zał. Nr 4 do Polityki RODO), a w przypadku czterech podmiotów umów takich nie zawarł, dokonując jedynie rozszerzenia zapisów umowy podstawowej o zapisy dotyczące przepisów RODO, co było odstępstwem od Polityki RODO przyjętej do stosowania przez Szpital, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości.* Wszystkie 16 badanych umów zawierało elementy określone w art. 28 ust. 3 przepisów RODO tj. przedmiot i czas trwania przetwarzania danych osobowych, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, a także prawa administratora.

Analiza 27 spraw dotyczących powierzenia danych wykazała, że 14 podmiotów z którymi ZCO zawarł umowy powierzenia przetwarzania danych osobowych, nie wymieniono w rejestrze stanowiącym załącznik Nr 5 Polityki RODO, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości.*

[50] Dz. U. z 2017 r. poz. 570, ze zm.

(akta kontroli str. 41-62, 112-136, 699-727, 728-831)

2.7. W rozdziale 5 Polityki RODO umieszczono *Instrukcję postępowania z incydentami (naruszeniami)*, w której określono m.in.: przykłady podatności i incydentów zagrażających bezpieczeństwu danych osobowych; sposób postępowania w przypadku wystąpienia takich zdarzeń; wynikający z art. 33 ust. 5 RODO obowiązek dokumentowania wszystkich naruszeń danych osobowych, ich okoliczności, skutków oraz podjętych działań zaradczych na formularzu rejestracji incydentu[51]. W ww. *instrukcji* wskazano obowiązek zgłoszenia organowi nadzorczemu, w terminie 72 godzin, każdego przypadku naruszenia danych osobowych, skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych. Załącznikiem Nr 11 do Polityki RODO były dokumenty *Raport z naruszenia* i *Rejestr naruszeń ODO*.

(akta kontroli str. 41-62, 71-83, 177-179)

W okresie objętym kontrolą w Szpitalu nie odnotowano przypadków naruszenia zasad ochrony danych osobowych pacjentów.

(akta kontroli str. 41-62, 927)

W badanym okresie nie stwierdzono skarg i wniosków, które dotyczyłyby nieprawidłowości związanych z ochroną danych osobowych pacjentów.

(akta kontroli str. 41-62, 927)

2.8. W okresie objętym kontrolą w Szpitalu funkcjonowały wewnętrzne procedury dotyczące udostępniania dokumentacji medycznej, sformalizowane zarządzeniem Nr 14/2017 Dyrektora ZCO z dnia 13 grudnia 2017 r.[52] W myśl tych regulacji oraz zgodnie z przepisem art. 24 ust. 1 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta[53], dokumentację medyczną Szpital mógł udostępniać pacjentowi lub jego przedstawicielowi ustawowemu bądź osobie upoważnionej przez pacjenta oraz podmiotom określonym w ust. 3 powołanego przepisu. W procedurach wewnętrznych wskazano również, że można udostępnić tą dokumentację pacjentowi lub jego przedstawicielowi ustawowemu, osobie upoważnionej przez pacjenta oraz upoważnionym organom. Szpital, chcąc zapewnić dostęp do żądanej dokumentacji bez zbędnej zwłoki, przyjmował wnioski o udostępnienie dokumentacji medycznej od pacjentów, ich przedstawicieli ustawowych i osób upoważnionych bezpośrednio w komórce medycznej, w której dokumentacja ta została wytworzona bądź w Kancelarii Zakładu (sekretariacie Dyrektora). W § 3 ww. zarządzenia określono m.in., że w przypadku osób fizycznych miało odbyć się to po sporządzeniu wniosku o udostępnienie dokumentacji medycznej wg wzoru w postaci załącznika nr 1 do ww. zarządzenia, a w przypadku organów (m.in. firm ubezpieczeniowych) - po przedłożeniu pisemnego wniosku oraz po sporządzeniu protokołu udostępnienia dokumentacji medycznej wg wzoru w postaci załącznika nr 2 do ww. zarządzenia.

