NAJWYŻSZA IZBA KONTROLI

Delegatura w Olsztynie

LOL. 411.5.1.2023

Rafał Laszczak
Dyrektor
Miejskiego Szpitala Zespolonego w Olsztynie
ul. Niepodległości 44,
10-045 Olsztyn

WYSTĄPIENIE POKONTROLNE

I/23/003 - Ochrona danych pacjentów przed cyberatakami w podmiotach leczniczych na terenie województwa warmińsko-mazurskiego.

NAJWYŻSZA IZBA KONTROLI
Delegatura w Olsztynie
ul. Artyleryjska 3e, 10-165 Olsztyn
T +48 89 678 82 00, F +48 89 678 82 30
lol@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana

Miejski Szpital Zespolony w Olsztynie, 10-045 Olsztyn, ul. Niepodległości 44 (dalej: Szpital, MSZ).

Kierownik jednostki kontrolowanej

Rafał Laszczak, Dyrektor Miejskiego Szpitala Zespolonego w Olsztynie od 1 grudnia 2023 r. W okresie od 1 lipca 2023 r. do 30 listopada 2023 r. p.o. Dyrektora Szpitala Zespolonego w Olsztynie (dalej: Dyrektor)

W okresie objętym kontrolą funkcję kierownika jednostki poprzednio pełnili:

- Marian Stempniak, Dyrektor MSZ w Olsztynie, od 1 marca 2021 r. do 30 czerwca 2023 r.
- Lucyna Kiełbasa, p.o. Dyrektora MSZ w Olsztynie, od 1 sierpnia 2020 r. do 9 sierpnia 2020 r., od 7 grudnia 2020 r. do 28 lutego 2021 r.,
- Andrzej Bujnowski Dyrektor MSZ w Olsztynie, od 7 września 2020 r. do 26 grudnia 2020 r.,
- Jacek Zachariasz, p.o. Dyrektora MSZ w Olsztynie, od 10 sierpnia 2020 r. do 6 września 2020 r.,
- Joanna Szymankiewicz-Czużdaniuk, Dyrektor MSZ w Olsztynie, od 1 stycznia 2009 r. do 31 lipca 2020 r.

Zakres przedmiotowy kontroli

1. Działania związane z przygotowaniem technicznym i organizacyjnym dotyczącym przetwarzania i ochrony danych pacjentów przed cyberatakami.
2. Funkcjonowanie przyjętych rozwiązań i ich wpływ na ochronę danych pacjentów przed cyberatakami.

Okres objęty kontrolą

Lata 2020-2023 (I półrocze) z uwzględnieniem okresów wcześniejszych i późniejszych, jeżeli miało to wpływ na realizowane zadania (według stanu na 16 lutego 2024 r.).

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 Olsztynie

Kontrolerzy

1. Joanna Majkowska, starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LOL/148/2023 z 20 listopada 2023 r.
2. Sebastian Helbrecht, specjalista kontroli państwowej upoważnienie do kontroli nr LOL/149/2023 z 20 listopada 2023 r.
3. Bartosz Kościukiewicz, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LOL/171/2023 z 21 grudnia 2023 r.
4. Agnieszka Kiełbik, specjalista kontroli państwowej, upoważnienie do kontroli nr LOL/10/2024 z 8 stycznia 2024 r.

(akta kontroli str. 1-10)

[1] Dz. U. z 2022 r. poz. 623, dalej: ustawa o NIK.

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

W okresie objętym kontrolą w Szpitalu prowadzono działania mające zapewnić ochronę danych pacjentów w trakcie przetwarzania tych danych.

Wprawdzie opracowano system zarządzania bezpieczeństwem informacji w celu zapewnienia poufności, integralności, dostępności i autentyczności danych osobowych, niemniej jednak jego wdrożenie i realizacja nie odbywała się w sposób rzetelny i adekwatny do rodzaju i skali przetwarzanych danych. Przyjęty zarządzeniem Dyrektora[3] system zarządzania bezpieczeństwem informacji (dalej: SZBI) uregulował procedury zarządzania bezpieczeństwem w systemie informatycznym dotyczące m.in. udzielania i odwoływania upoważnień do przetwarzania danych, prowadzenia analiz ryzyka, szkolenia osób zaangażowanych w proces przetwarzania danych osobowych oraz identyfikowania, ewidencjonowania i zgłaszania incydentów naruszenia bezpieczeństwa informacji. Nie uwzględniono w nim natomiast niektórych wymagań wynikających z rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[4] (dalej: rozporządzenie KRI). Nie określono w nim podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i przy pracy na odległość. Do 29 marca 2022 r. nie przeprowadzono również cyklicznego szkolenia przypominającego w tematyce bezpieczeństwa informacji i ochrony danych, a w okresie do 1 stycznia 2020 r. do 30 marca 2022 r. nie egzekwowano obowiązku potwierdzenia zrealizowanych szkoleń przez niektóre osoby zaangażowane w proces przetwarzania informacji.

We właściwy sposób wyznaczono inspektora ochrony danych osobowych (dalej: IODO), tj. zgodnie z rozporządzeniem 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[5] (dalej: rozporządzenie RODO).

Szpital zapewnił także przeglądy SZBI, które doprowadziły do zmiany polityki bezpieczeństwa[6] po upływie trzech lat licząc od 2020 r. (zmiana środowiska przetwarzania informacji). Wpływ na długość tego okresu miały zarówno pandemia wywołana wirusem SARS-CoV-2, jak i zmiany na stanowisku Dyrektora.

Nie w pełni przestrzegano również postanowień obowiązujących przepisów i regulacji wewnętrznych związanych z przetwarzaniem danych. Personelowi administracyjnemu (17% badanych przypadków) oraz medycznemu (6% badanych przypadków) nadano uprawniania dostępu do systemu Optimed NXT w szerszym zakresie niż były niezbędne do realizacji ich zadań. Byłym pracownikom (63,8% ogółu) nie odbierano uprawnień niezwłocznie po zakończeniu z nimi stosunku pracy, co w dwóch przypadkach skutkowało nieuprawnionym dostępem do systemu Optimed NXT. Przyjęte procedury nie zapewniały niezwłocznego odbioru uprawnień i dostępów do systemów informatycznych pracownikom, z którymi Szpital kończył współpracę.

---

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

[3] Z dnia 29 marca 2019 r. nr 27/2019 w sprawie wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji w Miejskim Szpitalu Zespolonym (dalej: zarządzenie 27/2019).

[4] Dz. U. z 2017 r. poz. 2247.

[5] Dz. Urz. UE L 119 z 4 maja 2016 r., str. 1.

[6] Zarządzenie Dyrektora z dnia 31 maja 2023 r. nr 73/2023 w sprawie wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji w Miejskim Szpitalu Zespolonym (dalej: zarządzenie 73/2023).

W toku kontroli NIK podjęto działania naprawcze, wskutek czego osobom wykonującym pracę w Szpitalu odebrano uprawnienia dostępu do systemów informatycznych, które były nieadekwatne do realizowanych przez nich zadań.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[7] kontrolowanej działalności

OBSZAR

1. Działania związane z przygotowaniem technicznym i organizacyjnym dotyczącym przetwarzania i ochrony danych o pacjentach przed cyberatakami

Opis stanu faktycznego

1.1. W Szpitalu funkcjonował SZBI[8], wprowadzony na podstawie dwóch zarządzeń Dyrektora MSZ. Pierwsze z nich (nr 27/2019) obowiązywało w okresie od 26 marca 2019 r. do 4 czerwca 2023 r., drugie zaś (nr 73/2023) od 5 czerwca 2023 r. Ustanawiając ww. System wypełniono obowiązek wynikający z § 20 ust. 1 rozporządzenia KRI.

SZBI przyjęte w 2019 r. stanowiło dokumentację zbudowaną hierarchicznie, obejmującą:

- Politykę Bezpieczeństwa Informacji (dalej: PBI), na którą składały się m.in. zadania IODO, administratora systemów informatycznych (dalej: ASI), administratora danych osobowych (dalej: ADO), procedura prowadzenia analizy ryzyka, instrukcja postępowania w sytuacji naruszenia bezpieczeństwa informacji;
- Politykę ochrony danych osobowych (dalej: PODO) w tym przetwarzanych w zbiorach papierowych i informatycznych, procedura postępowania w zakresie nadawania/odwoływania upoważnień do przetwarzania danych osobowych oraz protokół przestrzegania wymogów rozporządzenia RODO;
- Procedurę: PR II PD 2 Zarządzanie Systemem Informatycznym Szpitala.

SZBI, zgodnie z § 2 PBI, miało zastosowanie do wszystkich rodzajów informacji oraz dotyczyło wszystkich osób przetwarzających te informacje w Szpitalu.

SZBI obowiązujące od 5 czerwca 2023 r. obejmowało m.in.: PBI, w tym Politykę bezpieczeństwa informacji i systemów IT, Instrukcję bezpieczeństwa, Procedurę zarządzania incydentami z zakresu bezpieczeństwa informacji i systemów IT, Metodykę szacowania ryzyka dla systemów IT oraz PODO.

Dyrektor wyjaśnił, że przyczyną zmiany SZBI był brak dostosowania poprzednich procedur do wymagań jednostki. Szpital zaczął korzystać z nowych systemów informatycznych. Wskazał, że przed ww. zmianą przeprowadzono weryfikację sposobu funkcjonowania dotychczasowych procedur.

Analiza niektórych postanowień obu ww. zarządzeń w sprawie ustanowienia SZBI pod względem wymagań określonych rozporządzeniem KRI oraz normą PN-EN ISO/IEC 27001[9] wykazała m.in., że odwoływały się one do:

- Zapewnienia aktualizacji regulacji wewnętrznych dotyczących zmieniającego się otoczenia, co było zgodne z § 20 ust. 2 pkt 1 rozporządzenia KRI. Wprowadzono bowiem zapisy dotyczące aktualizacji dokumentacji przynajmniej raz w roku oraz po każdej zmianie, która mogła mieć wpływ na

[7] 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.

[8] Szpital nie został uznany za Operatora Usługi Kluczowej, tj. podmiot o którym mowa w art. 5 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913, ze zm.).

[9] Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Systemy zarządzania bezpieczeństwem informacji – Wymagania.

system zabezpieczeń (§ 16 pkt 3 lit. b PODO[10]), kontroli bezpieczeństwa informacji, którą należało przeprowadzić co najmniej raz w roku (§ 15 PBI). W latach 2020-2023 wykonano te przeglądy w ramach spotkań rady jakości i przeglądu Zintegrowanego Systemu Zarzadzania Jakością (dalej: ZSZJ).

W zarządzeniu 73/2023 nie wskazano odstępów czasu w jakich należało dokonywać wspomnianych przeglądów. Dyrektor wyjaśnił, że wynikało to z niedopatrzenia oraz że zaplanowano przegląd SZBI, w trakcie którego SZBI zostanie uzupełnione w ww. zakresie.

