NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.411.002.01.2018

07143918

Pan Grzegorz Tomaszuk
Dyrektor
Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Hajnówce
ul. Doc. Adama Dowgirda 9, 17-200 Hajnówka

WYSTĄPIENIE POKONTROLNE

R/18/002 – Ochrona danych osobowych pacjentów w Samodzielnym Publicznym Zakładzie Opieki Zdrowotnej w Hajnówce

NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku
ul. Akademicka 4, 15-267 Białystok
T +48 85 874 81 00, F +48 85 874 81 33
lbi@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Samodzielny Publiczny Zakład Opieki Zdrowotnej w Hajnówce (dalej: „Szpital" lub „ZOZ"), ul. Doc. Adama Dowgirda 9, 17-200 Hajnówka
Kierownik jednostki kontrolowanej	Grzegorz Tomaszuk, dyrektor od 30 sierpnia 2008 r.
Zakres przedmiotowy kontroli	1. Organizacja systemu zabezpieczenia danych osobowych pacjentów i danych medycznych. 2. Wdrożone i wykorzystywane rozwiązania techniczno-organizacyjne zapewniające bezpieczeństwo danych osobowych pacjentów i danych medycznych.
Okres objęty kontrolą	Od 1 stycznia 2018 r. do dnia zakończenia czynności kontrolnych. Badania kontrolne mogą dotyczyć działań sprzed tego okresu, jeśli mają 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 Białymstoku
Kontroler	Wojciech Zambrzycki, starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LBI/148/2018 z 10 października 2018 r. (akta kontroli str. 1)

[1] Dz. U. z 2017 r. poz. 524, ze zm. Ustawa zwana dalej: ustawą o NIK.

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

Szpital opracował i wdrożył dokumentację oraz procedury dotyczące ochrony danych osobowych, jednak ich aktualizacja nastąpiła dopiero po pięciu miesiącach od wejścia w życie przepisów 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 (ogólne rozporządzenie o ochronie danych)[3]. Nie wprowadzono natomiast kompleksowego systemu zarządzania bezpieczeństwem informacji, mimo takiego wymogu określonego w § 20 ust. 1 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[4]. Jedynie części personelu ZOZ zapewniono szkolenia związane z wejściem w życie RODO oraz zagadnieniami dotyczącymi bezpieczeństwa danych, naruszając tym samym przepisy § 20 ust. 2 pkt 6 rozporządzenia KRI.

Szpital właściwie zrealizował swoje obowiązki związane z przeprowadzeniem analizy procesów przetwarzania danych, dokonaniem oceny skutków przetwarzania danych osobowych i prowadzeniem rejestru czynności przetwarzania. Wprowadzone rozwiązania organizacyjne, zmierzające do zapewnienia ochrony danych osobowych pacjentów, gwarantowały poszanowanie ich prywatności. Personelowi szpitala zapewniono odpowiedni dostęp do danych medycznych. Wystąpiły jednak przypadki nadania pracownikom administracyjnym zbyt dużych uprawnień w systemach informatycznych oraz nieodbierania możliwości dostępu do tych systemów byłym pracownikom. Stanowiło to naruszenie art. 5 pkt 1 lit. c oraz § 20 ust. 2 pkt 5 rozporządzenia KRI.

NIK negatywnie ocenia praktyki personelu medycznego związane z nieblokowaniem komputerowych stacji roboczych podczas nieobecności w miejscu pracy, korzystaniem przez kilka osób z jednego konta użytkownika oraz przekazywaniem pomiędzy pracownikami danych (haseł) do autoryzacji w systemach informatycznych. Działania te stanowiły bowiem naruszenie regulacji wewnętrznych, określonych w rozdziale 5 pkt 5 RODO oraz pkt 6.2 ppkt. 1 Instrukcji Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Hajnówce[5]. NIK negatywnie ocenia również przypadki przekazania dostawcy oprogramowania danych osobowych i medycznych pacjentów, gdyż było to sprzeczne z regulacjami art. 24 ust 2 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta[6].

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

OBSZAR

1. Organizacja systemu zabezpieczenia danych osobowych pacjentów i danych medycznych

Opis stanu faktycznego

1.1. W § 8 pkt 2 lit. h) regulaminu organizacyjnego Szpitala z 20 września 2017 r. wskazano stanowisko Inspektora Ochrony Danych (dalej: *IOD*), jako samodzielne stanowisko pracy. W dalszej części tego regulaminu nie doprecyzowano jego obowiązków służbowych, jak zostało to uczynione w przypadku pozostałych samodzielnych stanowisk pracy. W myśl art. 8 i art. 10 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[8], Szpital terminowo wywiązał się z obowiązku zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu na stanowisko IOD Kierownika Sekcji Informatyki (28 sierpnia 2018 r. formularzem elektronicznym). Osoba ta do 24 maja 2018 r. pełniła obowiązki

---

[2] Najwyższa Izba Kontroli formuluje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.
[3] Dz. Urz. UE L 119 z 2016 r., str. 1, ze zm. Rozporządzenie zwane dalej: RODO.
[4] Dz. U. z 2017 r. poz. 2247. Rozporządzenie zwane dalej: rozporządzeniem KRI.
[5] Zwanej dalej: „IZSI".
[6] Dz. U. z 2017 r. poz. 1318, ze zm. Ustawa zwana dalej: ustawą o prawach pacjenta.
[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] Dz. U. poz. 1000.

Administratora Bezpieczeństwa Informacji. Przekazane zawiadomienie zawierało wszystkie elementy określone art. 10 ust. 3 ustawy o ochronie danych osobowych. Dane IOD oraz sposób i formę kontaktu udostępniono na stronie internetowej Szpitala – wymóg art. 37 ust. 7 RODO. (akta kontroli str. 2-78)

IOD umożliwiono wykonywanie obowiązków w sposób niezależny, stosownie do art. 38 ust. 3 RODO. Sekcja Informatyki, której IOD był kierownikiem, wchodziła w skład Działu Techniczno-Administracyjnego. Kierownik tego działu formalnie był przełożonym kierownika Sekcji Informatyki. Określał on sposoby i cele przetwarzania danych – w tym zakresie podlegał dyrektorowi Szpitala[9]. Dyrektor Szpitala wyjaśnił jednocześnie, że: *„zlecenia związane z informatycznym dostosowaniem wymagań związanych z wdrożeniem RODO zlecane są nie bezpośrednio kierownikowi sekcji informatyki, a firmie zewnętrznej, z którą mamy podpisaną umowę na obsługę informatyczną."* Osoba pełniąca funkcję IOD oraz kierownika Sekcji Informatyki miała poddział czasu pracy odpowiednio w stosunku $^1/_3$ do $^2/_3$. Spełniono zatem wymóg wskazany w art. 38 ust. 6 RODO wskazujący, że IOD może wykonywać inne obowiązki, ale administrator lub podmiot przetwarzający zapewniają aby takie zadania nie powodowały konfliktu interesów. (akta kontroli str. 2-78, 460-462)

