NAJWYŻSZA IZBA KONTROLI
Delegatura w Lublinie

LLU.410.003.01.2019

Pan Gabriel Maj
Dyrektor
Wojewódzkiego Szpitala Specjalistycznego
im. Stefana Kardynała Wyszyńskiego
Samodzielnego Publicznego Zakładu Opieki
Zdrowotnej w Lublinie
al. Kraśnicka 100, 20-718 Lublin

WYSTĄPIENIE POKONTROLNE

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

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

I. Dane identyfikacyjne

Jednostka kontrolowana	Wojewódzki Szpital Specjalistyczny im. Stefana Kardynała Wyszyńskiego Samodzielny Publiczny Zakład Opieki Zdrowotnej w Lublinie (dalej: „Szpital" lub „ZOZ") al. Kraśnicka 100, 20-718 Lublin
Kierownik jednostki kontrolowanej	Gabriel Maj, dyrektor od 1 listopada 2014 r.
Zakres przedmiotowy kontroli	1. Opracowanie wymaganej dokumentacji oraz procedur związanych z ochroną przetwarzania danych osobowych. 2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych.
Okres objęty kontrolą	Kontrola objęła okres od 25 maja 2018 r. (data 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[1]) do dnia zakończenia czynności kontrolnych. Badania kontrolne mogły dotyczyć działań sprzed tego okresu, jeśli miały związek z zagadnieniami będącymi przedmiotem kontroli.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[2]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Lublinie
Kontroler	Sławomir Dąbrowski, doradca prawny, upoważnienie do kontroli nr LLU/30/2019 z 29 stycznia 2019 r.

(akta kontroli str. 1-2)

[1] Dz. Urz. UE L 119 z 2016 r., str. 1, ze zm. Rozporządzenie zwane dalej: RODO.
[2] Dz. U. z 2019 r. poz. 489, dalej: „ustawa o NIK".

II. Ocena ogólna[3] kontrolowanej działalności

OCENA OGÓLNA

Najwyższa Izba Kontroli[4] pozytywnie ocenia podjęte przez Szpital działania w celu zapewnienia prawidłowej ochrony i przetwarzania danych osobowych.

Uzasadnienie oceny ogólnej

ZOZ wywiązał się z obowiązku opracowania, zatwierdzenia i wdrożenia wymaganej dokumentacji oraz procedur dotyczących ochrony danych osobowych. Personel ZOZ został właściwie poinformowany o przepisach RODO oraz regulacjach wewnętrznych Szpitala. Rzetelnie przeprowadzono analizę procesów przetwarzania danych oraz ocenę skutków dla ochrony danych osobowych. Prowadzony rejestr czynności przetwarzania zawierał wszystkie wymagane elementy. Personelowi Szpitala zapewniono szkolenia związane z wejściem w życie przepisów RODO oraz zagadnieniami dotyczącymi bezpieczeństwa danych, a także zapewniono dostęp do danych medycznych oraz nadano uprawnienia w systemach informatycznych adekwatne do miejsca pracy i wykonywanych zadań. Poprawnie wykorzystywano mechanizmy zdalnego zgłaszania usterek dostawcom oprogramowania. Rzetelnie wywiązano się z obowiązku zawarcia umów powierzenia przetwarzania danych. Udostępnianie dokumentacji medycznej pacjentów odbywało się zgodnie z obowiązującymi przepisami prawa oraz regulacjami wewnętrznymi ZOZ. Podejmowano właściwe działania w celu minimalizacji ryzyka utraty danych osobowych w wyniku awarii, błędów lub nieuprawnionej modyfikacji. Stwierdzono jednak, że przyjęty w Szpitalu sposób oznaczania opasek identyfikacyjnych pacjentów oraz stosowania ramek na karty przyłóżkowe był niezgodny z obowiązującymi w tym zakresie przepisami, a w jednym z gabinetów w poradni specjalistycznej nie zastosowano odpowiednich środków ochrony podczas nieobecności lekarza, co stwarzało niebezpieczeństwo dostępu do danych osobowych i medycznych pacjentów przez osoby nieuprawnione. Nieterminowo poinformowano również Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu IOD.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[5] kontrolowanej działalności

OBSZAR

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

Opis stanu faktycznego

1.1 Zarządzeniem Dyrektora Szpitala Nr 88/2018 z dnia 11 maja 2018 r., z mocą obowiązującą od dnia 25 maja 2018 r., w ZOZ powołano Inspektora Ochrony Danych (dalej: IOD). Zgodnie z wymogami art. 37 ust. 5 RODO, IOD miał należyte przygotowanie i kwalifikacje zawodowe do pełnienia swojej funkcji. Osoba ta do 24 maja 2018 r. pełniła obowiązki Administratora Bezpieczeństwa Informacji (dalej: ABI), a także ukończyła szkolenia z zakresu bezpieczeństwa informacji i ochrony danych osobowych.

Szpital zawiadomił w dniu 14 września 2018 r. Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu IOD tj. 14 dni po terminie określonym art. 158 ust. 2 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[6]. Przekazane

[3] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.
[4] Zwana dalej: „NIK".
[5] 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.
[6] Dz. U. poz. 1000, ze zm. Dalej: u.o.d.o.

zawiadomienie zawierało wszystkie elementy określone w art. 10 ust. 3 ustawy o ochronie danych osobowych.

Dane kontaktowe IOD oraz sposób i formę kontaktu udostępniono na stronie internetowej Szpitala, co było zgodne z art. 37 ust. 7 RODO oraz art. 11 u.o.d.o.