- Sporządzenia inwentaryzacji sprzętu i oprogramowania. W Szpitalu zapewniono inwentaryzację w zakresie posiadanych serwerów (fizycznych i wirtualnych) oraz urządzeń końcowych. Przed wejściem w życie zarządzenia 73/2023 nie zapewniono takiej inwentaryzacji w odniesieniu do aplikacji i systemów informatycznych, a także nie określono fizycznej i logicznej architektury tych zasobów (opisane w punkcie 1 sekcji stwierdzone nieprawidłowości).
- Opracowania i wdrożenia procesu szacowania ryzyka w bezpieczeństwie informacji, co było zgodne z § 20 ust. 2 pkt 3 rozporządzenia KRI.

  W 2021 r. oraz 2022 r. nie sporządzono natomiast planu postępowania z ryzykiem, nie prowadzono rejestru ryzyka oraz nie dokonano przeglądu przydatności, przeglądu zagrożeń i ryzyka oraz przeglądu skuteczności mechanizmów zabezpieczających (opisano w punkcie 2 sekcji stwierdzone nieprawidłowości). W pozostałym okresie objętym kontrolą dochowano wykonania powyższych obowiązków.
- Ustanowienia procedur przydzielania oraz odbierania uprawnień dostępu do systemów informatycznych osobom zaangażowanym w proces przetwarzania informacji, co było zgodne z § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI (szerzej opisano w obszarze drugim niniejszego wystąpienia).
- Zapewnienia szkoleń osób zaangażowanych w proces bezpieczeństwa informacji i jej przetwarzania (szerzej opisane w punkcie 1.6 niniejszego wystąpienia).
- Zapewnienia zasad zgłaszania incydentów naruszenia bezpieczeństwa, zgodnie z wymaganiami wynikającymi z § 20 ust. 2 pkt 13 rozporządzenia KRI (szerzej opisane w punkcie 1.3 niniejszego wystąpienia).

Ogólne zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, o których mowa w § 20 ust. 2 pkt 8 rozporządzenia KRI, obowiązywały dopiero od 5 czerwca 2023 r. (opisano w punkcie 3 sekcji stwierdzone nieprawidłowości). Określono w nich wówczas m.in. mechanizmy ochrony dla urządzeń mobilnych[11].

Dokumentacja SZBI została zamieszczona na serwerze Szpitala jako dokumenty do użytku wewnętrznego. Zgodnie z § 37 ust. 14 i 17 Regulaminu organizacyjnego MSZ, została ona przekazana kierownikom komórek organizacyjnych oraz pracownikom zatrudnionym na samodzielnych stanowiskach celem zapoznania się z jej postanowieniami.

(akta kontroli str.11-504)

1.2. SZBI określało, że za bezpieczeństwo informacji odpowiadał każdy pracownik, bez względu na formę zatrudnienia, a nadzór pełnili kierownicy komórek organizacyjnych.

[10] Wprowadzonej zarządzeniem 27/2019.

[11] § 7 Polityki bezpieczeństwa informacji i systemów IT oraz w punkcie 4.4.15 PODO przyjętego zarządzeniem 73/2023.

Zgodnie z treścią zarządzenia 27/2019 odpowiedzialność za obszary mające wpływ na bezpieczeństwo informacji została przypisana:

- Dyrektorowi Szpitala, jako osobie odpowiadającej za stworzenie warunków, aby zapewnić bezpieczeństwo, w szczególności za zorganizowanie i zapewnienie funkcjonowania ochrony.
- ASI, który realizował zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym. Miał także przeciwdziałać dostępowi osób nieuprawnionych do systemów, zarządzać nadawaniem i odbieraniem uprawnień, nadzorować działanie mechanizmów uwierzytelniania. Przypisane mu zostały zadania związane ze stwierdzeniem naruszenia bezpieczeństwa informacji. Do 29 września 2022 r. zadania ASI realizowane były przez Dział Informatyki bez ich formalnego uregulowania w zakresie zadań tej komórki organizacyjnej Szpitala oraz bez wskazania konkretnego pracownika tego działu, któremu powierzono funkcję ASI (opisane w punkcie 4 sekcji stwierdzone nieprawidłowości). Zadania ASI przydzielono[12] pracownikom Działu Informatyki i jako osobę odpowiedzialną za ww. zadanie wskazano jednego z pracowników.
- IODO – którego zadania szerzej opisano w punkcie 1.4 niniejszego wystąpienia.
- Pełnomocnikowi ds. ochrony informacji niejawnych (dalej: POIN) – odpowiadał on za zapewnienie ochrony informacji niejawnych, w tym stosowanie środków bezpieczeństwa fizycznego oraz szkolenia w zakresie tych informacji. Obowiązki POIN powierzono specjaliście do spraw obronnych, zajmującego stanowisko wyodrębnione w strukturze organizacyjnej Szpitala. Po 26 marca 2019 r. w zakresie obowiązków POIN pozostawiono zadania dotyczące ochrony danych osobowych, pomimo powierzania ich z tym dniem wyznaczonemu IODO (opisane w punkcie 5 sekcji stwierdzone nieprawidłowości).

W okresie objętym kontrolą, w ramach ZSZJ, powołano pełnomocnika odpowiedzialnego za SZBI (dalej: Pełnomocnik ds. SZBI). Funkcję tę pełnili kolejno: Zastępca Dyrektora ds. Pielęgniarstwa, IODO oraz Kierownik Działu Informatyki. Odpowiedzialność w zakresie bezpieczeństwa informacji od 5 czerwca 2023 r. przypisano Pełnomocnikowi ds. SZBI. W zarządzeniu 73/2023 wskazano, że odpowiadał on za bezpieczeństwo informacji w zakresie niezastrzeżonym dla kompetencji innych osób, w szczególności za:

- zapewnienie zgodności SZBI z polską normą PN-EN ISO/IEC 27001 oraz dokonywanie jego przeglądów i aktualizacji,
- inicjowanie oraz nadzorowanie działań wdrożeniowych, korygujących i zapobiegawczych w zakresie bezpieczeństwa informacji,
- koordynowanie procesu zarządzania ryzykiem bezpieczeństwa informacji,
- opracowywanie i przeprowadzanie szkoleń z zakresu SZBI,
- nadzorowanie procesu zarzadzania incydentami bezpieczeństwa,
- prowadzenie rejestru aktywów,
- wydawanie opinii, zaleceń oraz rekomendacji w zakresie związanym z funkcjonowaniem SZBI.

Z dniem 7 czerwca 2023 r. POIN otrzymał pełnomocnictwo Dyrektora do nadawania upoważnień do przetwarzania danych osobowych.

(akta kontroli str. 13-280, 505-630)

1.3. W latach 2020-2023 (I półrocze) w Szpitalu określono obowiązek i zasady zgłaszania naruszeń bezpieczeństwa informacji. Przyjęto katalog zdarzeń, które należało traktować jako to naruszenie i które mogły zostać uznane za incydent, niezależnie od wystąpienia skutków. W przypadku ich wystąpienia należało podjąć

[12] Zarządzeniem wewnętrznym nr 129/2022 z 29 września 2022 r. dotyczącym Regulaminu Organizacyjnego MSZ.

działania zgodne z Instrukcją postępowania w sytuacji naruszenia bezpieczeństwa informacji[13].

W ww. Instrukcji określono odpowiedzialność za nadzór nad jej realizacją, opisano postępowanie w przypadku stwierdzenia naruszenia, w tym zasady zgłaszania organowi nadzorczemu oraz zawiadamiania osób, których dobra zostały naruszone. Przewidziano także analizę incydentów i dalsze działania związane z oceną ich skutków oraz opracowaniem zaleceń mających na celu podniesienie poziomu bezpieczeństwa. Instrukcja określała ponadto wzory dokumentów pozwalające na weryfikowanie przestrzegania obowiązków gromadzenia i zgłaszania danych o naruszeniach, które wynikały z art. 33 i 34 rozporządzenia RODO[14].

Pracownicy Szpitala, zgodnie z postanowieniami § 4 ust. 1 pkt 3 ww. Instrukcji, byli zobowiązani do zgłoszenia incydentu. W przypadku natomiast naruszenia danych osobowych, zgodnie z art. 33 ust. 1 rozporządzenia RODO, zdarzenie takie należało zgłosić Prezesowi Urzędu Ochrony Danych Osobowych (dalej: PUODO), w terminie 72 godzin, chyba że było mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Realizacja wyżej opisanych obowiązków została powierzona IODO[15], co prowadziło do konfliktu interesów, o którym mowa w art. 38 ust. 6 rozporządzenia RODO (opisane w punkcie 8 sekcji stwierdzone nieprawidłowości).

Obowiązująca w Szpitalu po 5 czerwca 2023 r.[16] Procedura zarządzania incydentami z zakresu bezpieczeństwa informacji i systemów IT określała m.in. sposób zgłaszania incydentów, otwarty katalog zdarzeń wymagających zgłoszenia oraz wskazywała osoby odpowiedzialne i ich role. Wzór karty rejestru naruszeń ochrony danych zawierał informacje pozwalające na spełnienie obowiązków wynikających z art. 33 ust. 3 i 5 rozporządzenia RODO.

W latach 2020-2023 (do 5 czerwca 2023 r.) nie prowadzono ewidencji naruszeń ochrony danych osobowych, o której mowa w § 7 ust. 9 Instrukcji postępowania w sytuacji naruszenia bezpieczeństwa informacji. Szpital posiadał natomiast dokumentację dwóch incydentów naruszenia bezpieczeństwa. Pierwszy z nich wystąpił od 30 października 2021 r. do 2 listopada 2021 r. Polegał na nieuprawnionym przełamaniu zabezpieczeń poczty elektronicznej. Uzyskano wówczas dostęp do danych osobowych 43 osób (pacjentów i pracowników). W związku z wysokim poziomem ryzyka naruszenia praw i wolności osób incydent ten 5 listopada 2021 r., tj. w terminie wynikającym z art. 33 ust. 1 rozporządzenia RODO, został zgłoszony PUODO. Zawiadomiono o tym również organy ścigania[17] oraz osoby, których ww. dane dotyczyły. Dokumentowanie naruszeń ochrony bezpieczeństwa danych osobowych w zakresie sporządzenia raportów i przesyłania zawiadomień były niezgodne z wymaganiami Instrukcji postępowania w sytuacji naruszenia bezpieczeństwa informacji oraz rozporządzenia RODO (opisane w punkcie 6 sekcji stwierdzone nieprawidłowości).

Drugi z incydentów wystąpił w listopadzie 2022 r. i dotyczył naruszenia poufności danych jednego z pacjentów w związku z udzieleniem nieuprawnionej osobie informacji na jego temat. Poziom ryzyka naruszenia określono na niski i nie zgłoszono go do PUODO.

(akta kontroli str. 631-669)

---

[13] Stanowiącą załącznik do PBI (§ 12) przyjętego zarządzeniem 27/2019.

[14] Raport z incydentu naruszenia bezpieczeństwa informacji, zawiadomienie organu nadzoru o naruszeniu ochrony danych osobowych, zawiadomienie osoby o naruszeniu ochrony danych osobowych, ewidencja naruszeń ochrony danych osobowych.

