NAJWYŻSZA IZBA KONTROLI
Delegatura w Krakowie

LKR.410.002.04.2019

Pan Marcin Kuta
Dyrektor Specjalistycznego Szpitala
im. E. Szczeklika w Tarnowie
ul. Szpitalna 13, 33-100 Tarnów

WYSTĄPIENIE POKONTROLNE

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

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

I. Dane identyfikacyjne

Jednostka kontrolowana	Specjalistyczny Szpital im. Edwarda Szczeklika w Tarnowie (dalej: *Szpital*)
Kierownik jednostki kontrolowanej	Marcin Kuta, dyrektor od 4 stycznia 2004 r. (dalej: *Dyrektor Szpitala*)
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 21 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[1]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Krakowie
Kontroler	Rafał Rossowski, starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LKR/40/2019 z 29 stycznia 2019 r.

(akta kontroli str. 1-2)

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

W ocenie Najwyższej Izby Kontroli przyjęte w Szpitalu rozwiązania techniczne i organizacyjne nie zapewniały należytej ochrony danych osobowych i nie eliminowały ryzyka nieuzasadnionego dostępu do danych przetwarzanych w systemach informatycznych Szpitala.

Szpital wywiązał się z obowiązku sporządzenia w terminie procedur dotyczących ochrony danych osobowych uwzględniając przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (tzw. ogólne rozporządzenie o ochronie danych)[3]. Szpital przeprowadził analizy procesów przetwarzania danych. W sposób właściwy wywiązano się z obowiązku powołania Inspektora Ochrony Danych (dalej: *IOD*) i terminowego zgłoszenia tego faktu Prezesowi Urzędu Ochrony Danych Osobowych, a poprzez przyjęte rozwiązania organizacyjne zagwarantowano mu status niezależności w sprawowaniu tej funkcji. Personelowi Szpitala zapewniono odpowiedni dostęp do danych medycznych. W Szpitalu podejmowano właściwe działania w celu minimalizacji ryzyka utraty danych osobowych w wyniku awarii, błędów lub nieuprawnionej modyfikacji; w trakcie kontroli nie stwierdzono przypadków ujawnienia i przekazywania takich danych osobom lub podmiotom nieuprawnionym.

[1] Dz.U. z 2019 r. poz. 489. Dalej: *ustawa o NIK*.
[2] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej. W niniejszym wystąpieniu zastosowano ocenę opisową.
[3] Dz. Urz. UE L 119 z 4 maja 2016 r., str. 1; dalej: *RODO*.

W trakcie kontroli stwierdzono jednak istotne nieprawidłowości w realizacji zadań i obowiązków w zakresie ochrony danych osobowych pacjentów, tj.:

- obowiązujący Statut Szpitala oraz Regulamin Organizacyjny Szpitala nie zostały dostosowane do zmian organizacyjnych wynikających z wejścia w życie rozporządzenia RODO,
- od 25 maja do 10 lipca 2018 r. w Szpitalu nie był prowadzony *rejestr czynności przetwarzania danych,* a do 4 września 2018 r. nie zostały zaktualizowane PB i IZSI,
- niezorganizowanie szkoleń związanych z wejściem w życie przepisów RODO, w tym dotyczących bezpieczeństwa danych, dla całego personelu Szpitala uczestniczącego w procesie przetwarzania danych osobowych (przeszkolono tylko 5,7%),
- stosowanie u pacjentów opasek identyfikacyjnych zawierających dane osobowe, czym naruszono art. 36 ust. 5 ustawy o działalności leczniczej, a ponadto umieszczanie ich na łóżkach,
- w dwóch z 50 zgłoszeń usterek oprogramowania przekazanych dostawcy oprogramowania zamieszczono dane osobowe pacjentów,
- dostęp do systemu operacyjnego zainstalowanego na wszystkich 20 poddanych analizie komputerach użytkowanych przez personel medyczny wymagał podania tego samego loginu i hasła,
- posiadaniu uprawnień administratora w systemie operacyjnym przez wszystkich objętych próbą 30 użytkowników niebędących administratorami tych systemów.

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

OBSZAR

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

Opis stanu faktycznego

1.1. Zarządzeniem nr 13/2018 Dyrektora Szpitala z dnia 25 maja 2018 r. w sprawie wyznaczenia inspektora danych osobowych powołano IOD. W § 4 wskazano m.in., że IOD włączony jest we wszystkie sprawy dotyczące ochrony danych osobowych, a także ma dostęp do nich i operacji przetwarzania. IOD zgodnie z § 5 nie otrzymał instrukcji dotyczących swoich zadań, podlega bezpośrednio najwyższemu kierownictwu oraz nie jest odwoływalny ani karany za wypełnienie swoich zadań, co było zgodne z postanowieniami art. 38 ust. 3 rozporządzenia RODO. W Zarządzeniu wskazano, że IOD nie może wykonywać innych zadań jeżeli mogą one powodować konflikt interesów przy realizacji obowiązków IOD. Powyższa zapisy zawarto również w Polityce Bezpieczeństwa (*dalej: PB*) z 3 września 2018 r.

Do 24 maja 2018 r. funkcję Administratora Bezpieczeństwa Informacji pełnił Kierownik Działu Informatyki. IOD był zatrudniony w Szpitalu również na stanowisku Radcy Prawnego. Jak wyjaśnił Dyrektor Szpitala czas pracy został podzielony 0,75 etatu jako Radca Prawny i 0,25 jako IOD, a od 1 listopada 2018 r. odpowiednio 0,4 i 0,6 etatu. Zgodnie z wymogiem określonym w art. 37 ust. 7 rozporządzenia RODO, dane IOD oraz sposób i formę kontaktu udostępniono na stronie internetowej Szpitala[5].

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

[5] http://www.ssz.tar.pl/strefa_pacjenta/przetwarzanie_danych.html

Szpital 24 lipca 2018 r. zawiadomił Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu na stanowisko IOD, co było zgodne z art. 158 ust. 5 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[6].
Obowiązujący Statut Szpitala oraz Regulamin Organizacyjny Szpitala nie zawierał żadnych informacji dotyczących IOD.
Powołany przez Dyrektora Szpitala IOD zgodnie z wymogami art. 37 ust. 5 rozporządzenia RODO posiadał należyte przygotowanie i kwalifikacje zawodowe do pełnienia swojej funkcji, tj. m.in. ukończył kurs na IOD[7].
Dyrektor Szpitala na stronie internetowej Szpitala opublikował *Klauzulę informacyjną o przetwarzaniu danych osobowych*, w której wskazano m.in. kto jest Administratorem Danych Osobowych oraz Inspektorem Ochrony Danych wraz ze wskazaniem adresu, adresu e-mail oraz numeru telefonicznego i numeru faksu.

(akta kontroli str. 5-47, 184, 313-314, 464-470)

1.2. Przed wejściem w życie rozporządzenia RODO w Szpitalu funkcjonowały:

- PB z 9 lutego 2015 r., w której wskazano m.in.: organizację przetwarzania danych osobowych, Infrastrukturę przetwarzania danych osobowych, strukturę zbiorów danych, sposób przepływu danych w systemie i zakres przetwarzania danych, strategię zabezpieczenia danych osobowych.
- Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych z 2 marca 2015 r.

(akta kontroli str. 96-130)

Po wejściu w życie rozporządzenia RODO, IOD zaktualizował PB i Instrukcję Zarządzania Systemem Informatycznym służącą do przetwarzania danych osobowych (dalej: *IZSI*). Ich zaktualizowane wersje[8] zostały sprawdzone i 4 września 2018 r. zatwierdzone przez Dyrektora Szpitala. W PB zmiany polegały m.in. na dodaniu zapisów dotyczących zarządzania przypadkami naruszeń ochrony danych osobowych (incydentów), a także zgłaszania takich naruszeń oraz zapewnienia bezpieczeństwa danych na każdym etapie ich przetwarzania[9].
Zarówno Polityka jak i Instrukcja zostały dostosowane do zapisów rozporządzenia RODO. W dokumentach tych nie wskazano konieczności opracowania dodatkowych reguł i procedur uszczegóławiających je.