IOD umożliwiono pełnienie obowiązków w sposób niezależny, stosownie do art. 38 ust. 3 i ust. 4 RODO. W § 135 regulaminu organizacyjnego Szpitala z 16 lipca 2018 r. wskazano stanowisko Inspektora Ochrony Danych, jako samodzielne stanowisko pracy, podległe bezpośrednio Dyrektorowi Szpitala, a w Polityce Bezpieczeństwa Informacji[7] określono, że przy realizacji powierzonych zadań IOD m.in. ma prawo kontrolować komórki organizacyjne Szpitala oraz wydawać polecenia kierownikom tych komórek w zakresie bezpieczeństwa danych osobowych, a także żądać od wszystkich pracowników wyjaśnień w sytuacji naruszenia bezpieczeństwa danych osobowych. IOD nie zajmował w Szpitalu innego stanowiska ani nie pełnił innych funkcji.

(akta kontroli str. 5-18, 30-33, 438-440)

Szpital 4 grudnia 2018 r. otrzymał zawiadomienie o zakończeniu postępowania administracyjnego w sprawie uznania go za operatora usługi kluczowej, o którym mowa w art. 5 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[8] w zakresie udzielania świadczeń opieki zdrowotnej przez podmiot leczniczy oraz obrotu i dystrybucji produktów leczniczych. Do zakończenia kontroli nie otrzymał jednak od Ministra Zdrowia, będącego organem właściwym ds. cyberbezpieczeństwa, decyzji administracyjnej w tej sprawie. W myśl art. 5 ust. 1 ustawy, operatorem usługi kluczowej jest podmiot, wobec którego organ właściwy ds. cyberbezpieczeństwa[9] wydał decyzję o uznaniu za operatora usługi kluczowej.

(akta kontroli str. 434-437)

1.2 Zarządzeniem Dyrektora nr 100/2018 z dnia 23 maja 2018 r. wprowadzono w Szpitalu nową Politykę Bezpieczeństwa Informacji[10]. Określono w niej zasady i procedury obowiązujące przy przetwarzaniu danych osobowych pracowników ZOZ i pacjentów, zadania i uprawnienia IOD oraz Administratora Systemu Informatycznego[11]. PBI regulowała m.in. organizację bezpieczeństwa przetwarzania danych osobowych, zasady udostępniania danych osobowych, powierzanie przetwarzania danych, procedury postępowania w sytuacji naruszenia ochrony danych osobowych, zasady przetwarzania, udostępniania i przechowywania danych w formie nieelektronicznej, działania mające na celu zapewnienie integralności i poufności danych osobowych, zasady postępowania dla zachowania ochrony danych osobowych przy realizacji usług medycznych świadczonych w Szpitalu. Częścią Polityki Bezpieczeństwa Informacji była Instrukcja Zarządzania Systemem Informatycznym[12], w której uregulowano m.in. zasady eksploatacji systemów informatycznych, zasady dostępu do systemu informatycznego, procedury rozpoczęcia i zakończenia pracy w systemie informatycznym, a także zasady dotyczące tworzenia i przechowywania kopii awaryjnych, zabezpieczenie antywirusowe systemu informatycznego, zasady postępowania z nośnikami informacji, zasady komunikacji w sieciach komputerowych, zasady monitorowania, przeglądu i konserwacji systemów informatycznych, zasady dokonywania zmian

[7] Wprowadzonej zarządzeniem Dyrektora Szpitala Nr 100/2018 z dnia 23 maja 2018 r.
[8] Dz. U. poz. 1560.
[9] Wymieniony w art. 41 powołanej ustawy.
[10] Obowiązującą od 25 maja 2018 r., zwaną dalej: „PBI".
[11] Zwanego dalej: „ASI".
[12] Dalej: „IZSI".

w systemach informatycznych, odpowiedzialność i obowiązki użytkowników systemu informatycznego.

Integralną część PBI stanowiły załączniki: [1] tabela form naruszeń danych osobowych, [2] wzór wykazu osób upoważnionych do przetwarzania danych, [3] wzór rejestru naruszeń ochrony danych, [4] regulamin monitoringu wizyjnego, [5] klauzula informacyjna w przypadku zbierania danych od osoby, której dane dotyczą, [6] wzór rejestru udostępnianej dokumentacji medycznej, [7] wzór rejestru zbiorów danych osobowych, czynności przetwarzania i oceny skutków dla ochrony danych, [8] opis sposobu przepływu danych pomiędzy poszczególnymi systemami informatycznymi, w których przetwarzane są dane osobowe, [9] wzór karty szkolenia wstępnego z zakresu ochrony danych osobowych, [10] wzór oświadczenia zgody na przetwarzania danych osobowych, [11] wzór informacji Szpitala o zawartości zbioru danych osobowych, [12] wzór wniosku informacji szpitala o przetwarzanych danych, [13] wzór upoważnienia do przetwarzania danych osobowych, [14] wzory oświadczeń i zobowiązań o zachowaniu w tajemnicy danych osobowych oraz wniosek o udostępnienie dokumentacji medycznej.

Polityka Bezpieczeństwa Informacji została przedstawiona do zapoznania się i stosowania pracownikom Szpitala na spotkaniach wewnętrznych w dniach 5-6 czerwca 2018 r. oraz zamieszczona na stronie intranetowej Szpitala. Nowo zatrudnieni pracownicy Szpitala przy nawiązaniu stosunku pracy odbywali szkolenie wstępne z zakresu ochrony danych osobowych i podpisywali oświadczenie o zapoznaniu się z treścią PBI, a także zobowiązywali się do zachowania w tajemnicy danych osobowych, do których będą mieli dostęp w związku z wykonywanymi zadaniami służbowymi. Analiza dokumentacji 10 losowo wybranych osób wykonujących pracę w Szpitalu wykazała, że złożyli oni oświadczenia o zapoznaniu się z treścią PBI. Dla pracowników, których zadania związane były z przetwarzaniem danych osobowych i/lub medycznych, Dyrektor Szpitala wydawał upoważnienia do przetwarzania danych osobowych. W Szpitalu prowadzony jest rejestr osób upoważnionych do przetwarzania danych osobowych w wersji papierowej i elektronicznej.