(akta kontroli str. 41-62, 832-839)

W okresie objętym kontrolą w prowadzonych przez Szpital rejestrach (w różnych jednostkach organizacyjnych ZCO) odnotowano łącznie 250 przypadków udostępnienia dokumentacji medycznej osobom fizycznym i podmiotom zewnętrznym. Wśród nich odnotowano 38 przypadków udostępnienia informacji

[51] Formularz nosił nazwę: załącznik nr 11 - Rejestr naruszeń i P 601 – formularz F 601-000-001.

[52] w sprawie zasad i trybu udostępniania dokumentacji medycznej, udzielania zakładom ubezpieczeń informacji o stanie zdrowia ubezpieczonych oraz odpłatności za udostępnienie dokumentacji medycznej i udzielenie informacji o stanie zdrowia.

[53] Dz. U. z 2017 r. poz. 1318, ze zm. Ustawa zwana dalej: *u.o.p.p.*

komercyjnym instytucjom ubezpieczeniowym oraz 120 przypadków dotyczących udostępnienia tej dokumentacji osobom fizycznym, w tym 105 pacjentom i 15 osobom innym niż pacjent.

Analiza prawidłowości udostępnienia dokumentacji w odniesieniu do wszystkich tych przypadków wykazała, że:

- we wszystkich 15 przypadkach w których dokumentacja medyczna została udostępniona osobom innym niż pacjent, osoby te posiadały upoważnienie pacjenta do dostępu do tej dokumentacji;
- na 120 spraw nie sporządzono trzech wniosków o udostępnienie dokumentacji medycznej wg wzoru w postaci załącznika nr 1 do zarządzenia Nr 14/2017 Dyrektora ZCO, a pozostałe 83 wnioski obarczone były wadami formalnymi: brakiem adnotacji o odbiorze / wysyłce dokumentacji medycznej pacjenta, brakiem podpisu osoby przyjmującej lub składającej wniosek, brakiem daty sporządzenia wniosku, brakiem daty odebrania bądź wysłania dokumentacji, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości;*
- w 30 przypadkach (z 38) instytucje ubezpieczeniowe, którym Szpital udostępnił informacje o stanie zdrowia ubezpieczonego, posiadały upoważnienie pacjenta do dostępu do tej informacji;
- w ośmiu przypadkach (z 38) Szpital odmówił udostępnienia firmie ubezpieczeniowej informacji o stanie zdrowia z uwagi na brak pacjenta w bazie danych ZCO;
- na 30 spraw udostępniania informacji o stanie zdrowia pacjenta firmom ubezpieczeniowym nie sporządzono jednego protokołu udostępnienia dokumentacji medycznej wg wzoru w postaci załącznika nr 2 do zarządzenia Nr 14/2017 Dyrektora ZCO, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 41-62, 840-896, 897-906, 907-911)

2.9. Regulacje dotyczące ochrony danych przed ich utratą w wyniku awarii, błędów lub nieuprawnionej modyfikacji zostały opisane w *Regulaminie Ochrony Danych Osobowych* oraz w *Instrukcji zarządzania systemem informatycznym i wykaz zabezpieczeń*[54]. W dokumentach tych określono m.in. zasady: [1] bezpiecznego użytkowania sprzętu IT, dysków i programów; [2] zarządzania uprawnieniami, w tym procedurę rozpoczęcia, zawieszenia i zakończenia pracy; [3] polityki haseł; [4] zabezpieczenia dokumentacji papierowej z danymi osobowymi; [5] korzystania z Internetu i z poczty elektronicznej; [6] ochrony antywirusowej; [7] tworzenia, przechowywania i testowania kopii bezpieczeństwa; [8] zabezpieczeń fizycznych i technicznych; [9] procedury tworzenia kopii zapasowych, utylizacji elektronicznych nośników i wydruków oraz czyszczenia danych, zabezpieczenia systemu informatycznego i wykonywania przeglądów i konserwacji. Ponadto określono obowiązek zachowania poufności i ochrony danych osobowych i zasady postępowania dyscyplinarnego.