(akta kontroli str. 48-87)

Regulacje wewnętrzne (PB oraz IZSI) udostępniono pracownikom 3 września 2018 r. poprzez umieszczenie ich w Intranecie.
Dyrektor Szpitala jak i IOD wyjaśnił, że w taki właśnie sposób personel Szpitala został zapoznany z tą dokumentacją i był on komunikowany pracownikom Szpitala, na każdym organizowanym szkoleniu jak również na cyklicznych spotkaniach kadry kierowników, którzy przekazywali informację swoim podwładnym. Ponadto pracownicy korzystają często z wewnętrznego intranetu Szpitala, gdyż jest to jeden z głównych sposobów komunikowania się z grupą prawie 900 osób pracujących cały tydzień w systemie 24-godzinnym.

(akta kontroli str. 313-314, 464-470, 487-488, 513-515)

[6] Dz. U. poz. 1000, ze zm.
[7] W okresie od 7 do 10 maja 2018 r. uczestniczył w kursie dla Inspektora Ochrony Danych co potwierdzono certyfikatem nr 34/05/2018/IOD.
[8] Aktualizacja z 3 września 2018 r.
[9] Tj. ich zbierania, utrwalania, organizowania, porządkowania, przechowywania, adaptowania lub modyfikowania, pobierania, przeglądania, wykorzystywania, ujawniania poprzez przesyłanie, rozpowszechniania lub innego rodzaju udostępnienia, dopasowywania lub łączenia, ograniczania, usuwania lub niszczenia.

Jednym z elementów Systemu Zarządzania Jakością, była funkcjonująca instrukcja pn. Zasady udostępniania dokumentacji medycznej[10], która opisywała w jaki sposób należy udostępniać dokumentację medyczną pacjentom, przedstawicielom ustawowym lub osobom upoważnionych za życia pacjenta i pracownikom Szpitala, wraz ze sposobem udostępniania tej dokumentacji.

(akta kontroli str. 201-204)

Dyrektor Szpitala 14 maja 2018 r. zatwierdził Księgę Zarządzania Bezpieczeństwem Informacji[11], która zawierała 10 procedur dotyczących bezpieczeństwa informacji, systemów informatycznych oraz zarządzaniem aktywami informatycznymi czy incydentami bezpieczeństwa informacji. Procedury ujęto w Księdze Zarządzania Bezpieczeństwem Informacji.

(akta kontroli str. 131-185, 444-458)

Szpital zawierając umowy o pracę z osobami zatrudnianymi zobowiązywał ich do zachowania w ścisłej tajemnicy wszelkich informacji zawodowych i organizacyjnych pracodawcy. W kartach opisu stanowiska wskazywano na odpowiedzialność za przestrzeganie tajemnicy służbowej oraz wszelkich poufnych informacji, o których pracownik dowiedział się w związku z wykonywaniem powierzonych mu obowiązków pracowniczych, a których ujawnienie mogłoby narazić pracodawcę na szkodę.

(akta kontroli str. 489-503)

1.3. Wypełniając obowiązek wynikający z art. 30 rozporządzenia RODO w Szpitalu prowadzono, w wymaganej formie, zatwierdzony przez Dyrektora Szpitala *rejestr czynności przetwarzania danych*, którego szczegóły opisano w PB. Obok formy papierowej była forma elektroniczna (Word) tego rejestru. Rejestr prowadzono od 10 lipca 2018 r. i wg stanu na 28 lutego 2019 r. liczył on sześć pozycji, zawierających wszystkie dane wymagane art. 30 ust. 1 rozporządzenia RODO.

(akta kontroli str. 48-76, 88-95

1.4. Stosownie do art. 32 rozporządzenia RODO, 5 marca 2018 r. sporządzono dokument pn. *Plan postępowania z ryzykiem*, w którym m.in. zestawiono wskaźniki i działania, który po weryfikacji ostatecznie 18 kwietnia 2018 r. zatwierdził Dyrektor Szpitala. Przeprowadzono analizę procesów przetwarzania danych osobowych pacjentów Szpitala, na podstawie której zidentyfikowano 18 ryzyk[12], przypisując im odpowiednie skutki[13] oraz określając jego właściciela.
Dla wszystkich ryzyk jako rekomendowany typ reakcji na ich wystąpienie[14] wskazano *Redukcja* dla jednego ryzyka i dla pozostałych *Akceptacja*. Dla każdego ryzyka określono działania, które należy wprowadzić celem ograniczenia jego wystąpienia. Jednym ze zidentyfikowanych ryzyk wskazanych w planie był dostęp do danych pacjentów osób nieuprawnionych. Ryzyko określono jako małe o bardzo wysokich skutkach z proponowanym rodzajem reakcji w postaci *Redukcji ryzyka*. Celem ograniczenia powstania tego ryzyka wskazano trzy działania zaradcze tj.:

- odbieranie uprawnień osobom, które utraciły prawo dostępu do tych danych,
- zabezpieczenie dokumentacji papierowej przed utratą i uszkodzeniem, zniszczeniem poprzez korzystanie z zamykanych szafek, pomieszczeń, przenoszenie dokumentacji przez przeszkolonych pracowników,
- zgłaszanie problemów związanych z dokumentowaniem procesu leczenia w systemie informatycznym.

[10] Nr KPO-02/VIII obowiązujące od 24 kwietnia 2017 r.
[11] Z terminem obowiązywania od 25 maja 2018 r.
[12] 17 ryzyk średnich i jedno ryzyko niskie. Nie zidentyfikowano ryzyk wysokich.
[13] Dwa bardzo wysokie i 15 wysokich.
[14] Rodzaje reakcji na ryzyko wskazane w Planie to: eliminacja, redukcja, przeniesienie oraz akceptacja.

Innym wskazanym ryzykiem o poziomie średnim z bardzo wysokim skutkiem było niewylogowanie się z systemu informatycznego po zakończeniu pracy/odejście od stanowiska z proponowanym rodzajem reakcji w postaci jego *Redukcji.* Jako działanie ograniczające możliwość wystąpienia tego ryzyka wskazano przeprowadzanie szkoleń stanowiskowych, zwiększenie poziomu świadomości użytkowników oraz bieżący nadzór kierowników działów.

(akta kontroli str. 135-144, 186-199, 315-325)

1.5. W obowiązującym Planie postępowania z ryzykiem, zaktualizowanym 18 kwietnia 2018 r., w zestawieniu wskaźników i działań dokonano opisu skutków dla ochrony danych, o której mowa w art. 35 rozporządzenia RODO. Ocena zawierała część danych wymaganych art. 35 ust. 7 RODO. Wystąpienie żadnego z ryzyk nie oszacowano jako wysokie, a w dokumencie brak było oceny, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów oraz oceny ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1. Ocena ta była fakultatywna i taka pojedyncza (bieżąca) ocena dotyczyć powinna operacji wiążących się z wysokim ryzykiem. Również Grupa Robocza Art. 29 ds. Ochrony Danych[15] zdecydowanie zalecała dokonanie DPIA dla operacji przetwarzania już trwających przed 25 maja 2018 r.[16] oraz w przypadkach, gdy nie jest jasne, czy wymagana jest DPIA. Uznano, bowiem, że jest ona *przydatnym narzędziem, które może pomóc administratorom danych w zapewnieniu zgodności z prawem ochrony danych*, chociaż Prezes UODO w komunikacie[17] 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.

(akta kontroli str. 186-199, 315-325, 487-488, 513-515)

1.6. Jednym z zadań IOD, w myśl art. 39 ust. 1 lit. b rozporządzenia RODO, jest prowadzenie szkoleń personelu uczestniczącego w operacjach przetwarzania danych. Po wejściu w życie przepisów rozporządzenia RODO IOD pierwsze szkolenie zorganizował i przeprowadził dopiero 18 czerwca 2018 r., w którym udział wzięło łącznie 25 osób (głównie sekretarki medyczne). Na 2019 r. w zatwierdzonym planie szkoleń wskazano osiem szkoleń w okresie od lutego do września (po jednym w miesiącu) dla poszczególnych grup zawodowych w temacie *Ochrona danych osobowych wynikająca z przepisów rozporządzenia RODO*. Zgodnie z planem 26 lutego 2019 r. przeprowadzono szkolenie dla Pielęgniarek Oddziałowych, w którym udział wzięło 18 osób. W okresie od 25 maja 2018 r. do 26 lutego 2019 r. (9 miesięcy) łącznie w dwóch szkoleniach udział wzięło jedynie 43 z 755[18] (5,7%) pracowników Szpitala. Na stronie wewnętrznej Szpitala tj. w Intranecie zamieszczono prezentację szkoleniową zawierającą podstawowe informacje na temat rozporządzenia RODO, z którą każdy pracownik mógł się zapoznać. Prezentacja zawierała m.in. podstawy, zasady, bezpieczeństwo, rejestrowanie

[15] 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.