Zgodnie z wymogami art. 37 ust. 5 RODO, IOD miał należyte przygotowanie i kwalifikacje zawodowe do pełnienia swojej funkcji. Wcześniej był Administratorem Bezpieczeństwa Informacji w kontrolowanym Szpitalu, od marca 2018 roku był słuchaczem studiów podyplomowych *Zarządzanie Bezpieczeństwem Informacji* na Politechnice Białostockiej i ukończył szkolenie, podczas którego nabył kompetencje do świadczenia usług związanych z ochroną danych osobowych w systemach informatycznych. (akta kontroli str. 6-8)

1.2. Przed wejściem w życie RODO w Szpitalu funkcjonowały:

- Polityka Bezpieczeństwa Informacji w Zakresie Danych Osobowych (dalej: PBI) z 8 lutego 2016 r. z dwoma załącznikami, mającymi taki sam tytuł – Struktura zbiorów danych osobowych, opis sposobu przepływu danych pomiędzy systemami oraz opis środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych, przy czym w załączniku nr 1 opisano oprogramowanie wdrożone w ramach projektu „Podlaski System Informacyjny e-Zdrowie", a w załączniku nr 2 pozostałe oprogramowanie,
- IZSI z 8 lutego 2016 r. z załącznikami: [1] parametry haseł; [2] procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu; [3] parametry Platformy Archiwizującej; [4] szczegółowe wytyczne dotyczące zabezpieczenia stref i systemów przetwarzających informacje niejawne.

(akta kontroli str. 79-118)

Po wejściu w życie RODO, IOD zaktualizował PBI i IZSI, których zaktualizowane wersje zostały przyjęte 20 listopada 2018 r. W PBI zmiany polegały m.in. na dodaniu zapisów dotyczących prawa dostępu do danych, prawa bycia zapomnianym, ograniczenia przetwarzania, prawa do przenoszenia danych i prawa do sprzeciwu oraz utworzeniu rejestru przetwarzania. Usunięte zostały też załączniki, które wymagane były w poprzednim stanie prawnym[10] (opis struktury zbiorów danych i sposobu przepływu danych pomiędzy systemami). W IZSI m.in. dodano osobę IOD i jego zadania, opisano sposób rozpoczęcia pracy w systemie informatycznym (czego wcześniej nie było) oraz zmieniony został okres ważności haseł z 30 na 90 dni. IOD wyjaśnił, że aktualizacji PBI i IZSI dokonał w listopadzie 2018 roku, ponieważ czekał na kodeks branżowy, który nie został jeszcze przyjęty.

(akta kontroli str. 119-152, 463-465)

---

[9] Według wytycznych Grupy Roboczej Art. 29 ds. Ochrony Danych, zawartych w dokumencie „Wytyczne dotyczące inspektorów ochrony danych ('DPO'), IOD nie może zajmować w organizacji stanowiska pociągającego za sobą określanie sposobów i celów przetwarzania danych. Ze względu na indywidualny charakter każdej organizacji ten aspekt powinien być analizowany osobno dla każdego podmiotu. Wytyczne dostępne na stronie internetowej https://www.giodo.gov.pl/pl/1520344/10390 dostęp z 20 listopada 2018 r.

[10] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922, ze zm.) utraciła moc 25 maja 2018 r.

IOD wyjaśnił, że nie pamięta w jaki sposób PBI i IZSI w 2016 roku zostały przekazane personelowi Szpitala. Zaktualizowane dokumenty zostały rozdysponowane zaś wśród kierowników działów z poleceniem zapoznania personelu z ich treścią.
(akta kontroli str. 463-465)

Uzupełnieniem IZSI stały się *Plan ciągłości działania* i *Procedurą Ochrony danych osobowych w fazie projektowania i domyślnej ochrony danych (Priacy by design)*.

Jako jeden z elementów Systemu Zarządzania Jakością, funkcjonowała Instrukcja udostępniania dokumentacji medycznej. Opisywała, w jaki sposób należy udostępniać dokumentację medyczną pacjentom oraz jakie inne organy mają do niej dostęp, wraz ze sposobem udostępniania tej dokumentacji. (akta kontroli str. 153-196)

W ZOZ nie została opracowana Polityka Bezpieczeństwa Informacji, o której mowa w § 2 pkt 15 rozporządzenia KRI, spełniająca wymogi § 20 ust. 1 powołanego rozporządzenia. Szerzej tę kwestię opisano w dalszej części wystąpienia, w sekcji *„Stwierdzone nieprawidłowości"*. (akta kontroli str. 365-367)

1.3. W dokumentach podstawowych (PBI, IZSI) nie określono konieczności opracowania dodatkowych reguł i procedur uszczegóławiających te dokumenty. (akta kontroli str. 79-196)

1.4. Szpital nie stosował kodeksu dobrych praktyk. Nie brał również udziału w tworzeniu medycznego kodeksu branżowego i nie wykorzystywał go w praktyce (nie został on zatwierdzony przez Prezesa Urzędu Ochrony Danych Osobowych[11]). Po ukazaniu się (24 września 2018 r.) przewodnika „RODO w służbie zdrowia"[12] IOD planował kolejne szkolenia z zakresu przedstawianych w nim schematów postępowania, jednak – jak wyjaśnił – *„przewodnik ten nie zawiera nowych wskazówek, które wcześniej nie zostały zakomunikowane personelowi Szpitala na przeprowadzonych szkoleniach"*. Szerzej na temat szkoleń będzie mowa w punkcie 1.8. wystąpienia. Najwyższa Izba Kontroli zwraca jednak uwagę, że zapoznanie personelu z treścią tego poradnika nie powinno być uzależniane od faktu już przeprowadzonych szkoleń. (akta kontroli str. 365-367, 463-465)

1.5. IOD prowadził rejestr czynności przetwarzania, czym spełnił obowiązek wskazany w art. 30 RODO. Obok formy papierowej była forma elektroniczna (excel) tego rejestru. Według stanu na 25 października 2018 r. liczył on 19 pozycji, zawierających wszystkie dane wymagane art. 30 ust. 1 RODO. (akta kontroli str. 197-218)

1.6. Stosownie do art. 32 RODO, w dniach 21 – 22 maja 2018 r., IOD przeprowadził analizę procesów przetwarzania danych osobowych pacjentów Szpitala dla ośmiu ryzyk, przypisując im wartość oszacowanego ryzyka: [1] ryzyko nieobecności (hospitalizacja) dyrektora – 1 pkt; [2] ryzyko nieobecności (hospitalizacja) kierownika Sekcji Informatyki – 1 pkt; [3] zagrożenie ujawnienia danych przez personel medyczny – 4 pkt; [4] awaria fizyczna serwera – 3 pkt; [5] awaria fizyczna urządzenia sieciowego – 1 pkt; [6] brak dostępu do Internetu – 1 pkt; [7] brak aktualizacji powodujący włamanie do systemów HIS i ERP – 4 pkt; [8] pożar budynków Szpitala, powódź – 3 pkt. Akceptowalna była wartość ryzyka oszacowanego na 1 pkt. W pozostałych przypadkach w analizie wskazano, że sposobem postępowania z ryzykiem będzie *„redukcja ryzyka"* – nie wskazano jednak w jaki sposób. IOD wyjaśnił, że: *„polegać by to miało na wprowadzeniu różnych procedur organizacyjnych, technicznych, dostosowaniu procedur zabezpieczeń do właściwego stanu i ograniczenia ryzyka. Czynności te wykonuję cały czas, jest to proces bieżący"*.
(akta kontroli str. 219-223, 365-367, 463-465)