(akta kontroli str.170-195, 294-331, 358-373)

Oględziny jedynej serwerowni Szpitala wykazały, m.in. że: [1] właściwie zabezpieczono dostęp do tego pomieszczenia stosując niepalne drzwi metalowe bez oznaczeń informujących o przeznaczeniu pomieszczenia; [2] zamontowano system alarmowy, przeciwpożarowy (gazowy układ gaszenia), monitoringu wizyjnego; [3] w pomieszczeniu umieszczono gaśnicę oraz układ klimatyzacji i wentylacji; [4] w celu

[54] Regulamin i Instrukcja zostały zatwierdzone przez Dyrektora Szpitala w dniu 21 maja 2018 r.

zapobieżenia zalaniu wszystkie urządzenia znajdowały się na tzw. podłodze technicznej, tj. powyżej poziomu posadzki; [5] na wypadek czasowego zaniku zasilania zastosowano układy podtrzymujące napięcie UPS; [6] wszystkie urządzenia informatyczne zamontowano w specjalnie do tego przystosowanych szafach typu RACK; [7] w serwerowni nie było okien; [8] prowadzony był rejestr osób z zewnątrz, które miały dostęp do tego pomieszczenia, [9] przez serwerownię nie przebiegają rury wodno-kanalizacyjne; [10] nie gromadzono w tym pomieszczeniu materiałów łatwopalnych. Zgodnie z *Planem ciągłości działania*[55], Szpital wyposażono w agregat prądotwórczy.

ZCO zminimalizował ryzyko utraty informacji w wyniku awarii poprzez techniczne zabezpieczenie serwerowni.

Kopie zapasowe baz danych Szpitala były przechowywane w pomieszczeniu serwerowni, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 41-62, 63-70, 269-282, 629-632)

Oględziny 30 komputerów stacjonarnych Szpitala, w tym 20 wykorzystywanych na oddziałach Szpitala przez lekarzy, pielęgniarki i położne oraz 10 użytkowanych przez pracowników administracyjnych Szpitala wykazały m.in., że:

- dostęp do systemu operacyjnego wymagał podania indywidualnego loginu i hasła spełniającego wymagania określone w regulacjach wewnętrznych[56], w trakcie oględzin każdy pracownik logował się na swoje konto,
- wszystkie stacje zarządzane były domenowo i wykorzystywane do przetwarzania danych osobowych/medycznych w systemach HIS/EDM,
- w 26 komputerach nie zostały zablokowane porty USB, umożliwiając podłączenie do nich nośników pamięci i kopiowanie danych,
- na wszystkich stanowiskach użytkownicy posiadali ograniczone uprawnienia w systemie operacyjnym, które nie pozwalały na wprowadzanie zmian w konfiguracji tych urządzeń oraz instalację oprogramowania,

(akta kontroli str. 554-579, 645-669)

- za wyjątkiem dwóch stanowisk[57] na pozostałych został zainstalowany obowiązujący w Szpitalu program antywirusowy, posiadający aktualną wersję bazy sygnatur wirusów, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 41-62, 63, 66, 69, 189, 633-644, 645-698)

- na dysku jednego komputera[58] (w folderach *Moje dokumenty i pulpit*) znajdowało się 12 plików z kartami informacyjnymi zawierającymi: imię i nazwisko, pesel, opis pobytu (stanu pacjenta) i 144 pliki ze skierowaniami do poradni specjalistycznych zawierające imię i nazwisko, pesel pacjenta, rozpoznanie choroby. Jak wyjaśnił IOD, zgodnie z Regulaminem ODO[59] każdy użytkownik zobowiązany jest do usuwania plików z nośników, do których mają dostęp inni nieupoważnieni użytkownicy. Dostęp do wymienionych plików miał tylko użytkownik, który był zalogowany w trakcie oględzin. Dostęp do pomieszczenia

[55] Załącznik nr 18 RODO – Plan ciągłości działania.