[15] § 5 ust. 1 Instrukcji postępowania w sytuacji naruszenia bezpieczeństwa informacji.

[16] Zarządzenie 73/2023.

[17] Wydział dw. z Przestępczością Gospodarczą Komendy Miejskiej Policji w Olsztynie. Dochodzenie umorzono 30 stycznia 2023 r. w związku z niewykryciem sprawcy czynu zabronionego.

W latach 2020-2023 (I półrocze) do Szpitala wpłynęło 78 skarg i wniosków[18], w tym jedno dotyczyło ujawnienia danych osobowych i związana była z drugim, opisanym powyżej, incydentem naruszenia danych.

(akta kontroli str. 670)

1.4. Zgodnie z art. 8 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[19] w związku z art. 37 ust. 1 lit. a rozporządzenia RODO, w Szpitalu 15 maja 2018 r. wyznaczono IODO, tj. jednemu z pracowników Szpitala powierzono obowiązki w tym zakresie. W związku z długotrwałą nieobecnością IODO[20] nie zapewniono jednak jego wsparcia ADO (opisane w punkcie 7 sekcji stwierdzone nieprawidłowości). Pracownik ten został odwołany z funkcji IODO 14 lutego 2022 r., zaś kolejny Inspektor został wyznaczony 23 lutego 2022 r.[21] Szpital, zgodnie z art. 10 ust. 1 o ochronie danych osobowych, terminowo powiadomił PUODO o odwołaniu IODO i powierzeniu obowiązków kolejnej osobie.

Stosownie do art. 37 ust. 5 rozporządzenia RODO, osoby pełniące funkcję IODO posiadały fachową wiedzę w zakresie prawa i praktyk w dziedzinie ochrony danych osobowych oraz umiejętności umożliwiające pełnienie zadań. Jako potwierdzenie tego uznano historię przebiegu ich zatrudnienia, posiadane wykształcenie oraz ukończone szkolenia.

Bezpośredni nadzór nad stanowiskiem IODO, zgodnie ze strukturą organizacyjną Szpitala, sprawował Dyrektor. Do zadań IODO należało m.in.:

- informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe o obowiązkach spoczywających na nich na mocy rozporządzenia RODO oraz innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie,
- monitorowanie przestrzegania przepisów o ochronie danych osobowych, polityk wewnętrznych Szpitala w zakresie danych osobowych, w tym szkolenia personelu oraz powiązane z tym audyty,
- współpraca z organem nadzorczym,
- pełnienie funkcji punktu kontaktowego dla organu nadzorczego, tj. wszystkie zadania określone w art. 39 rozporządzenia RODO.

Zarządzeniem 27/2019 nałożono na IODO także inne obowiązki obejmujące swym zakresem zadania należące do właściwości ADO m.in. nadawania lub odwoływania upoważnień, przekazywania zgłoszeń do PUODO, zaś w umowie z 23 lutego 2022 r. o świadczenie usług inspektora zlecono wdrażanie rozporządzenia RODO, a więc czynności, których realizacja powodowałby konflikt interesów, ponieważ powinien on m.in. monitorować przestrzeganie przepisów o ochronie danych, a także nadzorować i kontrolować prawidłowe wykonywanie obowiązków przez administratora (opisane w punkcie 8 sekcji stwierdzone nieprawidłowości).

(akta kontroli str. 671-709)

1.5.1. W Szpitalu określono zasady organizacji szkoleń osób zaangażowanych w proces przetwarzania informacji.

W latach 2020-2023[22] zakładano przeprowadzenie szkoleń nowo przyjętych pracowników, praktykantów i stażystów. Szkolenia te miały być przeprowadzone przez IODO przed przystąpieniem ww. osób do wykonywania obowiązków służbowych i potwierdzone złożeniem oświadczenia, o którym mowa w § 16 ust. 3

[18] W tym: 14 w 2020 r., 19 w 2021 r., 30 w 2022 r. i 15 w I półroczu 2023 r.

[19] Dz. U. z 2019 r. poz. 1781.

[20] Od 15 kwietnia 2021 r.

[21] Szpital zlecił świadczenie usług związanych z ochroną danych osobowych i pełnieniem funkcji inspektora firmie zewnętrznej. IODO powołano zarządzeniem wewnętrznym nr 31/2022 z dnia 23 lutego 2022 r. w sprawie powołania IODO.

[22] Do 4 czerwca 2023 r.

PBI. Zgodnie z § 7 Procedury postępowania w zakresie nadawania/odwoływania upoważnień do przetwarzania danych osobowych, IODO był zobowiązany do prowadzenia rejestru dokumentów wydanych w związku z tymi upoważnieniami. Według stanu na 24 stycznia 2024 r. w Szpitalu nie prowadzono tego rejestru, natomiast od 30 marca 2022 r. prowadzono rejestr szkoleń.

Zgodnie z przyjętymi zarządzeniem 27/2019 założeniami zakładano również przeprowadzenie cyklicznych szkoleń pracowników, nie rzadziej niż raz na 3 lata.

(akta kontroli str. 13-100)

1.5.2. W Szpitalu w okresie od 1 stycznia 2020 r. do 30 marca 2022 r. 143 stażystów, praktykantów i pielęgniarka, złożyło oświadczenia o ukończeniu szkolenia w zakresie ochrony informacji prawnie chronionych. Treść tych oświadczeń była zgodna ze wzorem określonym w § 16 ust. 3 PBI. Nowo zatrudnieni w ww. okresie pracownicy Szpitala[23], stażyści oraz 472 praktykantów nie złożyło w ww. okresie takich oświadczeń (opisane w punkcie 9 sekcji stwierdzone nieprawidłowości). Od 30 marca 2022 r. prowadzono ewidencję szkoleń z zakresu danych osobowych, w której według stanu na 31 grudnia 2022 r. ujęto zapisy o szkoleniach 495 osób (studenci, praktykanci, personel Szpitala) a osoby przeszkolone składały oświadczenia. Szkolenia te były przeprowadzone przez IODO, a ich zakres był zgodny z § 20 ust. 2 pkt 6 rozporządzenia KRI.

(akta kontroli str. 710-711, 713-718)

1.5.3. Dokumentacja Szpitala nie potwierdzała odbycia przez cały personel Szpitala[24] nie rzadziej niż raz na 3 lata, szkolenia cyklicznego, o którym mowa w § 16 ust. 1 PBI (opisane w punkcie 9 sekcji stwierdzone nieprawidłowości). Szkolenie przeprowadzono bowiem po upływie ww. trzyletniego okresu, tj. od 20 października do 6 listopada 2022 r., kiedy to 563 osób[25] spośród 759 pracowników Szpitala zostało zobowiązanych do zapoznania się z prezentacją szkoleniową. Było to następstwem pisma PUODO z 6 września 2022 r.[26], wzywającego do złożenia wyjaśnień dotyczących m.in. wskazania czy pracownicy odbyli szkolenia w zakresie bezpiecznego korzystania z poczty elektronicznej, uświadamiającego ich w tematyce potencjalnych ataków socjotechnicznych oraz informatycznych oraz metod ochrony przed nimi. Wezwanie to było związane z wcześniejszym incydentem jaki miał miejsce w Szpitalu, dotyczącym naruszenia danych osobowych.

(akta kontroli str. 721-749)

1.5.4. W ogólnoszpitalnym i oddziałowym planie szkoleń na rok 2020 r. zaplanowano przeprowadzenie szkoleń w zakresie bezpieczeństwa informacji. Zrealizowanych miało zostać pięć szkoleń dla 578 osób (lekarzy, pielęgniarek, kierowników komórek organizacyjnych i liderów procesów oraz pracowników laboratorium)[27]. Jednakże plan ten nie został wykonany[28] z uwagi na pandemię covid-19. W latach 2021-2022 w planie nie uwzględniano szkoleń w powyższym zakresie

W latach 2020-2021 przeprowadzono dwa szkolenia dla 30 osób z kadry kierowniczej i liderów procesów zarządzania jakością w zakresie zarządzania bezpieczeństwem informacji oraz szkolenie na temat RODO w służbie zdrowia.

[23] 358 nowo zatrudnionych pracowników.
[24] Według stanu na 31 grudnia 2021 r. personel ten liczył wówczas 762 osoby.
[25] Studenci, rezydenci, personel medyczny i niemedyczny.
[26] Znak pisma DKN.5130.11378.2021.FS.
[27] Szkolenia zaplanowano na luty, kwiecień, wrzesień, październik 2020 r. w zakresie systemu zarządzania bezpieczeństwem informacji i polityki ochrony danych osobowych w ujęciu praktycznym oraz bezpieczeństwu informacji.
[28] W zakresie czterech szkoleń.

Ponadto, w okresie od lipca 2021 r. do grudnia 2022 r. POIN przeprowadził szkolenia 468 nowo zatrudnionych pracowników uwzględniające w swoim zakresie bezpieczeństwo informacji w Szpitalu.

(akta kontroli str. 749)

1.5.5. W Polityce bezpieczeństwa informacji i systemów IT[29] określono, że działania związane z edukacją i podnoszeniem świadomości powinny być prowadzone cyklicznie, nie rzadziej niż raz na rok. Wskazano przy tym, że osobą odpowiedzialną za realizację ww. działań był Dyrektor, zaś nadzór w tym zakresie sprawował Pełnomocnik ds. SZBI. Określono w niej również wzór ewidencji szkoleń dotyczących ochrony danych osobowych oraz plan szkolenia[30]. Plan ten uwzględniał zagadnienia dotyczące zagrożenia bezpieczeństwa informacji, skutków naruszenia zasad bezpieczeństwa, w tym odpowiedzialności prawnej, stosowania środków zapewniających bezpieczeństwo informacji. Ponadto określono, że szkolenia w zakresie swoich kompetencji prowadzić będzie także POIN i IODO.
Kierownik Działu Informatyki przesłał użytkownikom domeny Szpitala komunikaty z ostrzeżeniem o zagrożeniach związanych z użytkowaniem poczty elektronicznej oraz o kampanii phishingowej[31].

(akta kontroli str. 100-244)

1.6. W okresie objętym kontrolą Szpital jednokrotnie wystąpił do Warmińsko-Mazurskiego Oddziału Wojewódzkiego Narodowego Funduszu Zdrowia (dalej: NFZ) o wsparcie na dofinansowanie inwestycji poprawiającej bezpieczeństwo infrastruktury teleinformatycznej. W 2022 r. uzyskał wsparcie w wysokości 597,8 tys. zł ze środków funduszu przeciwdziałania covid-19. Środki te przeznaczone były na sfinansowanie działań w celu podniesienia bezpieczeństwa systemów teleinformatycznych. W ramach dofinansowania pozyskano nowe systemy ochrony: sieci wewnętrznej, aplikacji Web i poczty elektronicznej z funkcją serwera pocztowego oraz rozbudowano posiadany już system, a także przeprowadzono stosowny audyt.