(akta kontroli str. 19-104, 158-191, 218-239, 442-443, 445-448)

1.3. W ZOZ, od 25 maja 2018 r. prowadzony jest *rejestr zbiorów danych osobowych, czynności przetwarzania i oceny skutków dla ochrony danych* w formie papierowej oraz elektronicznej. Rejestr czynności przetwarzania danych osobowych sporządzony został oddzielnie dla 30 funkcjonujących w Szpitalu zbiorów danych osobowych i zawierał wszystkie elementy, o których mowa w art. 30 ust. 1 RODO: [1] nazwę zbioru danych, [2] nazwę i dane kontaktowe ADO [3] imię i nazwisko i dane kontaktowe IOD, [4] podstawy prawne upoważniające do przetwarzania danych, [5] cel przetwarzania danych, [6] opis kategorii osób, których dane są przetwarzane oraz kategorii przetwarzanych danych, [7] zakres przetwarzanych danych, [8] kategorie odbiorców, którym dane mogą być przekazywane, w tym odbiorców w państwach trzecich i organizacjach międzynarodowych, [9] źródło posiadanych danych, [10] informację o przekazaniu danych do państwa trzeciego lub organizacji międzynarodowej, [11] planowany termin usunięcia poszczególnych kategorii danych, [12] ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

(akta kontroli str. 105-157)

1.4. W okresie od lutego do kwietnia 2018 r. w Szpitalu przeprowadzony został audyt wewnętrzny w zakresie dostosowania ZOZ do uregulowań prawnych w obszarze ochrony danych osobowych w związku z wejściem w życie przepisów

RODO. W ramach audytu, zgodnie z art. 32 RODO, przeprowadzona została analiza obowiązującej dokumentacji i określone ryzyka w zakresie ochrony danych osobowych przetwarzanych przez Szpital. Na spotkaniu, które odbyło się 19 marca 2018 r. wyznaczono osoby, odpowiedzialne za przeprowadzenie analizy mającej na celu stworzenie ostatecznych dokumentów wymaganych na mocy RODO. Analiza prowadzona była w formie roboczej dokumentacji, która stanowiła podstawę do opracowania rejestru czynności przetwarzania oraz oceny skutków dla ochrony danych. W wyniku audytu, Szpital wdrożył środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający stwierdzonemu ryzyku. Dla każdej kategorii czynności przetwarzania danych osobowych ryzyko naruszenia praw lub wolności osób fizycznych określono na poziomie niskim. Opracowana została nowa Polityka Bezpieczeństwa Informacji wraz z: [1] wykazem zbioru danych osobowych i wskazaniem programów zastosowanych do ich przetwarzania, [2] wykazem osób odpowiedzialnych za poszczególne zbiory danych, [3] wykazem urządzeń medycznych, w których występuje możliwość przetwarzania danych osobowych pacjentów, [4] wykazem form naruszeń danych osobowych oraz sposobów postepowania w przypadku ich wystąpienia, [5] wykazem osób upoważnionych do przetwarzania danych osobowych, [6] rejestrem udostępnionej dokumentacji medycznej, [7] rejestrem zbiorów danych osobowych, czynności przewarzania i oceny skutków ochrony danych osobowych, [8] opisem sposobu przepływu danych pomiędzy poszczególnymi systemami informatycznymi, w których przetwarzane są dane osobowe. Działania mające na celu minimalizację ryzyka określono w ocenie skutków dla ochrony danych.

(akta kontroli str. 105-170)

1.5. W Szpitalu, jeszcze przed wejściem w życie RODO[13], została wykonana ocena skutków dla ochrony danych (dalej: DPIA[14]), o której mowa w art. 35 RODO, pomimo, że jej przeprowadzenie nie było obligatoryjne. Procesy związane z przetwarzaniem danych osobowych, dla których należy dokonać oceny skutków dla ochrony danych, zostały określone na spotkaniach wewnętrznych, w których udział brało m.in. kierownictwo ZOZ, ABI (obecny IOD), Administrator Systemu Informatycznego (dalej: ASI), audytor wewnętrzny oraz kierownicy komórek organizacyjnych odpowiedzialnych za przetwarzanie szczególnych kategorii danych osobowych. W ich wyniku opracowano kryteria analizy ryzyka oraz planowania środków mających na celu minimalizację ryzyka. Dokonanie DPIA dla operacji przetwarzania już trwających przed 25 maja 2018 r.[15] oraz w przypadkach, gdy nie jest jasne, czy taka ocena jest wymagana, zalecane było natomiast przez Grupę Roboczą ds. Ochrony Danych[16], według której jest ona *przydatnym narzędziem, które może pomóc administratorom danych w zapewnieniu zgodności z prawem ochrony danych*, chociaż Prezes UODO w komunikacie[17] wydanym na podstawie art. 35 ust. 4 RODO wśród rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony, nie zawarł danych medycznych przetwarzanych w szpitalach, jako wymagających oceny skutków przetwarzania. DPIA dokonana przez Szpital zawierała elementy wymagane art. 35

[13] Tj. w dniach 09.-16.04.2018 r.