1.7. Stosownie do art. 35 RODO, w dniach 23 – 24 maja 2018 r. IOD przeprowadził ocenę skutków dla ochrony danych osobowych, zawierającą wszystkie elementy wymagane ust. 7 powołanego przepisu. Wysokie ryzyko oszacowano w związku z zagrożeniem nieuprawnionego dostępu do danych pacjenta i pracownika Szpitala, w związku z tym rekomendowano zwiększenie zabezpieczenia programowego i konfiguracyjnego systemów

[11] Projekt medycznego kodeksu branżowego przygotowała Polska Federacja Szpitali. W dniu 13 listopada 2018 r. został on złożony prezesowi Urzędu Ochrony Danych Osobowych, w celu zatwierdzenia, http://www.rodowzdrowiu.pl/wp-content/uploads/2018/11/2018-11-13-KODEKS-BRAN%C5%BBOWY-Wniosek-o-zatwierdzenie-kodeksu-postepowania.pdf – dostęp z 4 grudnia 2018 r.

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

informatycznych oraz zwiększenie zabezpieczeń organizacyjnych poprzez wdrożenie odpowiednich procedur postępowania, uzupełnione szkoleniami personelu. Wysokie ryzyko zostało również oszacowane w związku z zagrożeniem nieuprawnionego ujawnienia lub udostępnienia danych osoby, w związku z tym rekomendowano zwiększenie zabezpieczeń organizacyjnych poprzez procedury postępowania, szkolenia personelu i audyt miejsc, w których przetwarzane były dane osobowe. Dla pozostałych zagrożeń: [1] nieuprawnione zniszczenie, utrata lub uszkodzenie danych osoby, [2] nieuprawniona modyfikacja danych osoby, [3] kradzież tożsamości lub jej utrata przez osobę, [4] naruszenie zakazu dyskryminacji, [5] szkoda finansowa wobec osoby, [6] szkoda wizerunkowa – ryzyko ustalono na poziomie typowym, z rekomendacją szkoleń personelu i okresowych audytów. IOD wyjaśnił, że: *„szkolenia już były przeprowadzone, czekaliśmy na kodeks branżowy, ale nie został póki co wprowadzony, a „Przewodnik po RODO" ma zbieżną treść z tą prezentowaną na szkoleniach. Odpowiednia częstotliwość takich szkoleń to na przykład co trzy miesiące. Dużą wiedzą będzie dla mnie też wynik kontroli NIK i na podstawie zaprezentowanych z niej ustaleń, będzie można podjąć dalsze decyzje o zagadnieniach, jakie należy zaprezentować podczas szkoleń lub co powinno być przedmiotem audytu".* (akta kontroli str. 224-230, 365-367, 463-465)

Analizę procesów przetwarzania danych osobowych oraz ocenę skutków dla ochrony danych osobowych IOD przeprowadził, posiłkując się formularzami (pliki excel), do których miał dostęp w serwisie LEX, oraz wiedzą zasięgniętą od wykładowców akademickich.
(akta kontroli str. 463-465)

1.8. Jednym z zadań IOD, w myśl art. 39 ust. 1 lit. b RODO, jest prowadzenie szkoleń personelu uczestniczącego w operacjach przetwarzania danych. Po wejściu w życie przepisów RODO, pomiędzy 18 czerwca a 20 lipca 2018 r., jedynie 179 z 438[13] (41%) pracowników Szpitala zostało objętych szkoleniem w formie warsztatów, przeprowadzanych przez IOD, co szerzej opisano w dalszej części wystąpienia, w sekcji *„Stwierdzone nieprawidłowości"*. Szkolenia te obejmowały m.in. ogólną charakterystykę aktów prawnych w zakresie ochrony danych osobowych, omówienie obowiązku informacyjnego, konieczność zgłaszania naruszeń, anonimowość pacjentów na każdym etapie procesu leczenia, postępowanie z danymi pacjenta, omówienie praktyk związanych z ochroną danych osobowych (polityka czystego biurka, logowanie do systemu, polityka kluczy).
(akta kontroli str. 231-234, 466)

Jednocześnie 77 pracowników Szpitala wysłuchało 18 września 2018 r. wykładu pt.: *„Prawa i obowiązki personelu medycznego w związku z wejściem w życie RODO"*, który wygłosił radca prawny z zewnętrznej kancelarii, specjalizującej się w prawie medycznym i gospodarczym[14]. (akta kontroli str. 231-232)

1.9. Szpital 15 listopada 2018 r. otrzymał zawiadomienie o wszczęciu wobec niego postępowania administracyjnego w sprawie uznania go za świadczącego usługę kluczową[15]. Do zakończenia kontroli nie otrzymał jednak od organu właściwego ds. cyberbezpieczeństwa (Ministra Zdrowia) decyzji administracyjnej w tej sprawie. W myśl art. 5 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[16], operatorem usługi kluczowej jest podmiot, wobec którego organ właściwy ds. cyberbezpieczeństwa[17] wydał decyzję o uznaniu za operatora usługi kluczowej. Jeśli ZOZ zostałby uznany za taki podmiot, nakłada to na niego szereg obowiązków wskazanych w rozdziale 3 powołanej ustawy. Rodzaj podmiotów, jakie mogą być uznane za operatorów usługi kluczowej określa załącznik nr 1 do powołanej ustawy (podmioty lecznicze, o których mowa w art. 4 ust. 1 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej[18], mogą być uznane za operatorów usługi kluczowej). Wykaz usług kluczowych znajduje się w załączniku do rozporządzenia Rady Ministrów z dnia 11 września 2018 r.