[56] Załącznik do Instrukcji zarządzania systemami informatycznymi i wykaz zabezpieczeń - Procedura 2 – Polityka haseł.

[57] Na komputerach ARIA EDIT 02 (wykorzystywany w izbie przyjęć Oddziału Radioterapii p.019) i DIAG-VIAR8-K01 (wykorzystywany w pokoju lekarskim R8 USG) znajdował się program Defender, w tym na jednej stacji nie działał – został włączony w trakcie oględzin.

[58] Na komputerze CHIR-004-K01 wykorzystywanym w pokoju badań nr 04 Oddziału Chirurgii Onkologicznej.

[59] Załącznik nr 12 do Polityki RODO pkt 1 ppkt 9.

był monitorowany i możliwy poprzez użycie karty dostępu. Co dwie godziny wykonywana była kopia bezpieczeństwa plików partycji systemowej na stacjach roboczych.

(akta kontroli str. 41-62, 64, 67, 69, 70, 645-669)

W Szpitalu wykorzystywanych jest 46 komputerów przenośnych, nie stosuje się ochrony kryptograficznej i nie jest stosowana pseudonimizacja danych osobowych pacjentów. Polityka RODO Szpitala, w przypadku pracy na komputerze przenośnym, zabraniała przechowywania lokalnie danych osobowych pacjentów.

(akta kontroli str. 41-62)

Stwierdzone nieprawidłowości

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

1. W § 20 ust. 2 pkt 7 i 9 rozporządzenia KRI zapisano, że kierownictwo podmiotu publicznego jest obowiązane do podejmowania działań zapewniających ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także zabezpieczenia przetwarzanych informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie. W załączniku Nr 12 do Polityki RODO *Regulamin Ochrony Danych Osobowych* stwierdzono, że obowiązującym na wszystkich komputerach programem antywirusowym jest program ESET NOD32.

   Na dwóch stanowiskach komputerowych[60] nie został zainstalowany obowiązujący w Szpitalu[61] program antywirusowy.

   Jak wyjaśnił IOD, brak zainstalowanego oprogramowania antywirusowego spowodowany był umowami serwisowymi z dostawcami oprogramowania wykluczającymi instalowanie jakiegokolwiek obcego oprogramowania nie zatwierdzonego przez producenta sprzętu oraz ze względu bezpieczeństwa wyłączenia na obu stacjach dostępu do Internetu (co było warunkiem aktualizacji wykorzystywanego oprogramowania antywirusowego).

   W czasie kontroli w dniu 20.03.2019 r. dokonano zmiany wersji na nowszą programu antywirusowego ESET NOD 32. Ta wersja umożliwia rozszerzenie zarządzania aktualizacją oprogramowania o komputery nie posiadające dostępu do Internetu w oparciu o dane z serwera lokalnego.

   (akta kontroli str. 63, 66, 69, 189, 633-644, 645-698)

2. W art. 5 pkt 1 lit. c RODO wskazano, że dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane ("minimalizacja danych").

   Oględziny sposobu przekazania 51 (ze 100) zgłoszeń serwisowych, związanych z błędami lub wadliwym działaniem systemu informatycznego ESKULAP (47 zgłoszeń), ARIA (trzy zgłoszenia) i PATOMORFOLOG (jedno zgłoszenie) wykazały m.in., że: w jednym przypadku, w zgłoszeniu o nr 50877 z 31 grudnia 2018 r. dotyczącym systemu ESKULAP przekazano dane medyczne pacjenta Szpitala (imię i nazwisko, PESEL i nazwę choroby).

   Ww. oględziny wykazały, że w praktyce pracownicy ZCO przekazując informacje o usterkach anominizowali dane medyczne pacjentów.

[60] Na komputerach ARIA EDIT 02 (wykorzystywany w izbie przyjęć Oddziału Radioterapii p.019) i DIAG-VIAR8-K01 (wykorzystywany w pokoju lekarskim R8 USG) – zamiast programu ESET NOD32 - znajdował się program Defender, w tym na jednej stacji nie działał – został włączony w trakcie oględzin.