[16] 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

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

[18] Stan na 28 lutego 2019 r.

czynności przetwarzania danych oraz naruszenie bezpieczeństwa ochrony danych i związaną z tym odpowiedzialnością.

(akta kontroli str. 48-76, 313-314, 464-470, 473-479)

1.7. Szpital nie stosował kodeksu dobrych praktyk i nie uczestniczył w tworzeniu branżowego kodeksu.

Jak wyjaśnił Dyrektor Szpitala do chwili obecnej resort zdrowia nie opracował ani nie zarekomendował do stosowania w podmiotach medycznych branżowego *Kodeksu/Kodeksu dobrych praktyk*. Szpital od półtora roku monitoruje proces tworzenia branżowego kodeksu przez stronę społeczną. Polska Federacja Szpitali (w imieniu własnym i pięciu wiodących organizacji branżowych) złożyła 13 listopada 2018 r. do Urzędu Ochrony Danych Osobowych 22 wersję projektu Kodeksu - celem jego zatwierdzenia. Obecnie trwają prace nad jego kolejną wersją. W dniu 27 lutego 2019 r. IOD uczestniczył w ogólnopolskiej konferencji *RODO w zdrowiu – gdzie jesteśmy i dokąd zmierzamy* (II edycja), podczas której m.in. zaprezentowano wnioski z wdrażania RODO w sektorze ochrony zdrowia oraz proces akceptacji złożonego kodeksu branżowego. Przewodnik *RODO w zdrowiu* prezentuje rozwiązania, które personel Szpitala stosuje w codziennej pracy.

Jednocześnie Dyrektor Szpitala wyjaśnił, że Szpital od kilku lat stosuje w praktyce procedury mające na celu ochronę danych osobowych. Zostały one wprowadzone (2008 r.) w ramach Polityki bezpieczeństwa – Regulaminu ochrony danych osobowych oraz (2014 r.) Systemu Zarządzania Bezpieczeństwem Informacji[19]. Procedury te w znacznej mierze pokrywają się z proponowanymi rozwiązaniami zawartymi w projekcie branżowego *Kodeksu dobrych praktyk, a* kilka lat ich obowiązywania sprawia, iż dla personelu Szpitala jest to rutynowe zachowanie.

(akta kontroli str. 313-314, 464-470)

Stwierdzone nieprawidłowości

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

1. Obowiązujący Statut Szpitala[20] oraz Regulamin Organizacyjny Szpitala nie zawierał żadnych postanowień dotyczących IOD. Oba dokumenty nie zostały dostosowane do zmian organizacyjnych wynikających z wejścia w życie rozporządzenia RODO.

   Jak wyjaśnił Dyrektor Szpitala, ostatnia zmiana zapisów Statutu Szpitala miała miejsce 30 listopada 2017 r.[21], a więc jeszcze przed 25 maja 2018 r. od kiedy zastosowanie mają zapisy rozporządzenia RODO, a zapisy dotyczące IOD zostaną wprowadzone do Statutu Szpitala przy najbliższej zmianie Statutu. Wszelkie zmiany w Statucie dokonywane są poprzez Radę Miasta Tarnowa. Praktyką jest wprowadzanie równocześnie kilku zmian, aby prace Rady przebiegały efektywnie. Wprowadzenie zapisów o IOD do Regulaminu organizacyjnego Szpitala, możliwe będzie dopiero po wcześniejszym wprowadzeniu przedmiotowych zapisów do Statutu Szpitala.

   (akta kontroli str. 5-47, 313-314, 464-470)

2. Od 25 maja do 10 lipca 2018 r. w Szpitalu nie był prowadzony *rejestr czynności przetwarzania danych,* a do 4 września 2018 r. nie zostały zaktualizowane PB i IZSI. Nieprowadzenie rejestru i niezaktualizowanie ww. dokumentów stanowiło naruszenie przepisów, odpowiednio art. 30 oraz art. 24 ust. 1 i 2 RODO, zgodnie z którymi do obowiązków ADO, należy m.in. prowadzenie rejestru oraz

[19] ISO/IEC 27001:2013.

[20] Tekst jednolity styczeń 2018 r.

[21] Uchwałą Nr XLVI/496/2017 Rady Miejskiej w Tarnowie zmieniającą uchwałę w sprawie nadania Statutu Specjalistycznemu Szpitalowi im. E. Szczeklika w Tarnowie.

poddawanie przeglądom i aktualizacji przyjętych polityk ochrony danych i regulacji wewnętrznych w tym zakresie.
Jak wyjaśnił Dyrektor, w Szpitalu obowiązuje PB która została wprowadzona w 2009 r., następnie zmieniana w 2011 r. oraz w 2015 r. Praca nad aktualizacją Polityki Bezpieczeństwa (z września 2018 r.) pod kątem przepisów RODO była procesem złożonym i wymagającym. Szpital na przestrzeni ponad 10 lat obowiązywania ww. Polityki Bezpieczeństwa wypracował pewne rozwiązania i standardy w oparciu o uzyskane w tym okresie doświadczenia w codziennej pracy. Przyjęta została strategia, iż istniejąca dokumentacja w zakresie ochrony danych osobowych zostanie dostosowana do przepisów RODO. Za priorytet uznano, aby dokumentacja była maksymalnie dostosowana do specyfiki pracy Szpitala uwzględniając charakter, zakres, kontekst i cele przetwarzania z wykorzystaniem dotychczasowych doświadczeń.
Ponadto – według Dyrektora – Szpital w pierwszej kolejności priorytetowo potraktował faktyczne zabezpieczenia danych osobowych, choćby przetwarzanych w formie elektronicznej poprzez budowę nowej serwerowni.

(akta kontroli str. 48-87, 88-95)

3. IOD nie wywiązał się w pełni z zadania dot. prowadzenia szkoleń personelu uczestniczącego w operacjach przetwarzania danych, wynikającego z art. 39 ust. 1 lit. b rozporządzenia RODO. Po wejściu w życie tych przepisów (25 maja 2018 r.), pomiędzy 18 czerwca 2018 r. a 26 lutego 2019 r., jedynie 43 z 755[22] (5,7%) pracowników Szpitala zostało objętych takim szkoleniem. Ponadto 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 z § 20 ust. 2 pkt 6 rozporządzenia KRI.
   Jak wyjaśnił IOD szkolenia personelu są realizowane etapowo wg ustalonego harmonogramu szkoleń, a specyfika działalności podmiotu leczniczego jakim jest Szpital znacząco utrudnia przeszkolenie całej kadry w jednym ustalonym terminie. Proces ten wymaga realizacji etapami. Dyrektor Szpitala dodatkowo wskazał, że personel Szpitala od kilku lat stosuje w praktyce zachowania służące ochronie danych osobowych. Po wejściu w życie rozporządzenia RODO Inspektor ochrony danych przeszkolił przede wszystkim osoby mające pierwszy bezpośredni kontakt z pacjentami tj. rejestratorki medyczne i sekretarki medyczne (izba przyjęć, poradnie, oddziały szpitalne). Było to konieczne z uwagi na nowe irracjonalne zachowania pacjentów - pod wpływem medialnego nagłośnienia dyrektywy RODO.

   (akta kontroli str. 48-76, 313-314, 464-470, 473-479)

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

OCENA CZĄSTKOWA

Szpital wywiązał się z obowiązku sporządzenia w terminie procedur dotyczących ochrony danych osobowych i przeprowadzenia analizy procesów przetwarzania danych. W sposób właściwy wywiązano się z obowiązku powołania IOD i terminowego zgłoszenia tego faktu Prezesowi Urzędu Ochrony Danych

[22] Stan na 14 lutego 2019 r.

Osobowych. Jednocześnie stwierdzono, że prowadzenie rejestru czynności przetwarzania danych osobowych rozpoczęto ponad miesiąc od wejścia w życie rozporządzenia RODO, natomiast PB jak i Instrukcję dostosowano do przepisów tego rozporządzenia dopiero po czterech. Negatywnie należy ocenić przeszkolenie tylko 5,7% personelu Szpitala w zakresie obowiązujących regulacji dotyczących ochrony danych osobowych do lutego 2019 r., biorąc pod uwagę 25. miesięczny okres *vacatio legis* oraz prawie roczny okres obowiązywania tego rozporządzenia.