[14] Ang.: *Data Protection Impact Assessment*.

[15] Dokument pt.: Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679 https://www.giodo.gov.pl/1520281/id_art/9957/j/pl dostęp z dnia 11 lutego 2019 r.

[16] Grupa Robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym organem doradczym w zakresie ochrony danych i prywatności. Zadania grupy określone są w art. 30 dyrektywy 95/46/WE oraz art. 15 dyrektywy 2002/58/WE.

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

ust. 7 RODO. Dyrektor Szpitala wyjaśnił, że *wykonał ocenę skutków dla ochrony danych, ponieważ dokonanie takiej oceny zawarte zostało w opartym na metodologicznej analizie ryzyka planie audytu wewnętrznego. Obszar analizy ryzyka jest corocznie objęty audytem zapewniającym. W ZOZ podjęto decyzję o dokonaniu oceny skutków dla ochrony danych celem zwiększenia bezpieczeństwa danych osobowych.*

(akta kontroli str. 105-170, 430)

1.6. Jednym z zadań IOD, w myśl art. 39 ust. 1 lit. b RODO, jest prowadzenie szkoleń personelu uczestniczącego w operacjach przetwarzania danych. Przed wejściem w życie przepisów RODO, pomiędzy 12 lutego a 20 kwietnia 2018 r., IOD przeprowadził dla pracowników Szpitala 10 szkoleń wewnętrznymi oraz zorganizował jedno szkolenie zewnętrzne[18]. Szkoleniami wewnętrznym w formie warsztatów przeprowadzanych przez IOD oraz szkoleniem zewnętrznym objęto 1541 z 1595 (96,6%) pracowników Szpitala. Szkoleniami objęto niemal cały personel, za wyjątkiem osób przebywających na urlopach bezpłatnych, zasiłkach rehabilitacyjnych, urlopach macierzyńskich i wychowawczych[19].. Szkolenia te obejmowały m.in. ogólną charakterystykę zagadnień z zakresu ochrony danych osobowych, spełnienie obowiązku informacyjnego, prawa osób, których dane dotyczą, zasady postępowania i zgłaszania naruszeń ochrony danych, 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, zabezpieczanie danych osobowych w komunikacji wewnętrznej). Szkoleniami objęto zarówno kierownictwo ZOZ, jak i kierowników komórek organizacyjnych, personel medyczny oraz pracowników administracji ZOZ.

Inspektor Ochrony Danych wyjaśnił, że po wejściu w życie RODO wszystkie osoby przyjmowane do pracy w ZOZ odbywają przeszkolenia na bazie karty szkolenia wstępnego, które poprzedza podpisanie przez pracownika oświadczenia o zachowaniu w tajemnicy danych osobowych i sposobów ich zabezpieczania oraz upoważnienia do przetwarzania danych osobowych. Taka forma szkolenia wstępnego dotyczy również m.in. lekarzy delegowanych na staże specjalizacyjne, lekarzy stażystów z innych Szpitali i studentów odbywających praktyki. W dniu 1 października 2018 r. przeprowadzono szkolenie lekarzy odbywających roczny staż podyplomowy (44 osoby) oraz nowo przyjętych pracowników w tematyce dotyczącej bezpieczeństwa danych osobowych.

(akta kontroli str. 171-191)

1.7. Dyrektor Szpitala wyjaśnił, że pomimo niezatwierdzenia *Kodeksu postępowania dla sektora ochrony zdrowia* przez Prezesa Urzędu Ochrony Danych Osobowych, wybrane zapisy Kodeksu i przewodnika po RODO są uwzględniane przy realizacji zadań związanych z ochroną danych osobowych. Dodatkowo IOD poinformował, że w ramach dobrej praktyki, szkolenia wstępne pracowników poruszają zagadnienia przedstawione w projekcie *Kodeksu postępowania dla sektora ochrony zdrowia.*

(akta kontroli str. 172, 430)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następującą nieprawidłowość:

[18] Wykład miał miejsce w budynku Szpitala.
[19] Statystycznie 4%-5% personelu Szpitala była w ciągu roku była nieobecna.

1. Zawiadomienie Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu IOD nastąpiło w dniu 14 września 2018 r., tj. 14 dni po terminie określonym w art. 158 ust. 2 ustawy o ochronie danych osobowych.

   W wyjaśnieniu Dyrektor Szpitala podał, że opóźnienie wynikało z przeoczenia terminu określonego w art. 158 ust. 2.

(akta kontroli str. 449)

OCENA CZĄSTKOWA

NIK pozytywnie ocenia opracowanie przez Szpital wymaganej dokumentacji oraz procedur związanych z ochroną przetwarzanych danych osobowych. ZOZ wywiązał się z obowiązku opracowania, zatwierdzenia i wdrożenia dokumentacji oraz procedur dotyczących ochrony danych osobowych. Pracownicy ZOZ zostali właściwie poinformowani o przepisach RODO oraz regulacjach wewnętrznych w tym zakresie. Rzetelnie przeprowadzono analizę procesów przetwarzania danych, ocenę skutków dla ochrony danych osobowych. Prowadzony rejestr czynności przetwarzania zawierał wszystkie wymagane elementy. Personelowi Szpitala zapewniono szkolenia związane z wejściem w życie przepisów RODO oraz zagadnieniami dotyczącymi bezpieczeństwa danych.

OBSZAR

2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych

Opis stanu faktycznego

2.1. Oględziny trzech oddziałów szpitalnych, tj. Oddziału Gastroenterologii, Oddziału Alergologii i Chorób Płuc oraz Oddziału Chorób Wewnętrznych, Endokrynologii i Diabetologii wykazały, że w celu ochrony danych osobowych pacjentów funkcjonowały niżej wymienione rozwiązania.