---

[13] Stan na 31 października 2018 r.
[14] Wykład miał miejsce w budynku Szpitala.
[15] Usługa kluczowa to taka, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienioną w wykazie usług kluczowych.
[16] Dz. U. poz. 1560.
[17] Wymieniony w art. 41 powołanej ustawy.
[18] Dz. U. z 2018 r. poz. 160, ze zm.

w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych[19]. (akta kontroli str. 235-237)

Stwierdzone nieprawidłowości

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

1. Nie opracowano Polityki Bezpieczeństwa Informacji, o której mowa w § 2 pkt 15 rozporządzenia KRI, spełniającej wymogi § 20 ust. 1 tego rozporządzenia. W Szpitalu funkcjonowały PBI, IZSI i pojedyncze procedury, ale nie obejmowały one kompleksowo zagadnień związanych z zarządzaniem bezpieczeństwem informacji. IOD wyjaśnił, że nie wiedział o takim obowiązku i posiadał tylko część takiego systemu, związaną z ochroną danych osobowych. (akta kontroli str. 365-367, 463-465)
2. IOD nie wywiązał się w pełni z obowiązku prowadzenia szkoleń personelu uczestniczącego w operacjach przetwarzania danych, wynikającego z art. 39 ust. 1 lit. b RODO. Po wejściu w życie przepisów RODO, pomiędzy 18 czerwca a 20 lipca 2018 r., jedynie 179 z 438[20] (41%) 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. IOD wyjaśnił, że taka liczba osób przeszkolonych wynika ze specyfiki pracy Szpitala. *„Nie zawsze można zebrać więcej osób. Uczestnicy szkoleń – m.in. pielęgniarki oddziałowe, ordynatorzy – mieli przekazać pozostałym osobom zdobytą wiedzę. Poza tymi szkoleniami, prowadziłem indywidualne konsultacje z zagadnień RODO dla pozostałych osób. Planujemy dalsze podnoszenie wiedzy z zakresu ochrony danych osobowych wśród pracowników, szczególnie osób, które nie uczestniczyły w poprzednich szkoleniach".* Cykle szkoleń rozpoczęto przeprowadzać już po wejściu w życie RODO. IOD wyjaśnił, że na początku dużo rzeczy było niejasnych i czekał na przewodnik po RODO. *„Nie wiedziałem co miałbym przekazać na szkoleniach. Nie chciałem skupić się na cytowaniu przepisów, ale na aspektach praktycznych, co robić, jak się zachowywać. Widząc, że nie ma takich praktycznych wskazówek, posiłkując się informacjami zdobytymi z innych źródeł (artykuły prasowe, doniesienia medialne, wiedza ze studiów), zacząłem realizować te szkolenia w formie warsztatów."*

(akta kontroli str. 231-234, 465-466)

OCENA CZĄSTKOWA

ZOZ wywiązał się z obowiązku opracowania i wdrożenia dokumentacji oraz procedur dotyczących ochrony danych osobowych, jednak ich aktualizacja nastąpiła dopiero po pięciu miesiącach od wejścia w życie RODO, a przyjęty przez Szpital system zarządzania bezpieczeństwem informacji nie w pełni odpowiadał wymogom § 20 ust. 1 rozporządzenia KRI. Przeprowadzono analizę procesów przetwarzania danych, ocenę skutków przetwarzania danych osobowych i właściwie prowadzono rejestr czynności przetwarzania, jednak tylko części personelu ZOZ zapewniono szkolenia związane z wejściem w życie przepisów RODO oraz zagadnieniami dotyczącymi bezpieczeństwa danych.

OBSZAR

2. Wdrożone i wykorzystywane rozwiązania techniczno-organizacyjne zapewniające bezpieczeństwo danych osobowych pacjentów i danych medycznych

Opis stanu faktycznego

2.1. W celu właściwej ochrony danych osobowych w ZOZ funkcjonowały poniżej wymienione rozwiązania.

- Przed okienkami rejestracji wyznaczona była linia (ok. 2 m przed), za którą oczekiwali kolejni pacjenci. IOD wyjaśnił, że: *„pacjenci wiedzą, że nie powinni przekraczać linii i oczekiwać poza nią. Takie rozwiązanie funkcjonuje w SP ZOZ w Hajnówce od kwietnia 2018 r."* W trakcie oględzin pacjenci niebędący bezpośrednio przy okienku rejestracji, nie wchodzili poza wyznaczoną linię.

[19] Dz. U. poz. 1806.
[20] Stan na 31 października 2018 r.

- Nad okienkiem rejestracji znajdowała się informacja, że w związku z RODO Szpital zachowuje w tajemnicy dane osobowe, zatem pracownicy ZOZ nie wymawiają ich na głos i jednocześnie nie proszą o ich podawanie przez pacjentów, ale wymagane jest okazanie dowodu osobistego w celu weryfikacji danych. Obok na tablicy informacyjnej znajdowała się informacja o przetwarzaniu danych, na której wskazano m.in. administratora, IOD, cele i podstawy przetwarzania danych, ich kategorie, odbiorców, okres przechowywania danych oraz prawo do dostępu, sprostowania, przenoszenia, wnoszenia skargi.
- W obrębie wzroku pacjentów rejestrujących się na świadczenia medyczne nie znajdowały się dane osobowe innych pacjentów.
- Podczas rejestracji do gabinetu lekarza podstawowej opieki zdrowotnej pacjentowi przydzielany był kolejny numer, który przypinano do historii choroby. Pacjenci do gabinetu tej poradni wywoływani byli poprzez werbalne podanie przez lekarza kolejnego numeru.
- Podczas rejestracji pacjentów do poradni specjalistycznych pacjent otrzymywał karteczkę z datą i planowaną godziną przyjęcia oraz numerem w kolejce[21]. Wywoływanie pacjentów do poszczególnych gabinetów[22] odbywało się za pomocą wyświetlacza przytwierdzonego na suficie, na którym pojawiała się informacja z numerem pacjenta oraz numerem gabinetu, towarzyszył temu komunikat głosowy. Do pozostałych poradni pacjenci byli proszeni przez lekarzy, bez używania danych osobowych. IOD oświadczył, że: *„do poradni urazowo-ortopedycznej i chirurgicznej numery pacjentów, którzy powinni udać się do gabinetu lekarza, ukazują się na jednej tablicy świetlnej. Aby rozwiązanie to mogło funkcjonować dla pozostałych poradni, konieczne jest dokupienie jeszcze jednej takiej tablicy, a personel poradni ginekologicznej nie zgłaszał potrzeby korzystania z tego urządzenia".*
- W dwóch z trzech objętych oględzinami gabinetów poradni specjalistycznych dokumentację pacjentów przechowywano we właściwy sposób. W jednym zaś karty pacjenta leżały na biurku lekarza. Szerzej opisano to w dalszej części wystąpienia, w sekcji *„Stwierdzone nieprawidłowości"*.
- W dyżurkach pielęgniarskich na czterech objętych oględzinami oddziałach szpitalnych ruch chorych[23] prowadzony był w miejscu niewidocznym dla osób postronnych (dane pacjentów były ukryte). Podręczna dokumentacja pielęgniarska przechowywana była w zamykanych gablotach. Podobne zamykane miejsca do przechowywania dokumentacji medycznej znajdowały się w gabinetach lekarskich. W salach chorych łóżka oznaczono kodem[24], a pacjenci posiadali na nadgarstkach opaski z numerem księgi, inicjałami i nazwą oddziału. Nie były to wydruki ze specjalistycznych drukarek zakupionych w ramach projektu *Podlaski System Informacyjny e-Zdrowie* za 12,4 tys. zł.
- Personel pielęgniarski, opuszczając dyżurkę pielęgniarek, pozostawił w dwóch z czterech objętych oględzinami oddziałów szpitalnych, uruchomione komputery i nie zablokował dostępu do systemu komputerowego. Szerzej opisano to w dalszej części wystąpienia, w sekcji *„Stwierdzone nieprawidłowości"*. W trakcie kolejnych oględzin na oddziałach szpitalnych stwierdzono również niewłaściwe postępowanie z hasłami do systemu komputerowego oraz logowanie się pracowników na nie swoje konta użytkownika, co również opisano w sekcji *„Stwierdzone nieprawidłowości"*.
- Sposób udostępniania kopii dokumentacji medycznej został uregulowany w instrukcji, stanowiącej element Systemu Zarządzania Jakością. Do 25 października 2018 r. do ZOZ wpłynęło 400 wniosków o udostępnienie kopii dokumentacji medycznej od instytucji oraz 1.400 wniosków od osób fizycznych. Analizą objęto wszystkie 20 spraw, w których wnioskodawcą była firma ubezpieczeniowa[25] oraz 51 spraw, gdzie odbioru dokumentacji medycznej nie dokonał sam pacjent, a osoba upoważniona (wśród