Przeprowadzone audyty bezpieczeństwa wykazały, że inwestycje objęte finansowaniem przyczyniły się do wyraźnego podniesienia poziomu bezpieczeństwa, bowiem miały wpływ na:

- skuteczność działania infrastruktury (urządzenia i konfiguracja w zakresie ochrony poczty, sieci oraz systemów bezpieczeństwa),
- monitorowanie i wykrywanie incydentów bezpieczeństwa,
- zarządzanie tożsamością w zakresie przydzielania oraz odbierania dostępu do systemów,
- zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług (metody uwierzytelnienia).

(akta kontroli str. 750-821)

1.7. Dyrektor Szpitala wyjaśnił że podejmuje działania w celu zapewnienia spełniania wymogów rozporządzenia KRI. Wskazał, że szczególnym utrudnieniem w realizacji zadań w okresie 2020-2022 była pandemia covid-19. Dodatkowym utrudnieniem w jego ocenie jest rozmiar i złożoność struktury organizacyjnej MSZ oraz ilość zatrudnionego personelu, a także migracje pracowników między oddziałami Szpitala. Wyjaśnił, że podejmowane były działania mające zapewnić bieżącą aktualizację regulacji wewnętrznych oraz mające zapewnić odpowiedni poziom bezpieczeństwa poprzez uszczelnienie przyjętych rozwiązań. Podał, że rozpoczął prowadzenie rozmów w zakresie przyjęcia nowych procedur i schematów działania,

[29] Stanowiącej załącznik nr 2 do zarządzenia 73/2023.
[30] Stanowiący załącznik nr 20 do PODO.
[31] System komunikatów intranetowych otwierający się po zalogowaniu do domeny.

które w pełniejszym zakresie pozwolą na zorganizowanie działań określonych w rozporządzeniu KRI i wewnętrznych regulacjach.

(akta kontroli str. 608-617)

Stwierdzone nieprawidłowości

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

1. W Szpitalu do 2 lipca 2021 r. nie sporządzono inwentaryzacji oprogramowania, zawierającej niektóre informacje o elementach składowych tworzących infrastrukturę IT. Sporządzony natomiast w związku z wejściem w życie zarządzenia 73/2023 wykaz, został zatwierdzony przez Pełnomocnika ds. SZBI, mimo że nie odpowiadał w pełni wymogom określonym w § 6 Instrukcji bezpieczeństwa IT. Nie zawierał bowiem m.in informacji o: opisie fizycznej i logicznej architektury zasobu IT, zgodności zasobów IT z wymaganiami bezpieczeństwa, integracji i powiązań, lokalizacji, warunkach eksploatacji i utrzymania oraz wymaganiach dotyczących wycofania. Zgodnie z § 20 ust. 2 pkt 2 rozporządzenia KRI, kierownictwo podmiotu publicznego zobowiązane było do zapewnienia aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, obejmującej ich rodzaj i konfigurację.

   Dyrektor wyjaśnił, że ww. wykazu nie wykonano, bowiem Polityka Bezpieczeństwa Informacji nie definiowała takiego obowiązku.

   Pełnomocnik ds. SZBI wyjaśnił, że podjął decyzję o zatwierdzeniu sporządzonego wykazu, pomimo że był świadomy „absurdalnych" zapisów SZBI. W jego ocenie spełnienie zapisu Instrukcji wymaga dużego nakładu pracy pracowników. Inwentaryzacja taka powinna być uproszczona i prowadzona w sposób elektroniczny, z wykorzystaniem posiadanych narzędzi informatycznych. Szpital posiada dane określone w § 6 Instrukcji, lecz wymagają one inwentaryzacji i przełożenia na dokument.

   NIK nie podziela ww. wyjaśnień Dyrektora, bowiem wykaz taki został wymieniony w strukturze SZBI przyjętej zarządzeniem 27/2019. Ponadto obowiązek jego sporządzenia wynikał zarówno z § 20 ust. 2 pkt 2 rozporządzenia KRI, jak i postanowień polskiej normy PN-ISO/IEC 27001, która wprost wskazywała, że aktywa związane z informacjami i środkami przetwarzania tych informacji należy zidentyfikować oraz sporządzić i utrzymywać ich ewidencję.

   (akta kontroli str. 20, 124-130, 245-315, 495-502)

2. W latach 2021-2022 nie zrealizowano niektórych obowiązków określonych w SZBI, tj.:
   – nie opracowano planu postępowania z ryzykiem, co było niezgodne z § 2 Procedury przeprowadzania analizy ryzyka stanowiącej załącznik do zarządzenia 27/2019,
   – nie prowadzono rejestru ryzyk, co było niezgodne z § 5 ust. 2 ww. Procedury,
   – nie dokonano przeglądu przydatności, zagrożeń i ryzyka oraz skuteczności mechanizmów zabezpieczających, co było niezgodne z § 7 ust. 2 ww. Procedury.

   Dyrektor wyjaśnił, że pełnił obowiązki kierownika jednostki od 1 lipca 2023 r. i nie posiadał on wiedzy, dlaczego w okresie objętym kontrolą nie zrealizowano powyższych obowiązków.

   (akta kontroli str. 23-42, 319-337, 625-630)

3. Do 5 czerwca 2023 r. w Szpitalu nie ustalono podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość, do czego zobowiązywał § 20 ust. 2 pkt 8 rozporządzenia KRI. Wymóg

pisemności ww. zasad wynikał natomiast z celu A.5.1.1 normy PN-ISO/IEC 27001, zgodnie z którym zbiór polityk powinien być opracowany, zatwierdzony, opublikowany i zakomunikowany. Zarządzenie 27/2019 w sprawie wprowadzenia SZBI nie zawierało uregulowań dotyczących pracy na odległość. Ich brak miał istotne znaczenie, gdyż zarządzeniem Dyrektora[32], dopuszczono taką możliwość na podstawie polecenia bezpośredniego przełożonego, a w latach 2020-2023 (I półrocze), z możliwości dostępu do danych medycznych poprzez komputery prywatne skorzystało 35 osób.

Pełnomocnik ds. SZBI wyjaśnił, że Szpital nie uregulował tych zasad. Pracownikom Szpitala, podczas instalacji oprogramowania na komputerach prywatnych, udzielano informacji w zakresie zasad informatycznych dotyczących ich przetwarzania. Szpital tworzył bazę wiedzy, którą po opracowaniu udostępni na swoim serwerze. Od 9 stycznia 2024 r. pracownikom Szpitala doręczane były natomiast pisemne zasady dotyczące pracy zdalnej.

Dyrektor wyjaśnił, że Szpital analizował zapisy SZBI i dostrzegł potrzebę zaktualizowania dokumentacji, a także że podjął w tym kierunku działania. Jednakże z uwagi na zmiany kadrowe na stanowisku kierownika jednostki, pełnomocnika ds. jakości, IODO, Pełnomocnika ds. SZBI nie dokonano takiej aktualizacji. Ponadto w okresie od 2020 r. do 2022 r. przyczyniła się do tego pandemia covid-19.

(akta kontroli str. 13-100, 319-320, 338-340, 625-630, 975-1011)

4. Wyznaczenie ASI nastąpiło dopiero 31 marca 2023 r., tj. po ponad czterech latach od przyjęcia SZBI z 2019 r. Z tym dniem nastąpiło wyznaczenie konkretnego pracownika do pełnienia funkcji ASI poprzez wskazanie tej osoby w planie pracy Działu Informatyki na 2023 r. Zgodnie z § 8 ust. 5 PBI przyjętej zarządzeniem 27/2019 Dyrektor Szpitala upoważnia ASI do wykonania czynności związanych z administrowaniem i monitorowaniem użycia systemu oraz zapewniających poprawność jego działania.

   Dyrektor wyjaśnił, że ASI nie został powołany przez przeoczenie.

   (akta kontroli str. 13-31, 505-542, 618-624)

5. W okresie od 26 marca 2019 r. do dnia 24 stycznia 2024 r. nie dokonano aktualizacji zakresu obowiązków POIN. W zakresie tych obowiązków pozostawiono bowiem zadania dotyczące ochrony danych osobowych, które powierzono IODO. W zakresie czynności POIN wskazano m.in. wspieranie Administratora Bezpieczeństwa Informacji (dalej: ABI) w ochronie danych osobowych. Tymczasem z dniem 5 lutego 2019 r. uchylono ustawę z dnia 29 sierpnia 1997 r.[33] i przestało funkcjonować stanowisko ABI.

   Z wyjaśnień Dyrektora wynika, iż brak zmiany w zakresie obowiązków POIN w związku z powierzeniem takich samych obowiązków nowo powołanemu IODO, wynikał z niedopełnienia ww. obowiązku.

   (akta kontroli str. 35-36, 38, 543-547, 618-622, 671-673, 680-688)

6. W latach 2020-2023 (do 5 czerwca) nie realizowano niektórych przyjętych w Szpitalu zasad wynikających z Instrukcji postępowania w sytuacji naruszenia bezpieczeństwa informacji[34], tj.:

[32] Nr 22/2020 z dnia 16 marca 2020 r. w sprawie przeciwdziałania rozprzestrzeniania się wirusa SARS-CoV-2 wśród pracowników MSZ w Olsztynie.

[33] Dz. U. z 2016 r. poz. 922, ze zm.

[34] Przyjętej zarządzeniem 27/2019.

- W całym wskazanym okresie nie utworzono ewidencji naruszeń ochrony danych osobowych, o której mowa w § 7 ust. 9 ww. Instrukcji.
- W przypadku obu zidentyfikowanych incydentów naruszenia bezpieczeństwa danych osobowych[35], nie podjęto działań wymaganych postanowieniami § 4 ust. 5 ww. Instrukcji. Nie sporządzono bowiem raportu, a sporządzony rejestr naruszeń ochrony, nie zawierał niektórych, wymaganych Instrukcją danych o tych zdarzeniach[36], a także nie został uzupełniony w zakresie podjętych działań korygujących przez ASI[37].
- Zawiadomienia skierowane do 43 osób, w związku z incydentem polegającym na nieuprawnionym dostępie do ich danych osobowych, nie zostały sporządzone zgodnie z wzorem przewidzianym ww. Instrukcją oraz wymaganiami art. 34 ust. 2 rozporządzenia RODO[38]. W związku ze stanowiskiem PUODO zostały one przesłane powtórnie 31 października 2022 r., tj. po upływie 11 miesięcy od dnia, w którym miał miejsce ww. incydent.

Z wyjaśnień Dyrektora wynika, że nie prowadzono ewidencji naruszeń danych osobowych w związku z nieobecnością pracownika pełniącego funkcję IODO. Natomiast osoba pełniąca funkcję IODO po 23 lutego 2022 r. nie prowadziła ewidencji naruszeń, bowiem rozpoczęła pracę nad zaktualizowaniem obowiązującej dokumentacji i podejmowane były wówczas jedynie działania zmierzające do zapewnienia ochrony danych wynikające z przepisów do czasu wprowadzenia zaktualizowanej dokumentacji. Pracownik, który ujawnił pierwszy z incydentów nie sporządzali raportów w wyniku niedopełnienia obowiązków. IODO (pełniący obowiązki po 23 lutego 2022 r.) sporządził dokument w zakresie wynikającym z przepisów prawa.