- Na wszystkich łóżkach szpitalnych zajmowanych przez pacjentów, znajdowały się karty przyłóżkowe. Wprowadzono rozwiązanie polegające na zastosowaniu ramek na karty przyłóżkowe, zasłaniających dane medyczne zawarte w kartach. Celem odczytania danych medycznych pacjenta, niezbędne jest wyciągnięcie karty z ramki. Natomiast ramki nie zasłaniały imienia i nazwiska pacjenta.
- Pacjenci znajdujący się na oddziałach Szpitala zaopatrywani byli w opaski identyfikacyjne, na których znajdowały się ręcznie wypisane dane: imię i nazwisko, data urodzenia, numer księgi głównej. Opaski zakładane były wszystkim pacjentom w sposób, aby dane znajdowały się od wewnętrznej strony nadgarstka (dane te były jednak widoczne bez odchylania opaski).
- Dokumentacja medyczna przechowywana w dyżurkach pielęgniarskich i gabinetach lekarskich znajdowała się w zamykanych na klucz szafkach. Osoby postronne nie miały dostępu do danych osobowych i medycznych pacjentów. „Ruch chorych" prowadzony był w miejscu niewidocznym dla pacjentów oraz osób postronnych, w zamkniętym na klucz pomieszczeniu (w dwóch przypadkach zastosowano szyfrowany zamek), do którego dostęp miał wyłącznie personel oddziału.
- Nie stwierdzono sytuacji opuszczania dyżurki pielęgniarskiej lub gabinetu lekarskiego przez personel oddziału i pozostawienia tych pomieszczeń bez nadzoru. W dyżurkach pielęgniarskich znajdowały się cztery komputery, wszystkie były uruchomione i w trakcie oględzin były użytkowane przez pielęgniarki.

(akta kontroli str. 192-198)

W wyniku oględzin sposobu rejestrowania pacjentów w trzech rejestracjach (rejestracji ogólnej, rejestracji RTG, USG, tomografii komputerowej i rejestracji Zakładu Diagnostyki Laboratoryjnej, Koagulologii i Mikrobiologii) oraz procesu wywoływania i przyjmowania pacjentów przez lekarzy w trzech gabinetach poradni

specjalistycznych (gabinet Poradni Dermatologicznej, gabinet Poradni Chirurgii Naczyń oraz gabinet Poradni Otolaryngologicznej), stwierdzono, co następuje.

- Proces rejestracji pacjentów odbywał się w więcej niż jednej rejestracji. Przy każdym z okienek widniała informacja, że przy okienku może znajdować się tylko jedna osoba (ewentualnie z opiekunem prawnym). Odległość między sąsiadującymi okienkami rejestracji wynosiła około 3 metry, co zapewniało, że osoby znajdujące się przy sąsiednim okienku nie słyszały ani nie miały wglądu w dokumenty osoby znajdującej się obok. Dla osób oczekujących na rejestrację usytuowano kilkadziesiąt krzesełek w odległości około 3-4 metrów od rejestracji.
- W Szpitalu funkcjonuje system numerkowy rejestracji pacjentów polegający na tym, że pacjenci pobierali wydruk z numeratora, na którym uwidocznione były: dane lekarza, numer gabinetu oraz data i godzina wizyty, a następnie oczekiwali na wyświetlenie swojego numeru na ekranie.
- Przy okienkach rejestracji znajdowała się informacja o konieczności okazania dokumentu tożsamości. Pracownicy rejestracji nie posługiwali się nazwiskami pacjentów, tylko identyfikowali ich na podstawie okazanego dokumentu. Kolejność wizyt wynikała z otrzymanego przez pacjenta wydruku rejestracyjnego. Pacjenta wzywano na podstawie numeru widniejącego na wydruku rejestracyjnym. Obok okienek rejestracji znajdowała się klauzula informacyjna o przetwarzaniu danych osobowych, na której wskazano m.in. nazwę i dane kontaktowe ADO, imię i nazwisko oraz dane kontaktowe IOD, cele i podstawy przetwarzania danych, obowiązek podania danych osobowych, zakres przetwarzanych danych, odbiorców, okres przechowywania danych, przysługujące pacjentom prawa na mocy RODO oraz informacja o zautomatyzowanym przetwarzaniu, w tym profilowaniu.
- Ustawienie monitorów w rejestracji uniemożliwiało wgląd do danych w nich zawartych osobom postronnym. W obrębie wzroku pacjentów rejestrujących się nie znajdowały się dane osobowe innych pacjentów.
- W dwóch objętych oględzinami gabinetach poradni specjalistycznych (tj. w Poradni Dermatologicznej i Poradni Chirurgii Naczyń) dokumentację pacjentów przechowywano w sposób uniemożliwiający wgląd do niej przez osoby postronne. Na widoku znajdowała się jedynie dokumentacja pacjenta aktualnie przyjmowanego przez lekarza. Karty pozostałych pacjentów znajdowały się w oddzielnych szafkach zamykanych na klucz.
- W przypadku dwóch gabinetów w trakcie dokonywania oględzin nie zaobserwowano, aby lekarz opuszczał gabinet pozostawiając go bez nadzoru. Natomiast w przypadku gabinetu lekarskiego w Poradni Otolaryngologicznej, gabinet pozostawiono otwarty bez nadzoru. Szerzej opisano to w dalszej części wystąpienia, w sekcji „*Stwierdzone nieprawidłowości”*.