Zdaniem NIK za ryzyko dla bezpieczeństwa w zakresie ochrony danych, które może skutkować nieprawidłowościami w przyszłości (jeżeli Szpital nie podejmie odpowiednich działań) należy uznać ww. niesatysfakcjonujący, z punktu widzenia zadań IOD określonych w art. 39 ust. 1 lit. b) RODO, wskaźnik przeszkolonych pracowników Szpitala. Cykliczny system szkoleń z zakresu ochrony danych osobowych, w tym RODO dla personelu medycznego Szpitala, w szczególności tzw. szkoleń przypominających, sprzyjać będzie minimalizacji ryzyk dla bezpiecznego przetwarzania ww. danych.

OBSZAR

2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych

Opis stanu faktycznego

2.1. Przeprowadzone oględziny trzech funkcjonujących w Szpitalu rejestracji[23] wykazały, że w celu ochrony danych osobowych pacjentów funkcjonowały poniżej wymienione rozwiązania.

- Dwie rejestracje[24] zorganizowano tak, aby nie były możliwy wgląd w dokumenty osoby z sąsiedniego okienka.
- Jedną z rejestracji[25] umiejscowiono w osobnym pomieszczeniu z dwoma stanowiskami. Pomiędzy stanowiskami nie zamontowano przesłon ich oddzielających. W trakcie oględzin nie stwierdzono by rejestracja pacjentów odbywała się bez okazania dowodu osobistego.
- W pobliżu wszystkich rejestracji poza informacją o treści, że *przy okienku rejestracji może przebywać tylko jedna osoba, a rejestracja odbywa się po okazaniu dowodu osobistego,* na tablicach znajdowały się również informacje o prawach pacjenta, a na podłodze wyznaczone były strefy za pomocą przyklejonych taśm, których to pacjenci w trakcie oględzin przestrzegali.
- Przy każdej rejestracji umieszczono klauzule informacyjne o przetwarzaniu danych osobowych.
- Pracownicy rejestracji nie wypowiadali na głos informacji zawierających dane osobowe, przekazując jedynie dane dotyczące dalszego procesu postępowania po zarejestrowaniu się do danej poradni lub gabinetu.
- Dokumenty medyczne zarejestrowanych i rejestrujących się pacjentów nie znajdowały się w obrębie ich wzroku.
- Wszystkie cztery komputery znajdujące się w rejestracjach były ustawione w sposób uniemożliwiający wgląd w treści na nich wyświetlane osobom rejestrującym się.
- W dniu umówionej wizyty pacjenci zobowiązani byli do zgłoszenia się do rejestracji celem pobrania specjalnie przygotowanego numeru (zalaminowane

[23] Jedna rejestracja z dwoma stanowiskami znajdowała się w pomieszczeniu, do którego można było wejść z holu. Dwie rejestracje zorganizowane były w postaci okienek na korytarzu.
[24] Do poradni Chirurgii Urazowej i Ortopedycznej oraz do poradni RTG.
[25] Do poradni: Dermatologicznej, Kardiologicznej, Chirurgii Ogólnej, Chirurgii Naczyniowej, Gruźlicy i Chorób Płuc.

kolorowe karty), który identyfikował pacjenta do wejścia na umówioną wizytę u lekarza. W przypadku pracowni RTG rejestracja odbywała się bez uzgadniania daty i godziny przyjęcia.

Jak wyjaśnił Dyrektor w rejestracji znajdującej się w osobnym pomieszczeniu znajdują się dwa stanowiska pracy. Jedno z nich służy do obsługi pacjentów zgłaszających się osobiście do ustalenia/zmiany terminu wizyty, a drugie służy do rejestracji telefonicznej i bieżącej obsługi poradni tj. przygotowywania kart pacjentów, segregowania wyników badań, przygotowywania planów wizyt na dany dzień oraz archiwizowania dokumentacji.

(akta kontroli str. 263-265, 468-469, 471-472, 504-505)

Wywoływanie pacjentów do gabinetów poradni objętych kontrolą[26] odbywało się w sposób gwarantujący im anonimowość, tj. wywoływania kolejnych numerów nadanych w rejestracji.

We wszystkich objętych oględzinami gabinetach, dokumentację pacjentów przechowywano we właściwy sposób, tj. pacjent wchodzący do gabinetu nie miał możliwości zapoznania się z danymi osobowymi innych osób oczekujących w kolejce lub tych, którzy odbyli już wizytę. Ponadto w trakcie oględzin, nie zaobserwowano aby którykolwiek gabinet został pozostawiony bez opieki oraz nie stwierdzono przypadków pozostawienia klucza w drzwiach i opuszczenia przez personel gabinetu poradni.

(akta kontroli str. 272-273)

Przeprowadzone oględziny dyżurek pielęgniarskich, sal chorych oraz gabinetów lekarskich na trzech oddziałach szpitalnych[27] wykazały m.in., że:

- na oddziałach znajdowało się łącznie 31 sal chorych łącznie z 82 łóżkami (dodatkowo było siedem dostawek),
- wszyscy pacjenci posiadali umieszczone na nadgarstku wydrukowane opaski informacyjne zawierające kod kreskowy, nr karty głównej[28], nazwę Szpitala oraz ręcznie napisane imię i nazwisko chorego[29]; oględziny na trzech innych oddziałach[30] wykazały, że losowo wybranych 30 pacjentów posiadało opaski, na których długopisem było wpisane, trudne do odczytania ich imię i nazwisko; te same dane umieszczone były na łóżkach pacjentów,
- na oddziałach nie umieszczano kart przy/na łóżkach pacjentów,
- ruch chorych[31] prowadzony był w dyżurkach pielęgniarskich w miejscach niewidocznych dla osób postronnych,
- w dyżurkach pielęgniarskich podręczną dokumentację przechowywano w zamykanych na klucz gablotach lub szafkach,
- dyżurki pielęgniarskie wyposażono w sześć komputerów, z których pięć było uruchomionych, w tym na czterech pracowały pielęgniarki, a jeden zablokowany,
- na oddziałach znajdowało się trzy gabinety lekarskie, wyposażone w 16 komputerów, z których na 11 pracowali lekarze, a pozostałe były zablokowane,

[26] Chirurgii Naczyniowej, Dermatologicznej oraz Urazowo-Ortopedycznej.

[27] Oględziny przeprowadzono na Oddziale: Chirurgii Urazowej i Ortopedii, Pulmonologii oraz Dermatologii.

[28] Spseudonimizowane dane, możliwe do odczytania za pomocą oprogramowania zainstalowanego na tabletach znajdujących się w dyżurkach szpitalnych.

[29] Dane w postaci imienia i nazwiska umieszczano na opasce na podstawie wyrażonej zgodny pacjenta udzielanej pisemnie przy przyjmowaniu chorego Szpitala. (Zarządzenie nr 37/2012 Dyrektora Specjalistycznego Szpitala im. E. Szczeklika w Tarnowie z dnia 4 grudnia 2012 r. w sprawie zaopatrywania pacjentów Szpitala w znaki identyfikacyjne.

[30] Chorób Wewnętrznych i Nefrologii z Ośrodkiem Dializ, Rehabilitacji Ogólnej i Kardiologicznej oraz Ginekologiczno-Położniczym.

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

– dokumentacja medyczna pacjentów w gabinetach lekarskich przechowywana była szafach zamykanych na klucz.

(akta kontroli str. 266-271, 313, 326-337, 464-467, 528-530)

Ponadto w ramach przeprowadzonych oględzin stwierdzono, że na dwóch[32] z trzech oddziałów funkcjonuje monitoring wizyjny. Umieszczenie kamer nie pozwalało na wgląd w dokumenty osób, okazywane podczas procesu rejestracji. Umiejscowienie kamer uniemożliwiało wgląd w akta czy jakąkolwiek możliwość odczytu danych osobowych pacjentów. Informacja o funkcjonującym monitoringu na terenie Szpitala znajdowała się na drzwiach wejściowych do budynków zajmowanych przez Szpital. Monitoring na tych oddziałach został zainstalowany przed wejściem w życie rozporządzenia RODO, a personel szpitalny poinformowano o kwestiach związanych z monitoringiem wprowadzając Aneksem nr 11 z 24 października 2018 r. zapisy do Regulaminu pracy, w którym m.in. wskazano, że nagrania obrazu przetwarzane są wyłącznie do celów, dla których zostały zebrane[33], a dostęp do niego będą mieć upoważnieni pracownicy Działu Informatyki.