[61] zgodnie z Załącznikiem nr 12 Regulamin Ochrony Danych Osobowych do Polityki RODO „*Obowiązującym na wszystkich komputerach programem antywirusowym jest program ESET NOD32*"

Jak wyjaśnił IOD, *niezbędne zatem okazało się wskazanie konkretnego przykładu, którego problem dotyczy, z odpowiednią ilością informacji do przetworzenia, aby producent systemu mógł przeanalizować błędy w działaniu aplikacji. Wpisanie zanonimizowanych danych spowodowałoby brak odniesienia do konkretnego przypadku*.

(akta kontroli str. 41-62, 619-628, 927)

3. Zgodnie z art. 36 pkt. 5 ppkt 2 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej[62] pacjentów szpitala zaopatruje się w znaki identyfikacyjne zapisane w sposób uniemożliwiający identyfikację pacjenta przez osoby nieuprawnione.

   Wszyscy pacjenci w trzech kontrolowanych oddziałach Szpitala nosili na nadgarstku opaski informacyjne zawierające widoczne dane: imię i nazwisko pacjenta, pesel, kod kreskowy, nazwę szpitala, nazwę oddziału oraz, za wyjątkiem pierwszego piętra jednego oddziału, na wszystkich trzech oddziałach przy łóżkach pacjentów zostały umieszczone karty zawierające widoczne imię i nazwisko pacjenta i lekarza (lub jego inicjały), w sposób umożliwiający odczytanie danych na nich zapisanych.

   IOD wyjaśnił: „*Szpital zdecydował się na takie rozwiązanie ze względu na konieczność jednoznacznej identyfikacji leżącego na sali chorego. Zdarzało się, że pacjenci samowolnie zamieniali się łóżkami. Zgodnie z procedurą nr 10 (Bezpieczeństwo pacjenta) – pacjenci podczas przyjęcia na oddział szpitalny na izbie przyjęć podpisują następującą klauzulę zgody : „Wyrażam zgodę na hospitalizację oraz zlecone zabiegi diagnostyczne, terapeutyczne, leczenie operacyjne i pielęgnacyjne wraz z identyfikacją mojej osoby w celu zapewnienia mojego bezpieczeństwa”.*

   Odnosząc się do powyższych wyjaśnień należy podkreślić, że pacjenci wyrażali zgodę na ich identyfikację przez personel Szpitala, a nie przez osoby postronne, które miały dostęp do danych na opaskach.

   (akta kontroli str. 41-62, 68, 538-542)

4. Kopie zapasowe baz danych Szpitala były przechowywane w pomieszczeniu serwerowni, co było niezgodne z postanowieniami Polityki RODO Szpitala[63].

   Jak wyjaśnił IOD „*miejsce przechowywania kopii zapasowych jest najbezpieczniejszym z obecnie możliwych*”.

   (akta kontroli str. 41-62, 63-70, 144-150, 154-169, 269-282, 629-632)

5. Polityka RODO w ZCO zakłada powierzenie danych osobowych pacjentów lub pracowników przez ZCO lub dla ZCO w formie umowy powierzenia przetwarzania danych osobowych, której wzór przedłożono w formie załącznika Nr 4 do tej Polityki.

   W czterech z 16 analizowanych umowach dotyczących powierzenia danych osobowych stwierdzono, że nie zostały one zawarte według wzoru stanowiącego załącznik nr 4 do Polityki RODO. Dokonano jedynie rozszerzenia zapisów umowy podstawowej o zapisy dotyczące przepisów RODO i było to odstępstwo od Polityki RODO przyjętej do stosowania prze Szpital. Dyrektor wyjaśnił m.in., że *ZCO stosuje jednolite zasady wobec podmiotów, z którymi ma podpisane umowy o współpracy. Niemniej jednak zmianie ulegały wytyczne i zalecenia ekspertów w zakresie wdrażania RODO w branży medycznej. Aktualne*

[62] Dz.U z 2018 r. poz. 2190.