(akta kontroli str. 199-205, 206-209)

W ramach oględzin stwierdzono, że na żadnym z trzech oddziałów nie było zainstalowanych kamer monitoringu wizyjnego. W ZOZ funkcjonuje monitoring wizyjny, który obejmuje wejścia do budynków, ciągi komunikacyjne, częściowo parkingi oraz Szpitalny Oddział Ratunkowy. Monitoring wizyjny rejestruje obraz bez rejestracji dźwięku. Zapisy z kamer przechowywane są maksymalnie do 30 dni. Po tym okresie są kasowane poprzez nadpisanie kolejnych nagrań. Do zapisów monitoringu wizyjnego dostęp mają: dyrektor Szpitala, zastępcy dyrektora, policja, prokuratura i inne służby w sytuacjach nadzwyczajnych, oraz inne osoby po uzyskaniu zgody dyrektora Szpitala. Szpital spełnił obowiązek informacyjny – zgodnie z wskazówkami Urzędu Ochrony Danych Osobowych zastosowano warstwowe noty informacyjne, tj. skrócone klauzule informacyjne przy piktogramach o monitoringu wizyjnym oraz rozszerzoną klauzulę informacyjną dostępną w Służbie

Ochrony Szpitala i IOD. Sporządzono również regulamin monitoringu[20], który stanowił załącznik do PBI. Pracownicy składali pisemne oświadczenia o zapoznaniu się z obowiązującymi w Szpitalu przepisami oraz zasadami przetwarzania i ochrony danych osobowych, w tym z regulaminem monitoringu wizyjnego.

(akta kontroli str. 92-93, 192-210)

2.2. Personel działów administracyjnych[21] Szpitala liczył 73 osoby. Analiza uprawnień dostępu do systemu HIS[22] 30 spośród tych pracowników wykazała, że 29 osób nie posiadało dostępu do tego systemu. Dostęp do HIS miała jedna osoba - kierownik Działu Planowania i Analiz, na podstawie upoważnienia Dyrektora Szpitala[23]. Osoby zatrudnione w Dziale Informatyki, Dziale Dokumentacji i Statystyki Medycznej oraz Dziale Organizacji Świadczeń Medycznych i Dokumentacji Medycznej posiadały dostęp do systemu HIS, w myśl art. 24 ust. 2 pkt 2 ustawy o prawach pacjenta[24], 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.

(akta kontroli str. 211-239, 441)

2.3. Analiza przeprowadzona na próbie 30 (z 660) pielęgniarek i położnych zatrudnionych w Szpitalu wykazała, że 28 z nich posiadało dostęp w systemie HIS do danych medycznych pacjentów tylko na oddziałach szpitalnych, na których świadczyły pracę. W przypadku dwóch pielęgniarek (zatrudnionych w Oddziale Intensywnej Terapii i Anestezjologii) posiadały one dostęp w systemie HIS do pacjentów z innych oddziałów szpitalnych, a nie tylko z oddziału, na którym świadczyły pracę, co było uzasadnione charakterem działalności oddziału. Pielęgniarkom i położnym z wybranej próby ADO wydał upoważnienia do przetwarzania danych osobowych, a ich zakres odpowiadał wykonywanym przez nie obowiązkom służbowym.

Nie stwierdzono wydawania upoważnień do przetwarzania danych osobowych pracownikom, których obowiązki służbowe nie wiązały się z przetwarzaniem takich danych.

(akta kontroli str. 218-274, 442-443)

2.4. Po dniu 25 maja 2018 r. 109 osób zaprzestało świadczyć pracę w Szpitalu. Osoby te w okresie zatrudnienia miały przyznany dostęp do systemów informatycznych Szpitala, w tym do aplikacji HIS. Analiza uprawnień tych osób wykazała, że dostęp do systemów odbierano tym osobom następnego dnia po ustaniu zatrudnienia, przy czym ASI blokował konta użytkowników w systemie, ale ich trwale nie usuwał, w wyniku czego byli widoczni w panelu administratora. Stwierdzono, że wg stanu na dzień 7 marca 2019 r., 97 osób miało zablokowane konto, natomiast w przypadku 12 osób konta te zostały odblokowane z uwagi na ponowne podjęcie przez te osoby zatrudnienia na podstawie umów cywilnoprawnych lub odbywanie staży zawodowych.

(akta kontroli str. 275-289)

[20] Regulamin wykorzystania zapisów monitoringu wizyjnego zainstalowanego na terenie WSS im. Stefana Kardynała Wyszyńskiego SPZOZ w Lublinie z 10.03.2017 r., stanowiący załącznik do PBI z 2018 r.

[21] Z wyłączeniem Działu Informatyki, Działu Dokumentacji i Statystyki Medycznej oraz Działu Organizacji Świadczeń Medycznych i Dokumentacji Medycznej.

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

[23] Z dnia 25.05.2018 r.

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

2.5. Szpital zawarł umowę dotyczącą świadczenia usług serwisu oprogramowania oraz pomocy technicznej z firmą zewnętrzną. Błędy i usterki w działaniu systemu były zgłaszane online poprzez system zgłoszeń NCR. W okresie od 25 maja 2018 r. do 5 marca 2019 r. dokonano do dostawców oprogramowania 376 zgłoszeń. Szczegółowym badaniem objęto 50 z tych zgłoszeń, w wyniku którego nie stwierdzono ujawniania danych osobowych lub medycznych pacjentów. W przypadku zgłoszeń związanych z przetwarzaniem danych pacjentów zastosowano pseudonimizację (zamiast imienia i nazwiska pacjenta zamieszczano numer księgi głównej lub ID pacjenta) oraz anonimizację (rubryki zawierające dane pacjentów zostały przed wysłaniem zamazane w sposób uniemożliwiający odczytanie danych).