(akta kontroli str. 266-271, 274-277)

2.2. Według stanu na 14 lutego 2019 r. personel działów administracyjnych[34] Szpitala liczył 55 osób. Analiza, którą objęto 30 osób wykazała, że:

– 13 osób nie posiadało dostępu do systemu AMMS[35], co wynikało z ich zakresów obowiązków (nie realizowali oni zadań wymagających dostępu do danych medycznych pacjentów Szpitala);
– 10 posiadło nadane im uprawnienia w tym systemie, które pozwalały im na dostęp do danych medycznych niezbędny z punktu widzenia realizowanych przez nich zadań (zatrudnieni w Dziale Rozliczeń, Dziale Organizacji i Nadzoru oraz Pełnomocnik ds. Jakości);
– siedem osób posiadło ograniczony dostęp do danych w systemie AMMS (jedna w zakresie wyceny badań i procedur, dwie w zakresie zakażeń szpitalnym oraz kart zgłoszeń zakażeń szpitalnych oraz cztery w zakresie apteczki/apteki), co też było zgodne z zakresem wykonywanej pracy.

Osoby posiadające uprawnienia do pracy w systemie AMMS posiadały stosowne upoważnienia ADO do przetwarzania danych osobowych.

(akta kontroli str. 16-35, 262, 293-303)

2.3. Analiza przeprowadzona na próbie 30 (z 356) pielęgniarek i położnych zatrudnionych w Szpitalu[36] wykazała, że w ich aktach osobowych znajdowały się upoważnienia do przetwarzania danych osobowych a 29 z nich posiadało dostęp do AMMS wynikający z ich zakresów obowiązków. W badanej próbie nie stwierdzono przypadków posiadania przez pielęgniarki lub położne uprawnień w systemie AMMS do innych oddziałów niż te, w których były zatrudnione. W jednym przypadku położna była zatrudniona na bloku operacyjnym i nie posiadała uprawnień dostępowych do systemu.

(akta kontroli str. 75, 218-234, 442, 458-463)

Zatrudnieni w Szpitalu pracownicy gospodarczy pełnili funkcje przypisane salowym lub sanitariuszom. W ramach wewnętrznego transportu chorych wraz z pacjentem

[32] Oddział Pulmonologii i Chirurgii Urazowej.
[33] Zapewnienie bezpieczeństwa pracownikom i pacjentom, ochrony mienia oraz zachowania tajemnicy informacji.
[34] Dział Finansowo-Księgowy, Dział Statystyki Medycznej i Realizacji Świadczeń, Działa Zaopatrzenia i Magazynów, Dział Zamówień Publicznych, Dział Techniczny (bez Sekcji), Dział Kadr i Szkoleń, Dział Organizacji i Nadzoru, Dział Informatyki oraz stanowiska samodzielne w Administracji Szpitala.
[35] System typu HIS (Hospital Information System – rodzaj oprogramowania do obsługi ruchu pacjentów wewnątrz podmiotu leczniczego).
[36] Zatrudnionych na stanowiskach z grupy: pielęgniarki, położne. Dane wg. stanu na 14 lutego 2019 r.

pracownicy ci przewozili papierowe zlecenia na wykonywanie badań lub inną dokumentację. Na taki rodzaj pracy posiadali oni upoważnienia do przetwarzania danych osobowych w zakresie transportu dokumentacji – danych osobowych pomiędzy komórkami organizacyjnymi oraz wykonywania kserokopii dokumentacji na zlecenie komórek organizacyjnych. W karcie opisu stanowiska pracy wskazano, że do zadań tych osób należało m.in. dostarczanie we wskazane miejsca wszystkich pism do/z oddziałów i innych komórek Szpitala oraz wykonywanie innych zadań zleconych przez przełożonego, zgodnych z przepisami Kodeksu Pracy, mających związek z wykonywaną pracą. W karcie wskazano również, że pracownik ponosi odpowiedzialność m.in. za przestrzeganie tajemnicy ochrony danych osobowych i praw pacjenta.

(akta kontroli str. 293, 459-463, 516-527)

2.4. W okresie od 25 maja 2018 r. do 14 lutego 2019 r. Szpital rozwiązał stosunek pracy z 23 osobami, którzy w okresie zatrudnienia posiadali dostęp do systemów informatycznych, w tym systemu AMMS. Przeprowadzona analiza terminu odebrania uprawnień ww. osobom wykazała, że:

- w dziewięciu przypadkach dostęp do systemu AMMS zablokowano przed lub w dniu rozwiązania stosunku pracy (pielęgniarki),
- w ośmiu przypadkach dostępu do systemu nie zablokowano (lekarze, zmiana formy zatrudnienia na kontrakt),
- sześciu osobom konto w ww. systemie zablokowano w okresie do ośmiu dni po zakończeniu zatrudnienia[37] (pielęgniarki).

(akta kontroli str. 213-216, 293-302, 468-469, 471-472, 504-505)

Według stanu na 14 lutego 2019 r. 33 osoby przebywały na zwolnieniu lekarskim powyżej 32 dni. Nie stwierdzono przypadku, logowania się w tym czasie tych osób do systemu AMMS. Nie stwierdzono również przypadku by dokonywano, w czasie nieobecności tych osób, zmiany hasła dostępu do systemu AMMS[38] dla loginów przez nich użytkowanych.

(akta kontroli str. 303)

2.5. W myśl postanowień umów serwisowych, które obowiązywały w okresie objętym kontrolą[39], Szpital obowiązany był do zgłaszania błędów w działaniu systemu AMMS poprzez – wskazaną w niniejszych umowach - witrynę internetową *Centralnego Help-Desk'u Wykonawcy*. W przypadku trudności z rejestracją zgłoszenia we wskazanej witrynie, Szpital mógł je zrealizować drogą telefoniczną pod wskazanymi w umowach numerami, pocztą elektroniczną lub opcjonalnie faksem.

(akta kontroli str. 338-375)

Przeprowadzone oględziny sposobu przekazania 50 (z 72) zgłoszeń serwisowych[40] związanych z błędami lub wadliwym działaniem systemu informatycznego AMMS wykazały m.in., że w dwóch zgłoszeniach przekazano imię i nazwisko dwóch pacjentów Szpitala.

(akta kontroli str. 235-239, 471-472, 480-486, 487-488)

2.6. Szpital w okresie objętym kontrolą posiadał zawarte 66 umów dotyczących powierzenia przetwarzania danych osobowych, z tego w 50 wystąpił jako podmiot powierzający przetwarzanie danych a w 16 jako podmiot przetwarzający.

(akta kontroli str. 468-469, 471-472, 504-505)

---

[37] Pięć przypadków zablokowania konta od 2 do 5 dni po zakończeniu pracy i jeden przypadek po ośmiu dniach.
[38] System wymusza zmianę hasła co 30 dni.
[39] Umowy: nr 2/WR/2017 z 28 czerwca 2017 r. oraz nr 1/WR/ 2018 z 28 czerwca 2018 r., których przedmiotem było m.in. objęcie nadzorem autorskim oprogramowania aplikacyjnego InfoMedica/AMMS.
[40] Przekazanych przez Szpital w okresie od 25 maja 2018 r. do 18 lutego 2019 r.

Analiza pięciu umów dotyczących powierzenia przetwarzania danych osobowych obowiązujących w okresie objętym kontrolą wykazała m.in. że:

- zawierały one wymagane postanowienia określone w art. 28 ust. 3 rozporządzenia RODO,
- stanowiły integralną część umowy na świadczenie usług zawartej z danym podmiotem zewnętrznym (4) lub były zawierane jako dodatkowe umowy do zawartych wcześniej (1),
- wskazany zakres danych osobowych, jaki został powierzony przez Szpital podmiotowi zewnętrznemu, wynikał z rodzaju usług jakie zgodnie z umową na ich świadczenie miał na rzecz Szpitala realizować wykonawca.

(akta kontroli str. 352-354, 372-375, 390-398, 412-421, 433-443)

Bez względu na formę zatrudnienia lekarzy w Szpitalu[41] posiadali oni upoważnienie do przetwarzania danych w zakresie dotyczącym wykonywania obowiązków.