[63] Załącznik nr 7 *Lista potencjalnych zagrożeń*, załącznik nr 16 – *Plan postępowania z ryzykiem*, załącznik nr 18 – *Plan ciągłości działania* pkt. 4.3.

interpretacje wskazują, iż nie jest konieczne zawieranie osobnych umów na powierzenia przetwarzania danych. Potwierdzeniem ich jest oczekiwane zatwierdzenie przez Prezesa UODO tzw. „Kodeksu branżowego RODO dla ochrony zdrowia", w którym to w pkt. 5.4.7 znajduje się zapis: „Umowa powierzenia przetwarzania może również mieć postać klauzul umownych będących częścią umowy o szerszym zakresie np. umowy o świadczenie usług".

(akta kontroli str. 41-62, 112-136, 699-727, 728-831, 912-926)

6. Polityka Ochrony Danych Osobowych RODO w ZCO zakłada powierzenie danych osobowych pacjentów lub pracowników przez ZCO podmiotom lub dla ZCO przez podmioty w formie umowy powierzenia przetwarzania danych osobowych, których wykaz przedłożono w formie załącznika Nr 5 do tej Polityki.

   Analiza wpisów do rejestru wykazała, że nie był on aktualizowany. Z 27 analizowanych spraw dotyczących powierzenia przetwarzania danych wynika, że w rejestrze umów powierzenia danych osobowych wymieniono 13 podmiotów (trzy dwukrotnie), a 14 podmiotów, z którymi ZCO zawarło umowy powierzenia przetwarzania danych osobowych, nie wymieniono w rejestrze.

   Dyrektor wyjaśnił m.in., że w *zakresie bieżącego aktualizowania ww. rejestru doszło do uchybienia procedurom funkcjonującym w ZCO. Weryfikacja i aktualizacja rejestru umów nastąpi niezwłocznie tj. do 15.04.2019 r.*

   (akta kontroli str. 41-62, 129-136, 699-727, 728-831, 912-926)

7. Dokumentację medyczną pacjentów udostępniano w kontrolowanym okresie na podstawie zapisów zarządzenia Nr 14/2017 Dyrektora ZCO z dnia 13.12.2017 r. W § 3 ww. zarządzenia określono m.in., że w przypadku osób fizycznych odbywa się to po sporządzeniu wniosku o udostępnienie dokumentacji medycznej wg wzoru w postaci załącznika nr 1 do ww. zarządzenia.

   Analiza wykazała, że dokumentację medyczną udostępniano właściwym osobom (pacjentowi lub osobie przez niego upoważnionej), jednak w trzech przypadkach na 120 spraw pracownicy Szpitala udostępnili dokumentację medyczną bez wniosku wymaganego zarządzeniem Nr 14/2017 Dyrektora ZCO, a kolejne 83 wnioski o udostępnienie dokumentacji medycznej obarczone były wadami formalnymi: brakiem adnotacji o odbiorze/ wysyłce dokumentacji medycznej pacjenta, brakiem podpisu osoby przyjmującej lub składającej wniosek, brakiem daty sporządzenia wniosku, brakiem daty odebrania bądź wysłania dokumentacji.

   Dyrektor wyjaśnił m.in., że *prawo pacjenta do dokumentacji medycznej powinno być również respektowane poprzez indywidualne podejście do potrzeb wnioskodawcy, uwzględniające jego sytuację i potrzeby. Celem działania ZCO było każdorazowo nieczynienie przeszkód formalnych, w sytuacji gdy spełnione były przesłanki zachowania poufności i ochrony danych osobowych. Istotą procesu udostępnienia dokumentacji medycznej jest jej przekazanie osobom uprawnionym, zgodnie z wolą pacjenta i obowiązującymi przepisami.*