[21] Numer ten był pochodną planowanej godziny przyjęcia, np. wizyta planowana na godzinę 10:45 oznaczała, że pacjent miał przypisany numer 1045.

[22] Spośród sześciu poradni znajdujących się w obrębie tego samego korytarza, do dwóch pacjenci byli wywoływani za pomocą wyświetlacza oraz komunikatem głosowym.

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

[24] Numer sali / numer łóżka, np. sala 3 łóżko 2 to 3/2.

[25] Zapytania sądów, prokuratur, ZUS, KRUS, NFZ, Policji i ABW nie były objęte analizą.

tych spraw 13 dotyczyło odbioru dokumentacji dziecka przez rodzica). Stosownie do art. 26 ust. 1 ustawy o prawach pacjenta, w każdej ze spraw, gdzie było to wymagane, znajdowało się upoważnienie do udostępnienia kopii dokumentacji medycznej. (akta kontroli str. 242-252, 452-453)

2.2. Personel działów administracyjnych[26] Szpitala liczył 49 osób, z których 16 posiadało dostęp do systemu HIS[27], w tym dwie osoby, które nie wykonywały już obowiązków wymagających takiego dostępu. Będzie o tym mowa w dalszej części wystąpienia, w sekcji *„Stwierdzone nieprawidłowości"*. Pozostałych 14 osób zatrudnionych w Sekcji Informatyki (trzy osoby) oraz Sekcji Planowania, Monitorowania Świadczeń Zdrowotnych i Statystyki Medycznej (11 osób) posiadało dostęp do systemu HIS, w myśl art. 24 ust. 2 pkt 2 ustawy o prawach pacjenta, zgodnie z którym osoby wykonujące czynności pomocnicze przy udzielaniu świadczeń zdrowotnych, a także czynności związane z utrzymaniem systemu teleinformatycznego są uprawnione do dostępu do danych medycznych, na podstawie upoważnień administratora danych. Uprawnienia tym osobom oraz innym pracownikom, również medycznym, były jednak wydawane z opóźnieniem, co szerzej opisano w dalszej części wystąpienia, w sekcji *„Stwierdzone nieprawidłowości"*. W tej sekcji opisano również udzielanie upoważnień pracownikom Działu Higieny Szpitalnej, które nie powinny być wydane. (akta kontroli str. 267-286)

2.3. Na próbie 54 (z 269) pielęgniarek i położnych zatrudnionych w Szpitalu stwierdzono, że jedna z nich (1,9%) posiadała dostęp w systemie HIS do pacjentów z innych oddziałów szpitalnych, a nie tylko z oddziału, na którym świadczyła pracę. Jak wyjaśnił IOD, wynikało to z niepoinformowania Sekcji Informatyki przez służby kadrowe o zmianie stanowiska pracy pielęgniarki i wynikającej z tego potrzebie zmiany uprawnień.
(akta kontroli str. 255-266, 463-465, 467)

2.4. Od 1 stycznia do 19 października 2018 r. 47 osób zakończyło zatrudnienie w Szpitalu. Spośród nich, 30 w trakcie zatrudnienia miało przyznany dostęp do systemów informatycznych. Dostęp ten 22 osobom został odebrany podczas przeglądu posiadanych uprawnień, co – jak wyjaśnił IOD – miało miejsce latem 2018 roku[28]. Ośmiu byłych pracowników w dniu analizy NIK nadal posiadało możliwość dostępu do systemów informatycznych, o czym będzie mowa w dalszej części wystąpienia, w sekcji *„Stwierdzone nieprawidłowości"*. (akta kontroli str. 369-373)

2.5. Szpital był uczestnikiem projektu *Podlaski System Informacyjny e-Zdrowie*. Dla posiadanego oprogramowania miał uruchomioną usługę zdalnego zgłaszania dostawcy oprogramowania usterek w działaniu oprogramowania. Usterki były zgłaszane online. Usługa IZGL służyła do zgłaszania usterek dla oprogramowania używanego w części administracyjnej ZOZ, a NCR do oprogramowania związanego z ruchem chorych. Analiza wszystkich zgłoszeń wykonanych za pomocą NCR w 2018 roku (do 18 października) wykazała, że w 22 zgłoszeniach serwisowych zostały podane personalia pacjenta, PESEL lub opis procesu leczenia, co opisano poniżej, w sekcji *„Stwierdzone nieprawidłowości"*. W innych sytuacjach Szpital podawał numer ID pacjenta – indywidualny numer przypisywany pacjentowi w użytkowanym oprogramowaniu. ZOZ miał zawartą (22 maja 2018 r.) umowę powierzenia przetwarzania danych osobowych z dostawcą oprogramowania, któremu zgłaszał wspomniane usterki. (akta kontroli str. 386-451)

Stwierdzone nieprawidłowości

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

1. W jednym z trzech gabinetów lekarskich, w których przeprowadzano oględziny, karty historii choroby pacjentów znajdowały się na biurku lekarza przyjmującego w tym gabinecie. Stwarzało to niebezpieczeństwo ujawnienia danych pacjentów osobom postronnym – innym pacjentom. W myśl art. 13 ustawy o prawach pacjenta, pacjent

[26] Dział Ekonomiczny, Dział Techniczno-Administracyjny z Sekcją Informatyki, Sekcją Elektrotechniki i Aparatury Medycznej, Sekcją Zaopatrzenia i Zamówień Publicznych, Sekcja Służb Pracowniczych i Płac, Sekcja Planowania, Monitorowania Świadczeń Zdrowotnych i Statystyki Medycznej oraz samodzielne stanowiska pracy: radca prawny, specjalista ds. BHP, specjalista ds. komunikacji medialnej.