Jak wyjaśnił Dyrektor Szpitala zgodnie z projektem kodeksu branżowego dla podmiotów medycznych w zakresie ochrony danych osobowych (www.rodowzdrowiu.pl, wersja 22 z 13 listopada 2018 r. – pkt 4.6.3) pomimo przetwarzania danych pacjentów w celach zdrowotnych, podmiot wykonujący działalność leczniczą (w tym przypadku lekarz na kontrakcie) nie może być zakwalifikowany jako odrębny administrator danych tych pacjentów, jeżeli nie jest prawnie obowiązany do prowadzenia, przechowania i udostępniania dokumentacji medycznej, a także zapewnienia ochrony danych zawartych w tej dokumentacji, w sposób określony w art. 24 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta we własnym imieniu i na własny rachunek, lecz działa na rzecz innego podmiotu wykonującego działalność leczniczą (Szpitala). W szczególności ADO pacjentów nie jest osoba wykonująca zawód medyczny, prowadząca jednoosobową działalność gospodarczą, pozostająca w stosunku prawnym z innym podmiotem wykonującym działalność leczniczą, w zakresie w jakim wykonuje swoje zadania w ramach działalności leczniczej prowadzonej przez ten podmiot wykonujący działalność leczniczą w miejscu pobytu pacjenta.

W związku z powyższym lekarze zatrudnieni na kontraktach nie są zobowiązani zawierać ze Szpitalem umów powierzenia przetwarzania danych osobowych.

(akta kontroli str. 75, 444-445, 468-469, 471-472, 504-505)

2.7. W Szpitalu sporządzono Księgę Zarządzania Bezpieczeństwem Informacji będącą zbiorem 10 procedur. Jedną z nich była procedura pn. *Zarządzanie incydentami bezpieczeństwa informacji*, w której określono m.in.: przykładowy wykaz incydentów, które podlegają zgłoszeniu, sposób postępowania w przypadku ich wystąpienia, rejestr wynikający z art. 33 ust. 5 rozporządzenia RODO obowiązek dokumentowania wszystkich naruszeń danych osobowych, ich okoliczności, skutków oraz podjętych działań zaradczych na opracowanym formularzu rejestracji incydentu[42].

(akta kontroli str. 145-148)

Analiza zapisów prowadzonych w rejestrze naruszeń ochrony danych osobowych w 2018 r. wykazała w nim 113 incydentów, podzielonych na osiem kategorii[43]. Żaden nie został zakwalifikowany do zgłoszenia do Prezesa Urzędu Ochrony Danych Osobowych.

(akta kontroli str. 314, 458, 468-470)

---

[41] Umowa o pracę, kontrakt.

[42] Formularz w formie pliku Excel nosił nazwę: *Rejestr incydentów bezpieczeństwa informacji.*

[43] Modyfikacja danych pacjenta (18), zmiany dotyczące zleceń badań (41), zmiany dotyczące zleceń leków (3), cofanie autoryzacji dokumentacji (10), błąd użytkownika uniemożliwiający dostęp do systemu (0), błędy w oprogramowaniu cz. biała (29), błędy w oprogramowaniu cz. szara (0), błędy w module rozliczania z NFZ (12).

2.8. Jednym z elementów Systemu Zarządzania Jakością była procedura pn. *Zasady udostępniania dokumentacji medycznej*[44]., w której wskazano sposób udostępniania dokumentacji medycznej pracownikom Szpitala, pacjentom, ich przedstawicielom ustawowym lub osobom upoważnionym.

(akta kontroli str.201-204)

W okresie od 25 maja 2018 r. do 5 lutego 2019 r. w Szpitalu złożono 860 wniosków o udostępnienie dokumentacji medycznej. Wśród nich odnotowano 858 przypadków dotyczących udostępnienia tej dokumentacji w dwóch przypadkach dokumentacji nie udostępniono w powodu braku upoważnienia. Szczegółową analizą objęto wszystkie 29 przypadków udostępnienia dokumentacji medycznej pacjentów firmom ubezpieczeniowym oraz 30 wybranych przypadków udostępnienia dokumentacji medycznej innej osobie niż pacjent, którego ta dokumentacja dotyczyła[45].

- udostępnianie następowało w Dziale Organizacji i Nadzoru znajdującym się w Administracji Szpitala,
- we wszystkich 30 przypadkach dokumentacja medyczna została udostępniona osobom, które posiadały upoważnienie pacjenta do dostępu do tej dokumentacji na podstawie wniosków o jej udostępnienie określonych w przyjętych regulacjach wewnętrznych Szpitala,
- we wszystkich 29 przypadkach, firmy ubezpieczeniowe, którym udostępniono dokumentację medyczną posiadały upoważnienie pacjenta do dostępu do tej dokumentacji.

Stosownie do art. 26 ust. 1 ustawy o prawach pacjenta w każdej ze spraw znajdowało się upoważnienie do udostępnienia kopii dokumentacji medycznej.

(akta kontroli str. 200)

W okresie od 25 maja 2018 r. do 28 lutego 2019 r. w Szpitalu zarejestrowano łącznie 11 skarg: w tym 10 do końca 2018 r.[46] i jedną w 2019 r.

Przedmiotem jednej[47] ze złożonych skarg było niepoinformowanie skarżącego (członka rodziny) o wypisie pacjenta ze Szpitala. Powodem nieudzielenia takiej informacji był brak upoważnienia do udzielenia informacji o stanie zdrowia pacjenta.

(akta kontroli str. 443)

2.9. Regulacje dotyczące sposobu zarządzania systemem informatycznym, wykorzystywanym do przetwarzania danych osobowych obejmowały swym zakresem zabezpieczenia przed zagrożeniami, w tym: przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem[48]. W dokumentach tych określono m.in. zasady: bezpiecznego użytkowania sprzętu IT, metody i środki uwierzytelniania, procedury związane z ich zarządzaniem i użytkowaniem, określono zasady rozpoczęcia, zawieszenia i zakończenia pracy (zarówno na stacjach roboczych jak i komputerach przenośnych), tworzenia, przechowywania i testowania kopii bezpieczeństwa, likwidacji nośników zawierających kopie, naprawy urządzeń zawierających dane osobowe. Ponadto, określono sposób postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego.

(akta kontroli str. 77-87, 119-130)

W trakcie trwania kontroli w Szpitalu dokonano przeniesienia serwerowi do nowej lokalizacji. Przeprowadzone oględziny serwerowni wykazały, m.in. że właściwie:

[44] Nr KPO-02/VIII obowiązujące od 24 kwietnia 2017 r.
[45] Zapytania sądów, prokuratur, ZUS, KRUS, NFZ, Policji i ABW nie były objęte analizą.
[46] W całym 2018 r. w Szpitalu zrejestrowano 14 skarg.
[47] Skarga z 2 listopada 2018 r.
[48] Zatwierdzonej 25 lutego 2015 r. przez Dyrektora Szpitala. Zaktualizowanej 4 września 2018 r., w zakresie dostosowania do przepisów rozporządzenia RODO.

zabezpieczono dostęp do pomieszczenia serwerowni stosując drzwi metalowe, zamontowano system przeciwpożarowy; w pomieszczeniu umieszczono gaśnicę oraz układ klimatyzacji; w celu zapobiegnięcia zalaniu, wszystkie urządzenia znajdowały się na tzw. podłodze technicznej powyżej poziomu posadzki; na wypadek czasowego zaniku zasilania zastosowano dwa niezależne układy podtrzymujące napięcie UPS zasilane z dwóch niezależnych źródeł zasilania; wszystkie urządzenia informatyczne zamontowano w specjalnie do tego przystosowanych szafach typu RACK. Pobyt w serwerowni w celu przeprowadzenia oględzin został odnotowany w książce wejść/wyjść.

(akta kontroli str. 205-211)

Kopie zapasowe baz danych Szpitala, w myśl przepisów § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI oraz postanowień IZSI, były przechowywane w pomieszczeniu znajdującym się w innej niż serwerownia części budynku.
Jak wskazali uczestniczący w oględzinach pełne kopie zapasowe tworzono codziennie, a dodatkowo co tydzień w odrębnym budynku wykonywana była kopia baz danych na nośniki, które są tam przechowywane.
Jak wskazał Dyrektor Szpitala w okresie objętym kontrolą nie wystąpiły przypadki konieczności odtwarzania baz danych/systemów z kopii zapasowych.