   Wady formalne związane z brakiem adnotacji o odbiorze / wysyłce dokumentacji medycznej, brakiem podpisu osoby przyjmującej lub składającej wniosek, brakiem daty odebrania lub wysłania dokumentacji jak również brakiem wniosków o udostępnienie dokumentacji medycznej spowodowane były nienależytą uwagą podczas dokumentowania prawidłowości udostępnienia dokumentacji medycznej. W tym zakresie trwa procedura wyjaśniająca. Osoby odbierające dokumentację medyczną były weryfikowane na podstawie dokumentów tożsamości. W celu zapobieżenia tego typu uchybieniom formalnym w przyszłości ZCO ujednolici ścieżkę udostępnienia dokumentacji medycznej poprzez utworzenie jednego

centralnego rejestru wniosków o udostępnienie dokumentacji medycznej. Każdy wniosek będzie indywidualnie weryfikowany przez oddelegowanego pracownika pod kątem uzupełniania wymaganych danych. Ponadto ZCO znacznie wzmocni nadzór nad pracownikami w zakresie stosowania się do procedur wynikających z przepisów ogólnych jak i zarządzenia Dyrektora ZCO. ZCO dołoży wszelkich starań, aby stwierdzone braki formalne nie występowały w przyszłości.

(akta kontroli str. 41-62, 840-896, 897-906, 907-911, 912-926)

8. Dokumentację medyczną pacjentów udostępniano w kontrolowanym okresie na podstawie zapisów zarządzenia Nr 14/2017 Dyrektora ZCO z dnia 13.12.2017 r. W § 3 ww. zarządzenia określono m.in., że w przypadku organów (m.in. firm ubezpieczeniowych) odbywa się to po przedłożeniu pisemnego wniosku oraz po sporządzeniu protokołu udostępnienia dokumentacji medycznej wg wzoru w postaci załącznika nr 2 do ww. zarządzenia.

   Analiza wykazała, że na 30 spraw udostępniania informacji o stanie zdrowia pacjenta firmom ubezpieczeniowym nie sporządzono jednego protokołu udostępnienia dokumentacji medycznej wg wzoru w postaci załącznika nr 2 do zarządzenia Nr 14/2017 Dyrektora ZCO.

   Dyrektor wyjaśnił m.in., że *odstąpienie od wypełnienia załącznika nr 2 do Zarządzenia Nr 14/2017 Dyrektora ZCO spowodowana była przesłaniem przez firmę wnioskującą o udostępnienie danych osobowych własnego formularza do uzupełnienia informacji. W opisywanym przypadku naliczanie kosztów za udostępnienie informacji wraz z kosztami przesyłki odbyło się wedle ww. zarządzenia. Pragniemy zaznaczyć, iż aktualnie protokoły o udostępnienie dokumentacji medycznej są uzupełniane i dołączane do każdego wniosku o udostępnienie dokumentacji medycznej przesyłanego przez firmy ubezpieczeniowe. W celu zapobieżenia tego typu uchybieniom w przyszłości ZCO ujednolici ścieżkę udostępnienia dokumentacji medycznej poprzez utworzenie centralnego rejestru wniosków o udostępnienie dokumentacji medycznej. Każdy wniosek będzie indywidualnie weryfikowany przez oddelegowanego pracownika pod kątem uzupełniania niezbędnych danych. Ponadto ZCO znacznie wzmocni nadzór nad pracownikami w zakresie stosowania się do procedur wynikających z przepisów ogólnych jak i Zarządzenia Dyrektora ZCO.*

   (akta kontroli str. 41-62, 840-896, 897-906, 907-911, 912-926)

9. W dokumencie Polityka RODO - Procedura 9 – Monitoring w ZCO w pkt. 3.3.1 czas przechowywania nagrań z rejestratorów monitoringu wizyjnego został określony na okres do 1 miesiąca.

   W dokumencie Polityka RODO - Procedura 9 – Regulamin monitoringu wizyjnego (CCTV) na „nie dłużej niż 90 dni".