[27] Hospital Information System – rodzaj oprogramowania do obsługi ruchu pacjentów wewnątrz podmiotu leczniczego.

[28] IOD nie pamiętał dokładnej daty. Były to miesiące lipiec lub sierpień. Użytkownicy zostali trwale usunięci, a nie zablokowani, co uniemożliwiło ustalenie dokładnej daty.

ma prawo do zachowania w tajemnicy przez osoby wykonujące zawód medyczny informacji z nim związanych, uzyskanych w związku wykonywaniem tego zawodu. Lekarz pracujący w tym gabinecie oświadczył, że zazwyczaj przechowuje dokumentację medyczną w innym miejscu. Dyrektor wyjaśnił, że upomniał lekarza i zobligował go do gromadzenia kart pacjentów w miejscu znajdującym się poza zasięgiem wzroku osób postronnych. (akta kontroli str. 247-248, 456-459)

Fakt przechowywania kart pacjentów w obrębie wzrok osób postronnych został wpisany do rejestru naruszeń bezpieczeństwa prowadzonego przez IOD.
(akta kontroli str. 239-241)

2. W dwóch z czterech oddziałów szpitalnych, w których przeprowadzono oględziny, personel pielęgniarski, opuszczając dyżurkę pielęgniarek, pozostawił uruchomione wszystkie cztery komputery, nie blokując na nich systemu Windows, a na jednym z komputerów dodatkowo uruchomiony był system HIS. Stosownie do pkt 6.2 ppkt. 1 obowiązującej w Szpitalu IZSI[29], *„w przypadku zawieszenia pracy w systemie informatycznym w związku z tymczasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest do zablokowania dostępu do użytkowanego systemu komputerowego, w tym również do informacji prezentowanych na jego wyświetlaczu"*. Stosownie zaś do pkt 4 – 6 załącznika nr 2 do IZSI *„użytkownik zabezpiecza stację roboczą w czasie przebywania poza swoim stanowiskiem pracy"*, *„w trakcie zawieszenia pracy użytkownik wylogowuje się z systemu zapisując uprzednio wprowadzone dane"* oraz *„ma obowiązek zamykania systemu lub programu po zakończeniu pracy; stanowisko komputerowe z uruchomionym systemem lub programem nie może zostać bez kontroli pracującego na nim pracownika"*. (akta kontroli str. 97-118, 249-250)

Według Dyrektora Szpitala zachowanie personelu w trakcie oględzin było właściwe, zgodne z obowiązującym rozporządzeniem dotyczącym ochrony danych osobowych, a dostęp do danych medycznych był zabezpieczony. Dodał, że praca w punkcie pielęgniarskim czy też gabinecie lekarskim odbywa się w programie HIS po podaniu loginu i hasła, a w innych programach nie są wykonywane inne czynności. Dane przechowywane są tylko w bazie danych sytemu HIS na serwerze. Według Dyrektora, IZSI nakłada obowiązek zabezpieczenia danych przed wglądem osób trzecich i wystarczy wylogowanie się z systemu HIS, które całkowicie zabezpiecza dane pacjentów przed niepowołanym dostępem osób postronnych. Jednocześnie dostęp do stacji roboczych jest utrudniony poprzez centralną blokadę urządzeń typu dysk zewnętrzny i pendrive, co uniemożliwia wgrywanie złośliwych programów. Całkowite wylogowanie z systemu Windows następuje w momencie końca pracy na oddziale bądź konieczności używania stacji roboczej przez inny personel medyczny. Dyrektor za niewłaściwe uznał zachowanie jednej z pielęgniarek, która opuściła miejsce pracy nie wylogowując się z systemu HIS. Została ona pouczona. Według niej jej zachowanie spowodowane było stresem spowodowanym kontrolą, ale IOD uczestniczący w oględzinach był osobą upoważnioną i dane pacjentów nie były narażone na ujawnienie. (akta kontroli str. 456-459)

Wyjaśnienia Dyrektora Szpitala wskazują na rozbieżność między wymogami IZSI a stosowaną w Szpitalu praktyką postępowania.

Pozostawienie komputera z uruchomionym systemem HIS zostało wpisane do rejestru naruszeń bezpieczeństwa prowadzonego przez IOD. (akta kontroli str. 239-241)

3. Użytkownicy systemu Windows przekazywali między sobą hasła dostępu do tego systemu oraz wykorzystywali podczas pracy jedno konto użytkownika. Miało to miejsce w trzech z pięciu objętych oględzinami oddziałów szpitalnych. Dodatkowo na dwóch z tych oddziałów hasło dostępu do systemu operacyjnego było zapisane i przechowywane w umówionym miejscu. Stosownie do rozdziału 5 pkt 5 IZSI[30], *„ujawnianie przez użytkownika komukolwiek, jakichkolwiek aktualnych lub poprzednich*

[29] W dniu oględzin obowiązywała IZSI z 8 lutego 2016 r.
[30] W dniu oględzin obowiązywała IZSI z 20 listopada 2018 r.

haseł tymczasowych, haseł osobistych, haseł do kont uprzywilejowanych lub innych haseł powierzonych, jest surowo zabronione". (akta kontroli str. 131-152, 452-453)

Według wyjaśnień personelu pielęgniarskiego, logowanie się na konto innego użytkownika spowodowane było różnymi przyczynami:

- faktem zapomnienia dotychczasowego hasła – logowanie następowało na konto innego pracownika po uzyskaniu od niego hasła dostępu, a ze względu na konieczność szybkiego wykonywania swoich obowiązków – nie było sposobności do kontaktu z Sekcją Informatyki w celu uzyskania nowego hasła w miejsce zapomnianego (na dwóch oddziałach),
- na jednym oddziale było to typowe działanie – zawsze logowano się na konto jednej osoby, a hasło było przekazywane na bieżąco.

Na oddziale, gdzie działanie związane z logowaniem na jedno konto użytkownika przez wszystkie osoby personelu pielęgniarskiego było typowe, pielęgniarka oddziałowa wyjaśniła, że hasło przekazała w celu usprawnienia pracy. Na jej koncie użytkownika znajdywały się szablony dokumentów niezbędnych w codziennej pracy oraz na bieżąco uzupełniane sprawozdania. Dodała, że zgłaszała Sekcji Informatyki, że komputery działają na jej haśle i hasła miały być zmieniane. Jednocześnie, według niej, w razie potrzeby zrestartowania hasła do jej profilu użytkownika systemu Windows, pracownicy Sekcji Informatyki podawali nowe hasło personelowi (Kierownik Sekcji Informatyki zaprzeczył tym wyjaśnieniom). Wyjaśniła również, że z ww. powodów hasło było zapisane i dostępne innym pracownikom oddziału w ukrytym miejscu, gdyż zdarzało się, że było zapominane.