(akta kontroli str. 210-211, 313-314, 464-467)

Przeprowadzone oględziny 30 komputerów stacjonarnych Szpitala, w tym 20 wykorzystywanych na oddziałach Szpitala przez lekarzy, pielęgniarki i położne przy wykonywaniu ich obowiązków służbowych oraz 10 użytkowanych w Administracji Szpitala wykazały m.in., że:

- na wszystkich zainstalowany był program antywirusowy posiadający aktualną wersję bazy sygnatur wirusów,
- w żadnym nie zostały zablokowane porty USB umożliwiając podłączenie do nich nośników pamięci i kopiowanie danych,
- na wszystkich użytkownicy posiadali uprawnienia administratora w systemie operacyjnym,
- we wszystkich 20 komputerach użytkowanych na oddziałach Szpitalnych logowanie do systemu operacyjnego umożliwiał ten sam login i hasło – o długości siedmiu znaków,
- żaden z komputerów poddanych oględzinom nie był zarządzany domenowo;
- wszyscy użytkownicy komputerów w Administracji Szpitala do logowania do systemu operacyjnego używali indywidualnego loginu i hasła,
- 25 wykorzystywane było do przetwarzania danych medycznych w systemie AMMS (20 na Oddziałach Szpitalnych i pięć w Administracji Szpitala),
- trzy komputery posiadały zainstalowany system operacyjny, dla którego wsparcie techniczne ze strony producenta zakończyło się ponad pięć lat temu, z czego dwa wykorzystywano do dostępu do systemu AMMS.

Jak wskazał Kierownik Działu Informatyki komputery przenośne były użytkowane przez Kadrę Zarządzającą Szpitala[49] i z braku miejsca jeden z komputerów był zainstalowany na bloku operacyjnym. Komputery te nie były podłączone do systemu informatycznego szpitala, natomiast komputery przenośne znajdujące się w Dziale Informatyki były podłączone systemu. Jeden z komputerów, który był wykorzystywany poza terenem Szpitala posiadał szyfrowaną partycję.

(akta kontroli str. 239-271, 487-488, 513-515)

[49] Dyrektora Szpitala, Zastępców oraz Kierownika Działu Kadr i Szkoleń. Komputery te nie były podpięte do systemu informatycznego Szpitala.

Jak wyjaśnił Dyrektor Szpitala w Szpitalu użytkowanych jest ok. 330 stanowisk komputerowych z czego 200 komputerów z oprogramowaniem nie posiadającym wsparcia technicznego ze strony producenta zostało wymienione do końca 2017 r. Z pozostałych 125 szt., w roku 2018 wymieniono 50 komputerów, stąd do wymiany pozostało 75 szt. W dwóch miesiącach 2019 r. zostało wymienione kolejne 13 komputerów; między innymi właśnie w Oddziale Kardiologii Inwazyjnej. W ramach projektu *Małopolskiego Systemu Informacji Medycznej* planowany jest zakup celem wymiany kolejnych 33 komputerów. Jest to maksymalna dozwolona ilość, jaką można było ująć w projekcie, stanowiąca max. 25% wydatków w punkcie *Infrastruktura obsługi środowiska IT podmiotu leczniczego*. Wymiana pozostałych 29 szt. nastąpi do końca 2019 r. Nakładane na podmioty lecznicze wymogi związane z informatyzacją nie są powiązane z kierowaniem na ten cel dodatkowych środków przez NFZ. Stąd Szpital od lat sukcesywnie rozbudowuje system informatyczny głównie ze środków zewnętrznych, wspierając częściowo ze środków własnych.

(akta kontroli str. 313, 464-467)

Stwierdzone nieprawidłowości

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

1. W trakcie przeprowadzania oględzin trzech Oddziałów Szpitalnych stwierdzono, że identyfikacja pacjentów odbywała się poprzez umieszczone na nadgarstkach opaski, na których zawarto m.in. imię i nazwisko pacjenta. Jednocześnie te same dane zamieszczono na łóżkach pacjentów.
   Jak wyjaśnił Dyrektor Szpitala podstawą do dodatkowego wpisywania imienia i nazwiska pacjenta na opasce identyfikacyjnej jest Zarządzenie nr 37/2012 Dyrektora Szpitala z 4 grudnia 2012 r. wraz z kolejnymi aneksami. Zgodnie ze wskazanym Zarządzeniem dane osobowe pacjentów mają być wpisywane po wewnętrznej stronie opaski identyfikacyjnej - dostępne jedynie dla personelu medycznego. W sporadycznych przypadkach (pacjenci z ponadnormatywną wagą) dane osobowe są umieszczane na zewnątrz opaski. Każdy pacjent przy przyjęciu wyraża pisemną zgodę na umieszczenie swoich danych na opasce identyfikacyjnej. Wprowadzone rozwiązanie ma na celu zwiększenie bezpieczeństwa pacjenta w przypadku konieczności jego szybkiej identyfikacji. Przy wypisie pacjenta ze Szpitala, po sprawdzeniu zgodności znaku identyfikacyjnego, opaskę wydaje się pacjentowi albo jego opiekunowi prawnemu.

   Zdaniem NIK regulacje wewnętrzne Szpitala wprowadzone cyt. zarządzeniem są sprzeczne z przepisem art. 36 ust. 3 i 5 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej[50], który to nakazuje, aby umieszczone na opaskach dane pozwalające na ustalenie personaliów pacjenta były zapisane w sposób uniemożliwiający identyfikację pacjenta przez osoby nieuprawnione, czyli nie można zamieszczać tam imienia i nazwiska.
   Ponadto zgoda pobierana od każdego pacjenta na umieszczenie imienia i nazwiska na opasce nie może być podstawą do wyłączenia stosowania przez Szpital obowiązków wynikających z art. 36 ust. 3 i 5 ww. ustawy, a więc zakazu umieszczania na nich imienia i nazwiska.
   NIK zwraca uwagę, że dobrowolność takiej zgody jest wątpliwa. W myśl motywu 43 RODO, aby zapewnić dobrowolność, zgoda nie powinna stanowić ważnej podstawy prawnej przetwarzania danych osobowych w szczególnej sytuacji, w której istnieje wyraźny brak równowagi między osobą, której dane dotyczą, a administratorem, w szczególności gdy administrator jest organem publicznym i dlatego jest mało prawdopodobne, by w tej konkretnej sytuacji zgodę

[50] Dz. U. z 2018 poz. 2190 ze zm.

wyrażono dobrowolnie we wszystkich przypadkach. Zgody nie uważa się za dobrowolną, jeżeli od zgody uzależnione jest wykonanie umowy – w tym świadczenie usługi – mimo że do jej wykonania zgoda nie jest niezbędna.

2. W okresie od 25 maja 2018 r. do 14 lutego 2019 r. Szpital rozwiązał stosunek pracy z 23 osobami, z czego sześciu osobom konto w ww. systemie zablokowano w okresie od 2 do 8 dni po zakończeniu zatrudnienia[51] (pielęgniarki) co było niezgodne z § 20 ust. 2 pkt 5 KRI.
   Dyrektor Szpitala wyjaśnił, że wyrejestrowanie uprawnień dostępu do systemu następuje niezwłocznie po ustaniu zatrudnienia. *Wyrejestrowanie z systemu po ustaniu stosunku pracy mogło być spowodowane dniem wolnym od pracy, nieobecnością pracownika przed terminem rozwiązania umowy o pracę czy innymi szczególnymi przypadkami. Niemniej jednak chcę podkreślić, że czynności wyrejestrowania uprawnień do pracy w programie informatycznym są prowadzone bez zbędnej zwłoki.*
   (akta kontroli str. 213-216, 293-302, 468-469, 471-472, 504-505)

3. W dwóch z 50 objętych analizą zgłoszeń usterek oprogramowania przekazanych dostawcy oprogramowania między 25 maja 2018 r. a 18 lutego 2019 r., zamieszczono dane osobowe dwóch pacjentów, tj.: imię, nazwisko. W art. 5 pkt 1 lit. c RODO wskazano zasadę adekwatności i minimalizacji danych.
   Dyrektor Szpitala wyjaśnił, że: w czasie wprowadzania zgłoszeń wymienionych w pytaniu dwóch pacjentów nie było już w szpitalu. Przytoczone zgłoszenia dotyczyły modułu finansowo-księgowego. W pierwszym przypadku system nieprawidłowo przeliczał wartość razem netto np. wystawiając paragon, natomiast w drugim dotyczył zdublowanych paczek do paragonów.
   (akta kontroli str. 235-239, 471-472, 480-486, 487-488, 513-515)