NIK zwraca uwagę że, zgodnie z art. 33 ust. 5 rozporządzenia RODO obowiązki dokumentowania naruszeń ochrony danych osobowych spoczywają na ADO, który winien dokumentować wszystkie okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja taka musi pozwolić organowi nadzorczemu na weryfikowanie przestrzegania powyższego obowiązku. Powierzenie w tym zakresie obowiązków innej osobie, nie zwalnia ADO z odpowiedzialności za realizację zadania.

(akta kontroli str. 43-53, 319-322, 618-622, 631-667)

7. W Szpitalu w okresie od 15 kwietnia 2021 r. do 23 lutego 2022 r. przy wykonywaniu operacji przetwarzania szczególnych kategorii danych osobowych wymagających regularnego i systematycznego monitorowania nie zapewniono wsparcia IODO. Zgodnie z motywem 97 do rozporządzenia RODO, w sytuacji przetwarzania danych osobowych przez administratora, którego główna działalność polega na operacjach wymagających regularnego i systematycznego monitorowania osób, których dane dotyczą oraz na dużą skalę, podmiot przetwarzający powinien być wspomagany przez osobę dysponującą wiedzą fachową na temat prawa i praktyk w dziedzinie ochrony danych. W Szpitalu wyznaczony jednoosobowo IODO, nie świadczył pracy od 15 kwietnia 2021 r. Po jego rezygnacji od 14 lutego 2022 r. do 23 lutego 2022 r. nie wyznaczono IODO.

[35] Do których doszło w dniach od 30 października do 2 listopada 2021 r. oraz 19 listopada 2022 r.

[36] Nazwisko osoby zgłaszającej, loginu użytkownika, stanowiska, opisu podjętych działań przez pracowników Szpitala wraz z datą i podpisem.

[37] W przypadku drugiego z nich.

[38] Imienia i nazwiska oraz danych kontaktowych IODO, opisu możliwości konsekwencji naruszenia ochrony danych osobowych oraz opisu środków zastosowanych lub promowanych przez administratora w celu zaradzenia naruszeniu – w tym w stosownych przypadkach – środków w celu zminimalizowania jego ewentualnych negatywnych skutków.

W okresie od 15 kwietnia 2021 r. do 14 lutego 2022 r. nie skorzystano także z możliwości wyznaczenia osoby zastępującej IODO, o której mowa w art. 11a ustawy o ochronie danych osobowych. Skutkiem tego było niezapewnienie skutecznej realizacji zadań IODO, o których mowa w art. 39 rozporządzenia RODO oraz określonych w przyjętym SZBI.

Dyrektor wyjaśnił, że objął stanowisko 1 lipca 2023 r. i nie posiadał wiedzy, dlaczego w okresie objętym kontrolą nie zapewniono wsparcia IODO i nie skorzystano z możliwości wyznaczenia osoby zastępującej.

(akta kontroli str. 625-630, 671-709, 929-930)

8. Powierzenie zadań dotyczących nadawania i odbierania upoważnień do przetwarzania danych osobowych oraz zgłaszania naruszenia ochrony tych danych powodowały konflikt interesów, a wskazanych w § 8 ust. 4 pkt 2 PBI, § 2 pkt 3 litera d, § 4 pkt 1, § 5 i 6 Procedury postępowania w zakresie nadawania/odwoływania upoważnienia do przetwarzania danych osobowych, § 2 ust. 1, § 5 ust. 1 Instrukcji postępowania w sytuacji naruszenia bezpieczeństwa informacji oraz § 16 ust. 3 litera c PODO faktycznie prowadziło do konfliktu interesów. Zlecenie zadań polegających na wdrożeniu RODO, przygotowania PODO i opracowania regulaminu ochrony tych danych[39] w umowie z 23 lutego 2023 r. na świadczenie usług związanych z ochroną danych osobowych i pełnieniem funkcji inspektora danych pozostawały również w sprzeczności z ww. zasadą. Zgodnie bowiem z art. 38 ust. 6 rozporządzenia RODO administrator lub podmiot przetwarzający mogą powierzyć IODO inne zadania i obowiązki, jednak zapewniają, by nie powodowały one konfliktu interesów.

   Dyrektor wyjaśnił, że stanowisko PUODO w tym zakresie pojawiło się dopiero w 2022 r. i wskazywało, że powierzenie IODO takich obowiązków nie było prawidłowym działaniem. Jednocześnie wskazał, że po uzyskaniu ww. wiedzy wyeliminował ww. działania. W jego ocenie przygotowanie dokumentacji związanej z ochroną danych osobowych nie powoduje konfliktu interesów. Podkreślił, że przygotowana przez IODO część dokumentacji w tym zakresie była dokładnie analizowana w Szpitalu i dostosowana do jego potrzeb. W ocenie Dyrektora status IODO pozwala na efektywną, niezależną oraz prawidłową realizację obowiązków wynikających z przepisów prawa.

   NIK zwraca uwagę, że przepisy rozporządzenia RODO w powyższym zakresie nie ulegały zmianie. Były one przedmiotem orzeczeń PUODO przed 2022 r.[40] Ponadto NIK nie neguje, niezależnej pozycji IODO w Szpitalu, a wyłącznie powierzenie zadań mogących powodować konflikt interesów.

   (akta kontroli str. 13-100, 625-630, 666-667, 701-709,)

9. Osobom zaangażowanym w proces przetwarzania informacji nie zapewniono szkoleń w tym zakresie, w sposób określony w: SZBI, § 20 ust. 2 pkt 6 rozporządzenia KRI oraz w punkcie A.7.2.2 polskiej normy PN-ISO/IEC 27001. Zgodnie z § 20 ust. 2 pkt 6 KRI kierownictwo podmiotu winno zapewnić szkolenia osób zaangażowanych w proces przetwarzania informacji. W punkcie A.7.2.2 polskiej normy PN-ISO/IEC 27001 wskazano, że kierownictwo winno zapewnić szkolenia osób zaangażowanych w proces przetwarzania informacji. Ponadto, zgodnie z punktem 7.5.1 ww. normy organizacja powinna udokumentować informacje określone przez nią jako niezbędne do zapewnienia bezpieczeństwa informacji. Szpital natomiast:

[39] Zawarte w Opisie przedmiotu zamówienia na świadczenie usług związanych z ochroną danych osobowych i pełnieniem funkcji inspektora ochrony danych osobowych.

[40] ZWAD.405.31.331.2019 opublikowane na stronie https://uodo.gov.pl/

- Nie dysponował dowodami potwierdzającymi, że w okresie od 1 stycznia 2020 r. do 30 marca 2022 r. nowo zatrudnieni pracownicy, praktykanci i stażyści odbyli szkolenia dotyczące bezpieczeństwa informacji. Bowiem 358 nowo zatrudnionych w tym okresie pracowników i stażystów oraz 472 praktykantów[41] nie złożyło oświadczenia o odbytym szkoleniu, o którym mowa w § 16 ust. 1 i 3 PBI.
- W okresie od 1 stycznia 2020 r. do 30 marca 2022 r. nie prowadzono rejestru dokumentów wydanych w związku z wydanym upoważnieniem, o którym mowa w § 7 ust. 1 Procedury postępowania w zakresie nadawania upoważnień do przetwarzania danych osobowych oraz § 16 ust. 3 PBI. Zgodnie z ww. unormowaniami po odbytym szkoleniu pracownicy składają oświadczenia o odbyciu szkolenia, a IODO prowadzi rejestr wydanych dokumentów.
- Do 26 marca 2022 r. nie prowadzono cyklicznych szkoleń okresowych personelu, co było niezgodne z § 16 ust. 1 PBI, który stanowił że takie szkolenie przeprowadza się nie rzadziej niż raz na trzy lata.

Dyrektor wyjaśnił, że do 30 marca 2022 r. IODO zaniechał swoich obowiązków wynikających z Procedury postępowania w zakresie nadawania/odwoływania upoważnień do przetwarzania danych osobowych i było to spowodowane jego długą nieobecnością. Nie był stanie wskazać terminów i tematyki szkoleń prowadzonych do 15 kwietnia 2021 r., zaś po tej dacie nie były one prowadzone. Wyjaśnił także, że po 23 lutego 2022 r. firma zewnętrzna, której pracownik pełnił funkcje IODO w Szpitalu poinformowała, że nie mogła udzielać upoważnień, tym samym w konsekwencji nie prowadzono takiej ewidencji. Brak szkoleń cyklicznych uzasadnił nieobecnością IODO w Szpitalu. Wskazał natomiast, że pracownicy po 23 lutego 2022 r. byli zachęcani do odbywania cyklicznych szkoleń, jednakże PBI do 5 czerwca 2023 r. nie przewidywała narzędzi pozwalających na weryfikację realizacji cyklicznych szkoleń pracowników. Zobligował przełożonych pracowników do zapewnienia po 2023 r. aby każdy pracownik odbył szkolenie, co ma być weryfikowane przez IODO.

(akta kontroli str. 319-322, 608-622, 710-747, 1129)

OCENA CZĄSTKOWA

W Szpitalu zostały stworzone rozwiązania organizacyjne i techniczne w obszarze bezpieczeństwa informacji, w tym przetwarzania danych o pacjentach, niemniej nie uwzględniały one niektórych wymagań wynikających z rozporządzenia KRI. Wdrożenie tych rozwiązań było natomiast nieadekwatne do rodzaju i skali przetwarzanych danych. W funkcjonującym do czerwca 2023 r. SZBI nie uwzględniono bowiem podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i przy pracy na odległość. Szkolenia osób zaangażowanych w proces bezpieczeństwa informacji i ochrony danych były nieodpowiednie i nieadekwatne do przyjętych w rozwiązań organizacyjnych w Szpitalu. Nie odbywały się bowiem cykliczne szkolenia przypominające we wspomnianym zakresie. Ponadto w okresie do 1 stycznia 2020 r. do 30 marca 2022 r. nie zapewniono rzetelnego potwierdzenia zrealizowanych szkoleń przez niektóre osoby zaangażowane w proces przetwarzania informacji. We właściwy sposób wyznaczono IODO, który posiadał odpowiednie kwalifikacje i niezależność organizacyjną. Nie zapewniono jednak wsparcia ADO przez IODO oraz powierzono mu zadania, których realizacja doprowadziła do konfliktu interesów. W skontrolowanym okresie, wszystkie przypadki

[41] Ustalono na podstawie liczby osób wykazanych w Sprawozdaniach z działalności Sekcji Bezpieczeństwa i Higieny Pracy, Ochrony Przeciwpożarowej oraz stanu BHP i P.POŻ w nadzorowanych jednostkach za lata 2020-2021.

naruszenia bezpieczeństwa informacji w tym danych osobowych, obsłużono z pominięciem zasad określonych w § 20 ust. 2 pkt 13 rozporządzenia KRI.