Pielęgniarka oddziałowa z innego oddziału, gdzie również stwierdzono fakt zanotowania hasła i przechowywania go w umówionym miejscu wyjaśniła, że nie udostępniała hasła innym pracownikom i to jedynie zbieg okoliczności sprawił, że odnaleziony w trakcie oględzin zapisany ciąg znaków był hasłem do jej konta użytkownika w systemie Windows. (akta kontroli str. 463-465, 468-479)

Należy mieć na uwadze, że przy przyjętych w Szpitalu parametrach dotyczących haseł, prawdopodobieństwo, że ciąg znaków jest hasłem logowania dla użytkownika systemu Windows wynosi jak 1:8.874.660.387.840[31]. Każda z osób, które proszono o złożenie wyjaśnień stwierdziła, że znane były jej postanowienia IZSI w zakresie użytkowania systemów informatycznych, sposobów i metod logowania użytkowników, co wskazywać może na potrzebę dodatkowych szkoleń z tego zakresu. (akta kontroli str. 468-479)

4. Dwie z 33 analizowanych osób personelu administracyjnego posiadało dostęp do systemu HIS, chociaż nie wykonywały one już obowiązków, podczas których taki dostęp był niezbędny. Wcześniej pełniły one bowiem obowiązki sekretarki medycznej oraz pracownika Sekcji Planowania, Monitorowania Świadczeń Zdrowotnych i Statystyki Medycznej, a dostęp do tego systemu był im przyznany w związku z wykonywanymi obowiązkami służbowymi. Po zmianie miejsca pracy, dostęp do systemu HIS nie został im odebrany. Art. 5 pkt 1 lit. c RODO wskazuje zasadę adekwatności i minimalizacji danych, tj. wymóg ustalenia kto i w jakim zakresie jest uprawniony do przetwarzania danych, a zgodnie z art. 24 ust. 2 pkt 2 ustawy o prawach pacjenta osoby te nie wykonywały już czynności pomocniczych podczas udzielania świadczeń opieki zdrowotnej. (akta kontroli str. 267-272)

IOD wyjaśnił, że: *„Sekcja Służb Pracowniczych i Płac nie przekazała Sekcji Informatyki informacji o zmianie miejsca pracy i potrzeby weryfikacji dostępu do posiadanego oprogramowania. Obecnie dane takie są już na bieżąco przekazywane Sekcji Informatyki"*. Kierownik Sekcji Służb Pracowniczych i Płac wyjaśnił zaś, że nie sądził, aby informacje o zmianie miejsca pracy mogłyby być istotne. Dodał, że: *„nie było jasnego przekazu, aby takie informacje podawać Sekcji Informatyki. Są to sytuacje incydentalne, nie została wypracowana praktyka podawania takich informacji"*.
(akta kontroli str. 463-465, 467)

[31] Dla porównania prawdopodobieństwo skreślenia zwycięskiego kuponu w grze Lotto wynosi 1:13.983.816, czyli jest 634.638 bardziej prawdopodobne.

5. Personelowi Szpitala umożliwiono dostęp do danych osobowych oraz możliwość ich przetwarzania bez upoważnienia Dyrektora ZOZ (administratora danych). Przed wejściem w życie RODO nie funkcjonowały upoważnienia wydane przez administratora danych, do dostępu do danych osobowych, danych medycznych. Stosownie do art. 37 ustawy o ochronie danych osobowych w stanie prawnym przed 25 maja 2018 r., do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych. IOD wyjaśnił, że stosowanym rozwiązaniem było odbieranie od pracowników *„Oświadczenia o zachowaniu w tajemnicy służbowej i zasadach przetwarzaniu danych osobowych"*. Wraz z wejściem w życie przepisów RODO, IOD rozpoczął proces udzielania upoważnień pracownikom i wydawał je sukcesywnie do zakończenia kontroli NIK[32]. IOD wyjaśnił: *„przyznaję, że proces ten trwa dość długo, ale miałem też inne zagadnienia do zrealizowania w związku z wejściem w życie RODO. Skupiłem się na sprawach organizacyjnych w pierwszej kolejności"*. Tymczasem, według art. 32 ust. 4 RODO, administrator oraz podmiot przetwarzający podejmują działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego. Jednocześnie art. 5 pkt 1 lit. c RODO wskazuje zasadę adekwatności i minimalizacji danych, tj. wymóg ustalenia kto i w jakim zakresie jest uprawniony do przetwarzania danych. (akta kontroli str. 273-286, 365-368, 463-465)

6. Dziewiętnastu z 30 (63,3%) poddanych badaniu pracownikom Działu Higieny Szpitalnej[33] nadano upoważnienia do *„podglądu danych"* osobowych, medycznych pacjentów, pracowników, finansowo płacowych, rozliczeniowo-statystycznych, księgowych. Zadaniem pracowników tego działu, według § 75 Regulaminu Organizacyjnego Szpitala, było zapewnienie prawidłowych warunków sanitarno-higienicznych w pomieszczeniach ZOZ, zabezpieczenia wykonywania czynności pomocniczych opiekuńczo-higienicznych przy pacjencie obłożnie i ciężko chorym, realizacja transportu wewnętrznego, obsługa stacji łóżek, obsługa depozytu ubrań chorych i punktu pralniczego. W indywidualnych zakresach obowiązków analizowanej grupy osób nie stwierdzono zapisów o dostępie przez nich do danych medycznych. IOD wyjaśnił, że: *„są to pracownicy, którzy mogą mieć kontakt z danymi osobowymi podczas wykonywania swoich obowiązków. Podczas sprzątania mogą spotkać się z dokumentacją medyczną i stąd chciałem zabezpieczyć się przed ujawnieniem przetwarzanych danych poza szpital. Personel tego działu spotyka się w swojej pracy z danymi medycznymi, czasami przewozi pacjentów na badania wraz ze skierowaniem, gdzie są te dane medyczne. Z tego powodu udzieliłem im upoważnień do podglądania takich danych, co w moim mniemaniu chroni szpital przed wyciekiem takich danych"*.
(akta kontroli str. 308-364, 463-465)

   Zdaniem NIK podgląd już utrwalonych danych stanowi ich przetwarzanie. Pracownicy Działu Higieny Szpitalnej nie powinni mieć wglądu do dokumentacji medycznej, ze względu na przepisy art. 9 ust. 1 i 2 RODO, uzależniające dostęp do tzw. szczególnych kategorii danych, w tym danych dotyczących zdrowia, od spełnienia określonych, szczególnych warunków (np. zapewnienia opieki zdrowotnej lub leczenia). Jednocześnie, zgodnie z art. 24 ust. 2 i art. 26 ust. 1 ustawy o prawach pacjenta, dokumentację medyczną można ujawnić tylko określonym podmiotom, w tym podmiotom leczniczym, osobom wykonującym zawód medyczny uczestniczącym w udzielaniu świadczeń medycznych lub właściwym organom. Podobne zasady określają art. 40 i art. 41 ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty[34]. Nie mają też zastosowania przepisy art. 24 ust. 2 pkt 2 ustawy o prawach pacjenta, dotyczące osób wykonujących czynności pomocnicze przy udzielaniu świadczeń zdrowotnych, które są uprawnione do dostępu do danych medycznych, na podstawie upoważnień administratora danych. Zadania związane z dostępem do danych medycznych nie wynikają z – określonych w § 75 regulaminu

[32] Poza upoważnieniami dla dwóch osób, które zostały wydane odpowiednio 1 i 21 maja 2018 r.
[33] Dział ten liczył 65 pracowników.
[34] Dz. U. z 2018 r. poz. 617, ze zm.

organizacyjnego – obowiązków Działu Higieny Szpitalnej oraz zakresów obowiązków analizowanych osób.