4. W Szpitalu dostęp do systemu operacyjnego zainstalowanego na komputerach użytkowanych przez lekarzy, pielęgniarki i położne (we wszystkich badanych 20 przypadkach) wymagał podania loginu i hasła, przy czym na wszystkich używano tego samego loginu i hasła, co było niezgodne z § 20 ust. 2 pkt. 7 lit. a i c oraz § 21 ust. 2 pkt 3, w związku z § 20 ust. 1 rozporządzenia KRI, w myśl których należy zapewnić środki uniemożliwiające nieautoryzowany dostęp na poziomie systemów operacyjnych oraz wskazujące że bez przyznania indywidualnych loginów użytkownikom, nie będzie możliwa prawidłowa rozliczalność systemów.
   Powyższe działanie uniemożliwiało odebranie uprawnień do logowania w systemie operacyjnym byłym pracownikom ponieważ login i hasło były wspólne i znane wszystkim pracownikom medycznym.
   Dyrektor Szpitala wyjaśnił, że w systemie informatycznym Szpitala (AMMS) zmianę hasła wymuszał system co 30 dni. W systemach operacyjnych służących jako platforma dostępu do systemu Szpitala ze względów konfiguracyjnych hasło nie podlegało zmianie, ale dostęp do systemu operacyjnego nie daje dostępu do danych medycznych/osobowych pacjentów/pracowników. Dostęp ten jest możliwy dopiero po zalogowaniu się do systemu informatycznego Szpitala, który to wymusza zastosowanie odpowiedniego złożonego hasła, zmienianego w ustalonym cyklu i nie zezwala na zastosowanie takiego samego hasła jak poprzednio.
   (akta kontroli str. 240-271, 487-488, 513-515)

5. Na wszystkich 30 komputerach poddanych oględzinom (użytkowanych przez: administrację Szpitala, lekarzy, pielęgniarki i położne) użytkownicy posiadali uprawnienia administratora w systemie operacyjnym, mimo że nie byli

[51] Pięć przypadków zablokowania konta od 2 do 5 dni po zakończeniu pracy i jeden przypadek po ośmiu dniach.

administratorami systemów informatycznych. Pracownikom tym wbrew wymogom § 20 ust. 2 pkt 4 rozporządzenia KRI, umożliwiono instalowanie dowolnego oprogramowania. Praktyka taka została określona także w Załączniku A normy PN-ISO/IEC 27001:2014-12, punkt A.9.2.3 i stanowi, że przydzielanie i wykorzystywanie praw uprzywilejowanego dostępu należy ograniczyć i nadzorować.

Dyrektor Szpitala wyjaśnił, że poziom uprawnień administratora jest niezbędny do: otwierania płyt CD/DVD z obrazami badań diagnostycznych z zewnętrznych jednostek; system szpitalny wymaga praw administratora do poprawnego działania m.in. wydruków, uruchamiania starszych aplikacji systemu szpitalnego, środowisko JAVA do otwierania badań diagnostycznych w systemach szpitalnych. System operacyjny to platforma dla systemu szpitalnego. W systemie operacyjnym nie są przetwarzane dane osobowe - dostęp do systemu operacyjnego nie daje dostępu do danych medycznych/osobowych pacjentów/pracowników. Dopiero po zalogowaniu do systemu szpitalnego następuje dostęp do danych pacjenta.

Odnosząc się do tych wyjaśnień należy mieć na uwadze, że uprawnień administratora wymaga wiele działań podejmowanych przez szkodliwe oprogramowanie malware czy spyware[52], takich jak wyłączenie firewall i ochrony antywirusowej, modyfikacja rejestru, tworzenie plików w katalogach systemowych, uruchamianie i kończenie procesów. NIK zdaje sobie sprawę, że zastosowanie ograniczonych uprawnień użytkowników byłoby zadaniem czasochłonnym, niemniej w porozumieniu z dostawcą oprogramowania jest to wykonalne z korzyścią dla bezpieczeństwa zgromadzonych zasobów informacyjnych. Jednocześnie należy mieć na uwadze, że posiadanie uprawnień administratora w połączeniu z wykorzystywaniem tych samych loginów i haseł przez użytkowników sytemu operacyjnego, aktywnymi portami USB lub napędami optycznymi CD/DVD oraz korzystanie z systemów operacyjnych nieposiadających wsparcia producenta stanowi duże zagrożenie dla bezpieczeństwa przetwarzanych przez Szpital danych. Takie działania stanowią, naruszenie przepisów § 20 ust. 2 pkt 7 rozporządzenia KRI, w myśl których należy zapewnić ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami.

Dyrektor Szpitala wyjaśnił również, że Pkt IV ppkt 2 Instrukcji zarządzania systemem informatycznych służącym do przetwarzania danych osobowych mówi o długości znaków hasła do systemu szpitalnego w którym są przetwarzane dane osobowe, a nie o długości hasła do systemu operacyjnego (platformy). Szpital – jako partner - uczestniczy w realizacji strategicznego projektu informatyzacji placówek medycznych pn. *Małopolski System Informacji Medycznej* (MSIM), współfinansowanego ze środków strukturalnych. W ramach w/w projektu Szpital planuje zakup usług katalogowych, który zastąpi obecną metodę logowania do systemu operacyjnego. Sieć wewnętrzna Szpitala jest odseparowana od sieci Internet przy pomocy urządzenia klasy UTM[53].

Odnosząc się do tych wyjaśnień należy mieć na uwadze, że również w systemie operacyjnym mogą być przetwarzane dane osobowe, poprzez korzystanie z edytorów tekstowych lub kalkulacyjnych, zatem długość znaków hasła *do systemu szpitalnego w którym są przetwarzane dane osobowe* dotyczy również systemu operacyjnego.

(akta kontroli str. 240-271, 487-488, 513-515)

---

[52] Malware – złośliwe oprogramowanie infekujące komputery, Spyware – oprogramowanie szpiegujące.

[53] (ang. *unified threat management*) – wielofunkcyjne zapory sieciowe zintegrowane w postaci jednego urządzenia.

OCENA CZĄSTKOWA

W ocenie NIK w Szpitalu wdrożone zostały właściwe rozwiązania techniczne i organizacyjne, jakkolwiek nie zapewniały one w pełni prawidłowego przetwarzania i ochrony danych osobowych.

W okresie objętym kontrolą Szpital w sposób prawidłowy zawarł umowy powierzenia przetwarzania danych, które zawierały wymagane przez RODO postanowienia. W sposób właściwy udostępniano dokumentację medyczną pacjentów oraz podejmowano właściwe działania w celu minimalizacji ryzyka utraty danych osobowych w wyniku awarii, błędów lub nieuprawnionej modyfikacji. System organizacji rejestracji i udzielania świadczeń pacjentom zapewniał poszanowanie prywatności pacjentów, niemniej opaski identyfikacyjne zawierały dane osobowe, czym naruszono art. 36 ust. 5 ustawy o działalności leczniczej. Personelowi szpitala zapewniono odpowiedni dostęp do danych medycznych, przy czym nie wszystkim zwolnionym pracownikom bez zbędnej zwłoki odbierano dostęp do tych systemów. Negatywnie należy ocenić logowanie się do systemu operacyjnego przez personel medyczny za pomocą tego samego loginu i hasła oraz posiadanie uprawnień administratora przez zalogowanych użytkowników nie będących administratorami systemów informatycznych. Wystąpiły także dwa incydentalne przypadki przekazania dostawcy oprogramowania danych osobowych pacjentów, czym naruszono przepisy art. 5 pkt 1 lit. c RODO.

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) doprowadzenie do zaktualizowania regulacji wewnętrznych w zakresie dotyczącym statusu IOD;
2) intensyfikacja działań zmierzających do szkolenia personelu zaangażowanego w proces przetwarzania informacji z zakresu przepisów rozporządzenia RODO;
3) nieumieszczanie na opaskach identyfikujących pacjentów i na łóżkach danych w postaci ich imienia i nazwiska oraz dostosowanie zapisów w wewnętrznych regulacjach do obowiązujących przepisów w tym zakresie;
4) niezwłoczne odbieranie uprawnień osobom, z którymi Szpital rozwiązał stosunek pracy;
5) dokonywanie zgłoszeń serwisowych bez podawania danych osobowych pacjentów;
6) nadanie indywidualnych danych do autoryzacji w systemach operacyjnych wszystkim użytkownikom komputerów oraz wprowadzenie rozwiązań uniemożliwiających pracę kilku osób na jednym koncie użytkownika;
7) nienadawanie uprawnień administratora do systemu operacyjnego oraz cofnięcie tych uprawnień osobom aktualnie je posiadającym, a niebędącym administratorami tych systemów.

V. Pozostałe informacje i pouczenia

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

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 ustawy o NIK kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się

do dyrektora Delegatury NIK w Krakowie. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Obowiązek poinformowania NIK o sposobie wykonania wniosków

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

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

Kraków, kwietnia 2019 r.

Kontroler:

Rafał Rossowski
starszy inspektor kontroli państwowej