(akta kontroli str. 290-295, 432-433)

2.6. Szpital w okresie objętym kontrolę (do dnia 20 lutego 2019 r.) posiadał zawarte 404 umowy powierzenia przetwarzania danych osobowych. W 335 umowach Szpital wystąpił jako podmiot powierzający przetwarzanie danych, a w 69 jako podmiot przetwarzający.

Analiza pięciu umów, w których Szpital powierzył przetwarzanie danych osobowych (dwie umowy zawarte z lekarzami prowadzącymi indywidualne praktyki lekarskie, jedna z osobą prowadzącą usługi pielęgniarskie i rejestratorskie, jedna z Samodzielnym Publicznym Zakładem Opieki Zdrowotnej, jedna z osobą świadczącą usługi diagnostyczne) wykazała, że zawierały one wszystkie postanowienia wymagane art. 28 ust. 3 RODO. Dyrektor Szpitala poinformował NIK, że przesłanką, dla których ZOZ, jako ADO, zawarł umowy powierzenia przetwarzania, była realizacja obowiązków określonych w art. 28 ust. 3 RODO.

(akta kontroli str. 296-351, 429-430)

2.7 W Szpitalu funkcjonował rejestr naruszeń ochrony danych osobowych, którego wzór stanowi załącznik do PBI. Dodatkowo w Szpitalu prowadzono rejestr incydentów bezpieczeństwa oraz działań korygujących i zapobiegawczych. W rejestrze incydentów odnotowuje się zdarzenia niepożądane z zakresu ochrony danych osobowych, które nie skutkują naruszeniem praw i wolności osób, których dane dotyczą. Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych jest zawarta w rozdziale II Polityki Bezpieczeństwa Informacji. Załącznik do PBI stanowi również tabela form naruszeń danych osobowych, która zawiera przykładowe formy naruszeń oraz określa sposób postępowania. W okresie objętym kontrolą nie stwierdzono przypadków naruszenia praw i wolności osób, których dane dotyczą, skutkujące zgłoszeniem naruszenia do Prezesa Urzędu Ochrony Danych Osobowych. W rejestrze incydentów odnotowano cztery incydenty (dotyczące: znalezienia w windzie opaski identyfikacyjnej pacjenta, awarii przełącznika sieciowego w serwerowni, umiejscowienia klucza na zewnątrz w drzwiach gabinetu w trakcie przyjmowania pacjenta przez lekarza oraz pozostawienia niezamkniętych drzwi w gabinecie otolaryngologicznym podczas nieobecności lekarza). W okresie objętym kontrolą do ZOZ nie wpłynęły skargi związane z przypadkami ujawnienia danych osobowych. Analiza rejestru incydentów wskazuje, iż działania podjęte przez ZOZ były adekwatne do ryzyka naruszenia praw i wolności osób, których dane dotyczą. Incydent stwierdzony podczas oględzin kontrolera został odnotowany przez IOD w rejestrze incydentów.

(akta kontroli str. 19-104, 352)

2.8 W ZOZ zasady udostępniania dokumentacji medycznej określone zostały w PBI, a wzór wniosku o udostępnienie dokumentacji medycznej (stanowiący załącznik do tej polityki) zamieszczony został również na stronie internetowej Szpitala. W ZOZ

prowadzony jest rejestr dotyczący udostępniania dokumentacji medycznej. Na jego podstawie ustalono, że w okresie od 25 maja 2018 r. do 13 lutego 2019 r. wpłynęło 1378 wniosków o udostępnienie dokumentacji medycznej, w tym 56 od towarzystw ubezpieczeniowych, 327 od organów ścigania, 838 od pacjentów oraz 157 od innych podmiotów i osób innych, niż pacjent. Szczegółowym badaniem objęto 60 przypadków udostępnienia dokumentacji medycznej, w tym 30 spraw, w których dokumentacja medyczna została udostępniona firmom ubezpieczeniowym oraz 30 spraw, w których udostępniono dokumentację innej osobie, niż pacjent. Stwierdzono, że dokumentacja medyczna udostępniana była zgodnie z postanowieniami PBI oraz art. 26 ust. 1 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta[25]. W 59 przypadkach dokumentację medyczną wydano uprawnionym podmiotom lub osobom, zaś w jednym przypadku dokonano odmowy udostępnienia, z uwagi na brak wskazania wnioskodawcy jako osoby upoważnionej do odbioru dokumentacji medycznej pacjenta. Nie stwierdzono przekazywania dokumentacji medycznej osobom lub podmiotom nieuprawnionym.

(akta kontroli str. 19-104, 353-364)

2.9 Zasady zabezpieczeń minimalizujących ryzyko utraty danych osobowych pacjentów w wyniku awarii, błędów lub nieuprawnionej modyfikacji określała Instrukcja Zarządzania Systemem Informatycznym (dalej: IZSI), w tym m.in. zasady bezpieczeństwa systemów informatycznych oraz zasady tworzenia i przechowywania kopii zapasowych. W ramach bezpieczeństwa informacji i systemów informatycznych, w ZOZ dokonywano corocznie audyt teleinformatyczny, który polegał na sprawdzeniu spełnienia wymagań zawartych w § 20 ust. 2 i § 21 ust. 1 i 2 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[26]. Zgodnie z protokołami z przeprowadzonych audytów, systemy teleinformatyczne Szpitala spełniały wymogi w tym zakresie.