Opracowany i ustanowiony w 2019 r. SZBI we właściwy sposób uregulował procedury zarządzania bezpieczeństwem w systemie informatycznym. Określał on zasady dotyczące m.in. udzielania i odwoływania upoważnień do przetwarzania danych, prowadzenia analiz ryzyka, szkolenia osób zaangażowanych w proces przetwarzania danych osobowych oraz identyfikowania, ewidencjonowania i zgłaszania incydentów naruszenia bezpieczeństwa informacji. Przeglądy tego systemu zaowocowały jego udoskonaleniem dopiero w 2023 r.

OBSZAR

2. Funkcjonowanie przyjętych rozwiązań i ich wpływ na ochronę danych o pacjentach przed cyberatakami

Opis stanu faktycznego

2.1. W okresie objętym kontrolą w Szpitalu funkcjonowały 84 systemy i aplikacje medyczne[42]. Dane osobowe pacjentów przetwarzano w 35 z nich. Archiwizacja, przetwarzanie i udostępnianie danych związanych z realizacją procesu diagnostyczno - terapeutycznego[43] odbywały się m.in. w niżej wymienionych systemach:

- Optimed NXT[44], AMMS, Informedica – obsługa ruchu pacjentów w Szpitalu,
- Centrum, eLaborant, e-Lab – procesu realizacji badania od momentu pobrania materiału do wygenerowania wyniku,
- Infinitt Pacs, EchoPACK– dedykowany do przechowania, wyświetlania oraz zarządzania diagnostyczną informacją obrazową.

(akta kontroli str. 822)

2.2. W latach 2020-2023 zarządzanie siecią Szpitala odbywało się za pomocą usługi Active Directory, pozwalającej administratorowi sieci na centralne zarządzanie uprawnieniami użytkowników. Z poziomu jednego komputera mógł on także konfigurować urządzenia końcowe (komputery, laptopy, tablety), na których pracował personel.

Według stanu na 3 stycznia 2024 r. personel niemedyczny Szpitala[45] liczył 77 osób, z których 23 posiadały dostęp do dokumentacji medycznej przetwarzanej z wykorzystaniem Optimed NXT.

Analiza przydzielonych personelowi niemedycznemu uprawnień dostępu do systemów informatycznych wykazała m.in., że:

- dostęp do danych medycznych posiadało 19 osób[46], które wykonywały czynności pomocnicze przy udzielaniu świadczeń zdrowotnych oraz czynności związane z utrzymaniem systemu teleinformatycznego. Było to zgodne z art. 24 ust. 2 pkt 2 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i rzeczniku praw pacjenta[47],

[42] W tym 12 z nich wygaszonych.

[43] Obejmującymi dane o ruchu pacjentów (HIS), badaniach laboratoryjnych (LIS) i badań obrazowych (RIS).

[44] Analizę zasad przetwarzania danych osobowych w ww. wystąpieniu oparto na analizie sytemu Optimed NXT, jako podstawowym systemie typu HIS funkcjonującym w Szpitalu.

[45] Działach: Zaopatrzenia i zamówień publicznych, Rozliczeń i analiz medycznych, Informatyki, Technicznym, Epidemiologii i higieny szpitalnej, Finansowo-księgowym, Kadr i płac, Organizacyjnym, Sekcji BHP, Aptece, Dyrekcja, Kapelani, Specjalista ds. obronnych.

[46] Zatrudnionych w Dziale Informatyki (pięć osób), w Dziale Rozliczeń i analiz medycznych (6 osób), statystycy medyczni (3 osoby) oraz ich przełożony - Kierownik Działu Organizacyjnego, Dyrektor Szpitala, Kierownik Działu Epidemiologii i higieny szpitalnej, Zastępcy Dyrektora ds. Pielęgniarstwa oraz ds. Ekonomicznych.

[47] Dz. U. z 2023 r. poz. 1545, ze zm.

- cztery osoby posiadały dostęp do danych medycznych, mimo że nie wykonywały zadań, podczas których byłby on niezbędny (opisane w punkcie 1 sekcji stwierdzone nieprawidłowości),
- 10 osób posiadało stosowne, pisemne upoważnienia do przetwarzania danych osobowych, co było zgodnie z przepisem art. 29 oraz 32 ust. 4 rozporządzenia RODO. Takich upoważnień nie posiadało natomiast 13 pracowników (opisane w punkcie 2 sekcji stwierdzone nieprawidłowości),
- dostęp do systemu medycznego był możliwy wyłącznie po odpowiednim przeprowadzeniu autoryzacji, tj. podaniu loginu i hasła.

(akta kontroli str. 823-845)

2.3. Analiza uprawnień posiadanych przez personel medyczny przeprowadzona na próbie dotyczącej 30 z 338 pielęgniarek i położnych zatrudnionych w Szpitalu w latach 2020-2023 (I półrocze) wykazała m.in., że:

- 28 z nich posiadało dostęp do danych medycznych wyłącznie w zakresie wskazanym w upoważnieniu oraz w stopniu adekwatnym do realizowanych zadań i obowiązków. Dwie posiadały dostęp do danych pacjentów z oddziałów szpitalnych, na których nie świadczyły pracy (opisane w punkcie 5 sekcji stwierdzone nieprawidłowości),
- sześć z nich posiadało upoważnienia do przetwarzania danych osobowych pacjentów Szpitala wydane przez ADO. Pozostałe 24 pielęgniarki nie posiadały takich upoważnień (opisane w punkcie 3 sekcji stwierdzone nieprawidłowości),
- dwie pielęgniarki zostały dopuszczone do przetwarzania danych bez stosownego upoważnienia do ich przetwarzania oraz bez polecenia administratora. Posiadały one wprawdzie upoważnia do przetwarzania danych osobowych, jednak dotyczyły Oddziału Okulistycznego, zaś wykonywały pracę również w innych oddziałach (opisane w punkcie 5 sekcji stwierdzone nieprawidłowości).

(akta kontroli str. 846-931)

2.4. Analiza danych związanych z dostępem 69 pracowników[48], z którymi w okresie od 1 stycznia 2022 r. do 30 września 2023 r. rozwiązano stosunek pracy[49] wykazała, m.in.: że:

– 25 z nich odebrano uprawnienia dostępu do Optimed NXT przed dniem lub w dniu ustania stosunku pracy – 36,2% badanej próby,
– w przypadku 41 byłych pracowników dostęp do systemu odebrano im w terminie od 1 do 544 dni po jego rozwiązaniu – 59,4% (opisane w punkcie 6 sekcji stwierdzone nieprawidłowości),
– według stanu na 19 stycznia 2024 r., w trzech przypadkach byli pracownicy nadal posiadali dostęp do tych systemów – 4,3% (opisane w punkcie 6 sekcji stwierdzone nieprawidłowości),
– w rejestrze logowań do Optimed NXT w 67 przypadkach nie odnotowano aktywności loginów pracowników, z którymi rozwiązano stosunek pracy,
– w dwóch przypadkach stwierdzono logowanie się do systemu Optimed NXT przez byłych pracowników (opisane w punkcie 6 sekcji stwierdzone nieprawidłowości).

Wśród wcześniej wspomnianych 69 byłych pracowników, z 32 osobami zawarto kolejne umowy. W przypadku 20 z 32 tych pracowników posiadali one ważne upoważnienia, zaś w przypadku 12 (37,5%) – nie wystawiano nowych upoważnień do przetwarzania danych osobowych. Poprzednio wystawione im upoważnienia straciły

[48] Pracownicy w trakcie zatrudnienia mieli przyznany dostęp do danych zawartych w dokumentacji medycznej.
[49] W tym również świadczonej na podstawie umowy cywilnoprawnej.

ważność z chwilą ustania wcześniejszego stosunku pracy (opisane w punkcie 4 sekcji stwierdzone nieprawidłowości).

(akta kontroli str. 932-1029)

2.5. Według stanu na 9 stycznia 2024 r. w Szpitalu korzystano ze 338 stanowisk komputerowych. W wyniku oględzin przeprowadzonych w tym dniu w zakresie pięciu z nich[50] ustalono, m.in., że:

- żadne z nich nie było przypisane wyłącznie do jednego pracownika, tj. ze stanowisk tych mogli korzystać zarówno lekarze jak i pielęgniarki z danego oddziału,
- systemu operacyjnym na każdym stanowisku był Windows, ze środowiska którego zapewniony był dostęp do systemu Optimed NXT,
- użytkownicy tych stanowisk korzystali z indywidualnych kont domenowych tzw. zwykłego użytkownika (bez uprawnień administratora),
- w każdym przypadku dostęp do pulpitu użytkownika następował po podaniu wymaganych danych uwierzytelniających, tj. hasła o liczbie znaków od 8 do 9,
- dostęp do systemu Optimed NXT wymagał uwierzytelnienia loginem i hasłem, a liczba znaków we wpisywanych hasłach wynosiła od 8 do 12. Po zalogowaniu się do systemu Optimed NXT we wszystkich przypadkach zakres uprawnień nadanych w systemie był zgodny z zakresem uprawnień określonych na zajmowanym stanowisku,
- w przypadku czterech komputerów, porty USB były zablokowane w ustawieniach systemowych, zaś w jednym przypadku[51] po podłączeniu zewnętrznego nośnika pamięci możliwy był jego odczyt,
- wszystkie komputery posiadały dostęp do Internetu oraz miały zainstalowany program antywirusowy (Eset/FortiEDR) z aktualną na dzień oględzin bazą sygnatur antywirusowych,
- wszyscy użytkownicy korzystający z komputerów poddanych oględzinom posiadali dostęp do służbowej poczty email,
- w przypadku stanowiska K 1166 stwierdzono, że zalogowanym użytkownikiem do konta systemu operacyjnego Windows był użytkownik posiadający login „podbwero", zaś zalogowanym z tego środowiska do systemu Optimed NXT był inny użytkownik, którego login to „gorzgabr" (opisane w punkcie 7 sekcji stwierdzone nieprawidłowości).
- w przypadku jednego ze stanowisk komputerowych[52] stwierdzono, że folder „pobrane" zawierał pięć plików pdf oraz cztery pliki jpg z danymi osobowymi, którymi były m.in. imię, nazwisko, numer PESEL,
- na żadnym komputerze nie ustawiono blokady ekranu w taki sposób, aby następowała aktywacja wygaszacza ekranu po określonym czasie braku aktywności użytkownika.

Oględzinom poddano również ustawienia systemowe w zakresie wymagań stawianych hasłom użytkowników, które według stanu na 9 stycznia 2024 r. były ustawione w sposób odbiegający od wymagań określonych w punkcie 5.1.2. Polityki Bezpieczeństwa Informacji i Systemów IT stanowiącej załącznik nr 2 do zarządzenia 73/2023 oraz w punkcie 4.4.5. PODO – załącznik nr 6 (opisane w punkcie 8 sekcji stwierdzone nieprawidłowości).