   Na tabliczkach znajdujących się przy drzwiach wejściowych do budynków ZCO zamieszczono informację o 14 dniowym okresie.

   Zarejestrowany obraz przechowywany był do 63 dni, w zależności od wyposażenia rejestratora. Dostęp do nagrań miały tylko osoby upoważnione przez ADO.

   Dyrektor wyjaśnił m.in., że *dane obrazowe monitoringu CCTV faktycznie nie są przechowywane dłużej niż 90 dni. Różnice w czasie wynikające ze stosowania rejestratorów o różnej pojemności nagrań zostaną ujednolicone w Polityce RODO do dnia 15.04.2019 r.*

(akta kontroli str. 41-62, 840-896, 897-906, 907-911, 912-926, 927)

OCENA CZĄSTKOWA

W Szpitalu wdrożono rozwiązania organizacyjne i techniczne zmierzające do zapewnienia prawidłowej ochrony i przetwarzania danych osobowych. Nie były one jednak w pełni przestrzegane. Personel ZCO posiadał adekwatne do wykonywanych obowiązków prawo dostępu do zbioru danych osobowych w zintegrowanym systemie informatycznym. Szpital aktualizował na bieżąco zakresy pisemnych upoważnień do przetwarzania danych osobowych pracowników Szpitala i zablokował w tym systemie konta byłych pracowników. Podejmowano odpowiednie działania w celu minimalizacji ryzyka utraty danych. Stwierdzono przypadek przechowywania na komputerze służbowym dokumentacji medycznej pacjentów, lecz była ona odpowiednio zabezpieczona przed dostępem osób niepowołanych. Wyeliminowano ryzyko dostępu osób nieuprawnionych do danych pacjentów zamieszczonych na tablicach z ruchem chorych, lecz nie zapewniono ich anonimowości na opaskach nadgarstkowych i kartach przyłóżkowych. Przy udostępnianiu dokumentacji medycznej pacjentów i zawieraniu umów powierzenia przetwarzania danych osobowych nie zawsze stosowano się do procedur wewnętrznych przyjętych przez Szpital. Ponadto wystąpił jeden przypadek przekazania w zgłoszeniu serwisowym nadmiarowych danych pacjenta, co nie było konieczne do naprawy usterki. Nie zaktualizowano rejestru umów powierzenia przetwarzania danych osobowych. Stwierdzono także, że kopie bezpieczeństwa były przechowywane w tym samym pomieszczeniu, w którym znajdowały się dane produkcyjne poddawane procesowi tworzenia tych kopii. Powyższe działania były niezgodne z zasadami określonymi w Polityce RODO Szpitala.

IV. Uwagi i 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. *Wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających minimalizację ryzyka utraty danych osobowych poprzez przechowywanie kopii bezpieczeństwa w odrębnym pomieszczeniu od pomieszczenia, w którym znajdują się dane produkcyjne poddawane procesowi tworzenia tych kopii*.
2. *Stosowanie się do procedur wewnętrznych przyjętych przez Szpital przy udostępnianiu dokumentacji medycznej pacjentów i przy zawieraniu umów powierzenia przetwarzania danych osobowych*.
3. *Ujednolicenie zapisów dotyczących czasu przechowywania danych z monitoringu wizyjnego w Polityce RODO i zaktualizowanie dokumentów, których prowadzenie wynika z tej Polityki*.
4. *Zanonimizowanie danych pacjentów na opaskach nadgarstkowych i uniemożliwienie ich odczytu na kartach przyłóżkowych*.
5. *Anonimizowanie danych medycznych i osobowych pacjentów przy przesyłaniu informacji o awarii firmom zapewniającym serwis oprogramowania*.

Uwagi

Najwyższa Izba Kontroli nie formułuje uwag.

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 Szczecinie. 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 od dnia 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.

Szczecin, 19 kwietnia 2019 r.

Kontroler:

Leszek Smykowski
specjalista kontroli państwowej

DYREKTOR DELEGATURY
Najwyższej Izby Kontroli w Szczecinie