Zgodnie z art. 5 ust. 1 i art. 6 ust. 1 RODO przetwarzanie danych powinno być ograniczone do tego co jest niezbędne do celów przetwarzania. Sprzątanie pomieszczeń nie stanowi celu przetwarzania, uzasadniającego dostęp do danych. Podobnie przewóz pacjentów powinien być zorganizowany w sposób uniemożliwiający personelowi Działu Higieny Szpitalnej dostęp do danych medycznych transportowanych wraz z pacjentem.

W zakresie pozostałych danych, nie będących danymi medycznymi, nie ma zakazu udostępniania innym osobom takich danych i udzielenia im upoważnień, ale musi wynikać to z wykonywania obowiązków związanych z dostępem do takich danych.

7. Ośmiu osobom (z 30), które po 1 stycznia 2018 r. zakończyły pracę w Szpitalu, nie odebrano dostępu do systemów informatycznych, do których dostęp posiadali podczas zatrudnienia. Działanie to było niezgodne z § 20 ust. 2 pkt 5 rozporządzenia KRI, wedle którego zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez bezzwłoczną zmianę uprawnień, w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji. Jednocześnie art. 5 pkt 1 lit. c RODO wskazuje zasadę adekwatności i minimalizacji danych, tj. wymóg ustalenia kto i w jakim zakresie jest uprawniony do przetwarzania danych. IOD wyjaśnił, że nie odebrał dostępu, ponieważ służby kadrowe nie poinformowały go o zakończeniu pracy przez te osoby. Kierownik Sekcji Służb Pracowniczych i Kadr wyjaśnił zaś, że: *„nie było jasnego przekazu, aby takie informacje Sekcji Informatyki podawać".*
(akta kontroli str. 369-373, 463-465, 467)

8. W 22 (ze 117) zgłoszeniach usterek oprogramowania przekazanych dostawcy oprogramowania między 1 stycznia a 19 października 2018 r., za pośrednictwem platformy NCR, zamieszczono dane personalne pacjentów: imię, nazwisko, PESEL, dane medyczne. Spośród nich 20 zgłoszeń dokonano przed wejściem w życie RODO, dwa zaś po 25 maja 2018 r. Działanie to było niezgodne z art. 24 ust 2 ustawy o prawach pacjenta. IOD wyjaśnił, że: *„większość tych zgłoszeń była przed wejściem w życie RODO, po 25 maja 2018 r. Comarch, z którym posiadamy umowę powierzenia przetwarzania danych osobowych, zwrócił nam uwagę na podawanie tylko numerów ID pacjenta i stosujemy się do tego, wcześniej nie było wyraźnego komunikatu ze strony odbiorcy danych, że robimy coś niewłaściwie. Uważaliśmy, że mając podpisaną umowę o powierzeniu przetwarzania danych, sytuacja nie jest niewłaściwa".*
(akta kontroli str. 386-451, 463-465)

W podobnych sytuacjach dochodziło do wycieku takich danych, o czym informowały branżowe portale internetowe[35].

OCENA CZĄSTKOWA

ZOZ wprowadził rozwiązania organizacyjne zmierzające do zapewnienia ochrony danych osobowych pacjentów oraz poszanowania ich prywatności. Personelowi szpitala zapewniono odpowiedni dostęp do danych medycznych, jednak wystąpiły przypadki posiadania przez pracowników administracyjnych zbyt dużych uprawnień w wykorzystywanych systemach informatycznych, a części byłych pracowników nie odbierano dostępu do tych systemów. Było to niezgodne z zasadami określonymi przepisami art. 5 pkt 1 lit. c RODO oraz § 20 ust. 2 pkt 5 rozporządzenia KRI. Negatywnie należy ocenić też praktyki personelu medycznego związane z nieblokowaniem komputerowych stacji roboczych podczas nieobecności w miejscu pracy, korzystaniem przez kilka osób z jednego konta użytkownika oraz przekazywaniem pomiędzy pracownikami danych (haseł) do autoryzacji w systemach informatycznych. Takie działanie stanowi bowiem naruszenie przyjętych regulacji wewnętrznych, określonych w rozdziale 5 pkt 5 oraz pkt 6.2 ppkt. 1 obowiązującej w Szpitalu IZSI. Wystąpiły także przypadki przekazania dostawcy oprogramowania danych osobowych i medycznych pacjentów, czym naruszono przepisy art. 24 ust 2 ustawy o prawach pacjenta.

[35] https://niebezpiecznik.pl/post/dane-pacjentow-i-szpitali-wyciekly-z-helpdesku-eskulapa-szpitale-powinny-zmienic-hasla/ – dostęp 12 października 2018 r.

Wnioski

IV. Wnioski

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

1. Opracowanie Polityki Bezpieczeństwa Informacji, o której mowa w § 2 pkt 15 rozporządzenia KRI, spełniającej wymogi § 20 ust. 1 tego rozporządzenia.
2. Zwrócenie uwagi personelowi medycznemu na konieczność właściwej organizacji pracy w zakresie przechowywania dokumentacji medycznej, rozpoczynania i zawieszania pracy z systemami informatycznymi oraz właściwego postępowania z hasłami do tych systemów.
3. Rozważenie sformalizowania sposobu zmiany i odbierania uprawnień pracownikom w przypadku zmiany miejsca pracy lub zakończenia zatrudnienia.
4. Bieżące wydawanie upoważnień osobom przetwarzającym dane osobowe oraz zapewnienie szkoleń, o których mowa w § 20 ust. 2 pkt 6 rozporządzenia KRI, wszystkim pracownikom zaangażowanym w proces przetwarzania informacji.
5. Odebranie upoważnień do podglądu danych pracownikom Działu Higieny Szpitalnej.
6. Niepodawanie w zgłoszeniach serwisowych danych osobowych i medycznych pacjentów.

V. Pozostałe informacje i pouczenia

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

Prawo zgłoszenia zastrzeżeń

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

Białystok, 17 grudnia 2018 r.

Kontroler:
Wojciech Zambrzycki
starszy inspektor k. p.

podpis

DYREKTOR DELEGATURY
Najwyższej Izby Kontroli w Białymstoku
z up. WICEDYREKTOR
Robert Skwarko

podpis