(akta kontroli str. 608-617, 625-630, 1030-1034)

[50] Tj. trzech stanowisk, z których korzystały pielęgniarki, jednego lekarskiego oraz wspólnego na Izbie Przyjęć (stanowiska oznaczone K 1166, K1017, K 0107, K 1065, K 1107).
[51] Stanowisko lekarskie K 1065.
[52] K 1166.

2.6. W okresie objętym kontrolą Szpital zawarł 113 umów[53] powierzenia przetwarzania danych osobowych, w których występował jako podmiot powierzający przetwarzanie.

Od 5 czerwca 2023 r. w Szpitalu prowadzono wykaz zawartych umów powierzenia przetwarzania danych osobowych[54]. W wykazie tym zamieszczono tylko jedną z 54 umów, które pozostawały w realizacji według stanu na dzień wejścia w życie załącznika nr 16 do PODO stanowiącej część SZBI (opisane w punkcie 9 sekcji stwierdzone nieprawidłowości).

Szczegółowa analiza 5 z 113 ww. umów wykazała, że spełniały one wymagania określone w art. 28 rozporządzenia RODO, natomiast jedną z nich[55] zawarto, pomimo że w ramach jej realizacji nie dochodziło do powierzenia przetwarzania danych osobowych. Dyrektor wyjaśnił, że wymieniona „umowa powierzenia przetwarzania danych osobowych została zawarta w sposób nieprawidłowy".

(akta kontroli str. 668-669, 1035-1113)

Stwierdzone nieprawidłowości

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

1. Czterech pracowników Szpitala stanowiących personel niemedyczny według stanu na 3 stycznia 2024 r. posiadało dostęp do systemu Optimed NXT, tj. do dokumentacji medycznej zawierającej dane pacjentów, podczas gdy nie wykonywali oni czynności pomocniczych podczas udzielania świadczeń opieki zdrowotnej lub związanych z utrzymaniem systemu teleinformatycznego, zaś w zakresach ich nie powierzono im wykonywania ww. czynności. Powyższy dostęp polegał na tym, że specjaliście do spraw bezpieczeństwa i higieny pracy oraz trzem pracownikom Działu Organizacyjnego przyznano uprawnienia dostępu do wszystkich jednostek organizacyjnych Szpitala w roli: statystyka medyczna. Było to niezgodne z art. 24 ust. 2 pkt 2 ustawy o prawach pacjenta i rzeczniku praw pacjenta oraz naruszało wynikającą z art. 5 pkt 1 lit. c rozporządzenia RODO zasadę minimalizacji danych, tj. wymogu ograniczenia ich do tego co niezbędne do celów, w których były przetwarzane.

   Dyrektor wyjaśnił, że ww. specjaliście uprawnienia przyznane zostały na potrzeby sprawozdań statystycznych, natomiast trzem pracownikom Działu Organizacyjnego uprawnienia w roli: statystyka medyczna zostały przyznane z uwagi na wykonywane zastępstwa oraz obowiązki nałożone przez bezpośredniego przełożonego wynikające z potrzeb pracodawcy.

   Zdaniem NIK z zakresów czynności dwóch pracowników Działu Organizacyjnego wynikało, że mogli zastępować nieobecnego specjalistę lub specjalistę ds. organizacji, a nie statystyka medycznego. W trzecim zakresie czynności w ogóle nie wskazano zastępowanych osób bądź stanowisk.

   Na 9 lutego 2024 r. dostęp do systemu Optimed NXT został odebrany wszystkim ww. osobom.

   (akta kontroli str. 495-500, 823-845)

2. Personelowi niemedycznemu Szpitala (13 pracownikom) według stanu na dzień 30 stycznia 2024 r. umożliwiono dostęp do danych zawartych w dokumentacji medycznej bez upoważnienia do przetwarzania danych osobowych udzielonego przez ADO. Było to niezgodne z art. 29 oraz 32 ust. 4 rozporządzenia RODO, który stanowi, że każda osoba mająca dostęp do danych osobowych może je przetwarzać wyłącznie na polecenie administratora. Zgodnie zaś z § 4 ust. 1

[53] W tym: cztery umowy w 2020 r., 46 w 2021 r., 32 w 2022 r. i 31 w I półroczu 2023 r.
[54] Wg załącznika nr 16 do PODO.
[55] Na sukcesywną dostawę asortymentu chirurgicznego i implantów.

Procedury postępowania w zakresie nadawania/odwoływania upoważnień do przetwarzania danych osobowych do tego procesu mogą być dopuszczone wyłącznie osoby posiadające imienne upoważnienie nadane przez ADO lub działającego w jego imieniu IODO. Powyższy dostęp umożliwiono 13 pracownikom spośród 23 stanowiących personel niemedyczny Szpitala[56]. Pięć z tych 13 osób posiadało upoważnienie wystawione na czas określony, które utraciło ważność[57]. Kolejne cztery osoby posiadały upoważnienia wydane na poprzednio zajmowanym stanowisku[58]. Pozostałe cztery osoby nie posiadały takich upoważnień w ogóle.

Dyrektor wyjaśnił, że wynikało to z niedopełnienia obowiązku w tym zakresie. Wskazał, że każdy z pracowników realizował obowiązki zlecone przez pracodawcę, a tym samym, w jego ocenie, ADO polecił im wykonywanie tych zadań.

NIK zwraca uwagę, że uregulowania wewnętrzne Szpitala obligują ADO m.in. do nadawania imiennych upoważnień i ich odwołania.

(akta kontroli str. 618-622, 827)

3. W okresie od 19 kwietnia 2021 r. do 14 lutego 2022 r. pracownik Szpitala, który nie posiadał pełnomocnictwa do podpisywania upoważnień do przetwarzania danych osobowych upoważnił 393 osoby do ich przetwarzania[59]. Było to niezgodne z art. 29 oraz art. 32 ust. 4 rozporządzenia RODO, zgodnie z którymi administrator danych podejmuje działania w celu zapewnienia, by każda osoba fizyczna mająca dostęp do danych osobowych, przetwarzała je wyłącznie na podstawie upoważnienia ADO i na jego polecenie. W ww. okresie osoba wyznaczona na IODO nie świadczyła pracy. Konsekwencją powyższego było to, że w przypadku wspomnianych 393 osób nie doszło do ich skutecznego upoważnienia, tj. wykonania uprawnionej czynności zastrzeżonej dla ADO. Zatem powyższe 393 osoby nie posiadały upoważnienia do przetwarzania danych osobowych, a zapewniony im do tego dostęp był nieuprawniony.

   Z wyjaśnień pracownika Szpitala, który podpisał i opieczętował ww. druki upoważnień wynika, że działał na on prośbę nieobecnej wówczas w pracy IODO. Podał, że IODO przekazała mu swoją pieczęć imienną oraz, że nie został on upoważniony w tym zakresie przez ADO stosownym pełnomocnictwem.

   Dyrektor wyjaśnił, że pełni obowiązki Dyrektora od lipca 2023 r. i nie posiadał wiedzy dlaczego dopuszczono do przetwarzania danych na podstawie upoważnień wydanych przez tego pracownika.

   (akta kontroli str. 899-930, 1114-1128)

4. W latach 2022-2023, w przypadku 12 z 32 byłych pracowników Szpitala, z którymi zawarto kolejne umowy bądź kontrakty, według stanu na 31 stycznia 2024 r. nie wystawiano im nowych upoważnień do przetwarzania danych osobowych, mimo że ich wcześniejsze upoważnienia utraciły ważność.

   Dyrektor wyjaśnił, że nowych upoważnień do przetwarzania danych osobowych nie nadano przez niedopatrzenie.

   (akta kontroli str. 618-622, 1015-1029)

[56] Mający dostęp do Optimed NXT.
[57] 31 marca 2014 r., 15 października 2014 r., 30 kwietnia 2015 r. 28 lutego 2019 r. i 31 stycznia 2020 r.
[58] Statystyk medyczny miał upoważnienie do przetwarzania danych osobowych na stanowisku rzecznika prasowego i specjalisty ds. promocji; specjalista ds. organizacji na stanowisku statystyk medyczny; specjalista ds. organizacji na stanowisku sekretarka medyczna; specjalista informatyk na stanowisku statystyk medyczny.
[59] W tym 24 z 30 pielęgniarek i położnych objętych badaniem.

5. Według stanu na 15 stycznia 2024 r. dwóm pracownikom Szpitala nadano w systemie informatycznym uprawnienia dostępu do danych pacjentów leczonych w innych komórkach organizacyjnych Szpitala niż te, w których faktycznie wykonywały one swoją pracę, bowiem:
   - położna z Kliniki Ginekologii, Ginekologii Onkologicznej i Położnictwa posiadała uprawnienia w roli: pielęgniarka oddziałowa we wszystkich komórkach organizacyjnych Szpitala,
   - pielęgniarka z Oddziału Urologii i Onkologii Urologicznej posiadała uprawnienia w roli: pielęgniarka oddziałowa we wszystkich komórkach organizacyjnych, sekretarka medyczna na Oddziale Wewnętrznym oraz pielęgniarka w Pracowni RTG na Bloku Operacyjnym Głównym, na Bloku Operacyjnym Endoskopowym Urologii.

   Przyznanie tym osobom dostępu do danych zawartych w dokumentacji medycznej w ww. zakresie było niezgodne z § 20 ust. 2 pkt 4 rozporządzenia KRI, który obliguje kierownictwo podmiotu publicznego do podejmowania działań zapewniających, żeby osoby zaangażowane w proces przetwarzania informacji, uczestniczyły w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji. Nie było to również zgodne z zasadą „minimalizacji danych" – określoną w art. 5 pkt 1 lit. c rozporządzenia RODO, czyli ograniczenia przetwarzanych danych do tego, co niezbędne do celów, w których są przetwarzane. Dyrektor wyjaśnił, że w przypadku położnej i pielęgniarki na Oddziale Urologii i Onkologii Urologicznej szerszy zakres został przyznany omyłkowo, błąd został skorygowany, zakresy uprawnień zostały zweryfikowane oraz zawężone do zakresu niezbędnego do realizowania powierzonych zadań.

   (akta kontroli str. 495-500, 846-931)

6. Obowiązujące w Szpitalu procedury nie zapewniły bezzwłocznego odbierania uprawnień dostępów do systemów informatycznych pracownikom z którymi Szpital kończył współpracę. Nie gwarantowało to należytego bezpieczeństwa informacji, tj. istniała możliwość nieuprawnionego dostępu do tych informacji. Przyczyną natomiast było niezapewnienie w skuteczny sposób środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji, do czego obligował § 20 ust. 2 pkt 7 lit. c rozporządzenia KRI. Powyższa nieprawidłowość zaistniała w następujących przypadkach:

   - Uprawnień dostępu do systemu Optimed NXT nie odebrano 41 z 69 byłych pracowników niezwłocznie po zakończeniu z nimi stosunku pracy, w tym:
     - w 18 przypadkach w sytuacji, w której pracownicy nie wypełnili obowiązku rozliczenia karty obiegowej, która była podstawą do wyłączenia uprawnień. Uprawnienia odebrano dopiero po upływie od 71 do 544 dni od ustania zatrudnienia,
     - w 11 przypadkach uprawnienia odebrano pracownikom po terminie rozwiązania umowy, ale w terminie w którym rozliczyli kartę obiegową. Uprawnienia odebrano od 40 do 277 dni od ustania zatrudnienia,
     - dziewięciu pracownikom nie odebrano uprawnień po rozwiązaniu umowy mimo dostarczenia tej karty. Uprawnienia odebrano dopiero po upływie od 37 do 322 dni od ustania zatrudnienia,
     - w trzech pozostałych przypadkach, pracownicy rozliczyli kartę obiegową w Dziale IT, natomiast nie można określić daty jej rozliczenia.

Dyrektor wyjaśnił, że w przypadkach niedostarczenia przez pracowników karty obiegowej, uprawnienia zostały wyłączone w trakcie okresowego przeglądu 10 lipca 2023 r. mającego na celu dezaktywacje kont, które nie logowały się od początku poprzedniego roku.

Kierownik Działu Informatyki wyjaśnił, że konta byłych pracowników którzy rozliczyli kartę obiegową zostały zablokowane jedynie domenowo, natomiast nie zostały zablokowane w systemie Optimed NXT. Poinformował, że przyczyny tej sytuacji nie są do odtworzenia i należy przyjąć to za błąd ludzki. Nieodebranie w odpowiednim czasie uprawnień dostępu do sytemu Optimed NXT umożliwiło dwóm osobom zalogowanie się do niego po wcześniejszym ustaniu stosunku pracy. Miało to miejsce odpowiednio: 38 oraz 77 dni po tym zakończeniu stosunku pracy lub kontraktu.

Dyrektor wyjaśnił, że uprawnienia nie zostały odebrane na czas wskutek niedopatrzenia. Zgodnie z oświadczeniem Dyrektora, w obu przypadkach nie doszło do nieuprawnionego dostępu do danych pacjentów bez zgody Administratora Danych Osobowych.

NIK nie podziela powyższych wyjaśnień w części dotyczącej tego, że nie doszło do nieuprawnionego dostępu do danych pacjentów. Fakt zalogowania się do systemu zawierającego dane pacjentów osób, którym upoważnienie do przetwarzania danych osobowych wygasło w dniu rozwiązania umowy, już stanowi o nieuprawnionym dostępie.

(akta kontroli str. 608-617, 940-945, 1010-1160)

- Według stanu na 19 stycznia 2024 r. trzem osobom nie odebrano uprawnień do Optimed NXT, pomimo że zakończyły one prace odpowiednio: 31 marca 2023 r. (dwie osoby) oraz 31 grudnia 2022 r. Ich konta nadal były aktywne, a login jednej z nich wykazał aktywność po 77 dniach od rozwiązania stosunku pracy.

Dyrektor wyjaśnił, że pracownicy nie wypełnili obowiązku rozliczenia kart obiegowych, które były podstawą do wyłączenia uprawnień dostępu. Wskazał ponadto, że Dział Informatyki przy współpracy Działu Kadr i Płac dokonuje cyklicznych weryfikacji aktywności kont. Weryfikacje takie wykonano 6 lutego i 10 lipca 2023 r. Zaplanowano je również do powtórzenia w lutym 2024 r. Dyrektor mając na uwadze powyższe uchybienia, oświadczył że procedura odbierania uprawnień zostanie zweryfikowana i uszczelniona.

NIK zauważa, że w jednym przypadku karta obiegowa została rozliczona w Dziale Informatyki w dniu 17 listopada 2022 r., tj. 44 dni przed rozwiązaniem stosunku pracy z pracownikiem, co umożliwiało ustawienie daty ważności konta. Wskazane przez Dyrektora okresy cyklicznych weryfikacji aktywności kont nie gwarantowały bezzwłocznego odebrania dostępów osobom nieuprawnionym.

(akta kontroli str. 608-617, 940-945)

7. W trakcie oględzin NIK przeprowadzonych 9 stycznia 2024 r. pracownik personelu medycznego pracował w systemie informatycznym korzystając z konta innego użytkownika. Było to niezgodne z postanowieniami przyjętymi w PODO. O godzinie 9:20, na stanowisku komputerowym K1166 w systemie Optimed NXT zalogowana była pielęgniarka. Dostęp do ww. systemu uzyskała ona korzystając z aktywnego zalogowania konta innego użytkownika. Użytkownik tego konta zakończył pracę w dniu 8 stycznia 2024 r. o godz. 19:00, tj. w dniu poprzedzającym przeprowadzone oględziny. Zgodnie z uregulowaniami

Szpitala[60] niedopuszczalna była praca w systemie informatycznym na koncie innego użytkownika, a przy kończeniu pracy użytkownika w systemie wymagano jego wylogowania.

Dyrektor wyjaśnił, że wskazany przypadek nie skutkował nieupoważnionym dostępem do danych z uwagi na fakt, że sytuacja dotyczyła personelu pracującego na tym samym stanowisku komputerowym w tym samym zakresie uprawnień. Dyrektor oświadczył, że zostaną podjęte działania na rzecz zwiększenia świadomości użytkowników i uszczelnienia systemu.

(akta kontroli str. 608-617, 1016-1034)

8. Według stanu na 9 stycznia 2024 r. ustawienia systemowe domeny dotyczące wymagań złożoności haseł użytkowników były wyłączone, pomimo że uregulowania wewnętrzne Szpitala[61] obligowały do tego, żeby hasła składały się z przynajmniej z: jednej dużej, jednej małej litery, jednej cyfry i jednego znaku specjalnego. W trakcie oględzin NIK ustalono, że opcja wymagalności złożoności hasła była wyłączona co skutkowało tym, że zmiana hasła domenowego była możliwa na hasło niespełniające wymagań.

   Dyrektor wyjaśnił, że wymagania złożoności hasła zostały wyłączone, ponieważ system domenowy nie pozwalał definiować parametrów złożoności, a ustawienia domyślne narzucały nadmiarowe wymagania w stosunku do wymagań określonych w PBI. W jego ocenie wymagania określone w PBI nadmiernie komplikowały hasło (np. długa historia haseł i niemożność powtórzenia się dwóch tych samych liter co w loginie) powodując liczne problemy z utworzeniem i zapamiętaniem hasła przez użytkowników. Wskazał, że to mogło zwiększać ryzyko zapisywania przez użytkowników haseł na kartkach lub w innych miejscach.

   (akta kontroli str. 608-617, 1030-1034)

9. Wykaz zawartych umów powierzenia przetwarzania danych osobowych[62] wg stanu na 12 grudnia 2023 r. nie zawierał 53 z 54 (98,1%) umów jakie, pozostawały w realizacji według stanu na dzień wejścia w życie załącznika nr 16 do PODO stanowiącej część SZBI[63]. Umieszczono w nim wyłącznie umowy zawarte po 5 czerwca 2023 r. pomijając obowiązujące umowy zawarte przed tym dniem.

   Dyrektor wyjaśnił, że wprowadzony wykaz zawartych umów powierzenia miał na celu uregulowanie i zestawienie umów powierzenia zawartych po wprowadzeniu zarządzeniem załącznika nr 16 do PODO, tj. po 5 czerwca 2023 r. Dodał również, że 15 stycznia 2024 r. uzupełniono ten wykaz o wcześniej zawarte umowy.

   (akta kontroli str. 495-500, 1035-1113)

OCENA CZĄSTKOWA

W ocenie funkcjonowania przyjętych w Szpitalu rozwiązań organizacyjnych i technicznych w zakresie bezpieczeństwa informacji, w tym danych pacjentów, NIK stwierdził nieprawidłowości, które miały wpływ na działalność Szpitala w tym zakresie. Dotyczyły one m.in. przetwarzania danych osobowych przez 393 osoby wykonujące pracę w Szpitalu, tj. bez stosownego upoważnienia udzielonego przez ADO.

Nie w pełni przestrzegano również postanowień obowiązujących przepisów i regulacji wewnętrznych związanych z przetwarzaniem danych. Personelowi

[60] Punkty 16.12.3. i 16.12.4. PODO (załącznik nr 6 do zarządzenia 73/2023).
[61] Punkt 5.1.2. Polityki Bezpieczeństwa Informacji i Systemów IT (załącznik nr 2 do zarządzenia 73/2023), punkt 4.4.5. PODO (załącznik nr 6 zarządzenia 73/2023).
[62] Stanowiący załącznik nr 16 do PODO (załącznik nr 6 zarządzenia 73/2023).
[63] Na dzień 5 czerwca 2023 r.

administracyjnemu (17% badanych przypadków) oraz medycznemu (6% badanych przypadków) nadano uprawniania dostępu do systemu Optimed NXT w szerszym zakresie niż były niezbędny do realizacji ich zadań. Byłym pracownikom (63,8% ogółu) nie odbierano uprawnień niezwłocznie po zakończeniu z nimi stosunku pracy, co w dwóch przypadkach skutkowało nieuprawnionym dostępem do systemu Optimed NXT. Przyjęte procedury nie zapewniały niezwłocznego odbioru uprawnień i dostępów do systemów informatycznych pracownikom, z którymi Szpital kończył współpracę.

W toku kontroli NIK podjęto działania naprawcze, wskutek czego osobom wykonującym pracę w Szpitalu odebrano uprawnienia dostępu do systemów informatycznych, które były nieadekwatne do realizowanych przez nich zadań.

IV. Uwagi i wnioski

Uwzględniając podjęte w trakcie kontroli działania, w związku ze stwierdzonymi nieprawidłowościami, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK, przedstawia następujące wnioski:

Wnioski

1. Sporządzenie rejestru zasobów teleinformatycznych, zawierającego informację o elementach składowych tworzących infrastrukturę IT i zgodnego z wymogami SZBI.
2. Zmianę zakresu obowiązków POIN w zakresie powierzonych obowiązków dotyczących ochrony danych osobowych.
3. Podjęcie działań zmierzających do należytego dokumentowania naruszeń bezpieczeństwa informacji.
4. Zrealizowanie szkolenia z zakresu bezpieczeństwa informacji zgodnie z przyjętym harmonogramem lub planem.
5. Bezzwłoczne odbieranie uprawnień i dostępów do systemów informatycznych z dniem ustania stosunku pracy lub wygaśnięcia kontraktu.
6. Podjęcie działań zapewniających, że dostęp do danych będą posiadały osoby mające stosowne upoważnienie do przetwarzania danych osobowych zgodnie z zakresem uprawnień.

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

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

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

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

Olsztyn, 14 marca 2024 r.

Kontrolerzy

Agnieszka Kiełbik
Specjalista kontroli państwowej

.....
podpis

Joanna Majkowska
Starszy inspektor kontroli państwowej

.....
podpis

Najwyższa Izba Kontroli
Delegatura w Olsztynie
Dyrektor
z up. Piotr Wanic
Wicedyrektor

.....
podpis