(akta kontroli str. 19-104, 365-375)

W okresie objętym kontrolą w ZOZ funkcjonowała jedna serwerownia. Przeprowadzone oględziny wykazały, że Serwerownia posiadała zabezpieczenia przed nieuprawnionym dostępem, tj. drzwi antywłamaniowe zabezpieczone podwójnym zamkiem, sygnalizację systemu alarmowego i przeciwpożarowego. Serwerownię wyposażono w układ podtrzymywania napięcia UPS. Rejestr wejść do serwerowni prowadzony był przez ASI.

(akta kontroli str. 422-426)

IZSI określał również zasady dostępu do systemu informatycznego, procedury rozpoczęcia i zakończenia pracy w systemie informatycznym oraz zasady zabezpieczenia antywirusowego. Oględziny 30 komputerów, na których przetwarzane były dane osobowe (tj. po 10 użytkowanych przez lekarzy, pielęgniarki i położne oraz przez pracowników administracji ZOZ) wykazały, że pracownicy korzystający z komputerów byli uwierzytelniani za pomocą loginu i hasła. Liczba znaków w hasłach użytkowników była nie mniejsza niż wymagana w IZSI. Użytkownicy komputerów nie mieli uprawnień administratora, a komputery zabezpieczone były programem antywirusowym, który posiadał aktualną bazę sygnatur wirusów. W toku oględzin, stwierdzono, że spośród 30 komputerów objętych oględzinami, 20 komputerów działało na systemie operacyjnym Windows 7,

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

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

zaś 10 na systemie Windows XP. Uwzględniając, iż producent zakończył 8 kwietnia 2014 r. wsparcie techniczne systemu Windows XP, taki stan może w przyszłości stwarzać ryzyko dla bezpieczeństwa infrastruktury informatycznej. Każdy z komputerów objętych oględzinami posiadał aktywny port USB. W Szpitalu korzystano z odpowiednika dla Active Directory, tj. usługi domenowe oparte na serwerze Samba (Linux).

(akta kontroli str. 19-104, 376-421, 444)

Administrator Systemu Informatycznego Szpitala wyjaśnił, że *Kopie bezpieczeństwa baz danych tworzone są i weryfikowane poprzez dedykowane zautomatyzowane narzędzia. Poszczególne kopie tworzone są jako dzienne przyrostowe, tygodniowe przyrostowe oraz jako miesięczne pełne. Kopie wykonywane są dla baz danych wchodzących w skład systemów: HIS (medycznego), ERP (księgowość, kadry, magazyn, Płatnik ZUS), poczty email, serwera www, serwera intranetowego, serwera domenowego (oraz usług z nim związanych). Kopie przechowywane są na serwerze sieciowej przestrzeni dyskowej zlokalizowanym w oddzielnej lokalizacji niż sama serwerownia.*
W Szpitalu wykorzystywanych było 21 komputerów przenośnych. Nie stosowano na nich ochrony kryptograficznej. Zgodnie z PBI, dane osobowe w komputerach przenośnych mogły być przetwarzane tylko za pisemną zgodą ADO i było dopuszczalne wyłącznie wtedy, gdy dostęp do systemu operacyjnego był zabezpieczony hasłem.

(akta kontroli str. 52-53, 432-433)

Stwierdzone nieprawidłowości

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

1. W jednym z trzech gabinetów lekarskich, w których przeprowadzano oględziny, stwierdzono pozostawienie gabinetu bez nadzoru personelu medycznego (lekarza i pielęgniarki). Gabinet posiadał uchylone drzwi, zaś klucz znajdował się w drzwiach od wewnątrz. Karty pacjentów znajdowały się na biurku lekarza. W gabinecie pozostawał niezabezpieczony komputer, a na ekranie widoczne były informacje o przyjętych pacjentach (bez danych medycznych, jedynie dane osobowe).

   Powyższe zdarzenie stwarzało niebezpieczeństwo ujawnienia danych osobowych i/lub medycznych pacjentów osobom postronnym. Zgodnie z art. 24 ust. 1 RODO, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z tym rozporządzeniem. Jednocześnie, w myśl motywu 39 preambuły oraz art. 5 ust. 1 lit. f. RODO, dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich, niedozwolonym lub niezgodnym z prawem przetwarzaniem. W myśl art. 13 ustawy o prawach pacjenta, pacjent ma prawo do zachowania w tajemnicy przez osoby wykonujące zawód medyczny informacji z nim związanych, uzyskanych w związku wykonywaniem tego zawodu. Zdarzenie to naruszało również regulacje wewnętrzne ZOZ (w szczególności PBI i IZSI).

   Dyrektor Szpitala wyjaśnił, że upomniał pielęgniarkę i przeprowadził rozmowę z kierownikiem Wojewódzkiej Przychodni Specjalistycznej wskazując na konieczność objęcia szczególnym nadzorem zasad bezpieczeństwa danych osobowych. Powyższe zdarzenie zostało odnotowane w rejestrze incydentów.

   (akta kontroli str. 206-209, 427-428)

2. Opaski na nadgarstkach pacjentów trzech oddziałów[27] poddanych oględzinom zawierały, poza numerem księgi głównej, imię i nazwisko pacjenta oraz datę urodzenia. Było to niezgodne z art. 36 ust. 5 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej[28] oraz § 1 ust. 1, § 3 pkt 1) rozporządzenia Ministra Zdrowia z 20 września 2012 r. *w sprawie warunków, sposobu i trybu zaopatrywania pacjentów szpitala w znaki identyfikacyjne oraz sposobu postępowania w razie stwierdzenia ich braku*[29], które stanowią, że opaska zawierać powinna informacje zapisane w sposób uniemożliwiający identyfikację pacjenta przez osoby nieuprawnione.

   Dyrektor Szpitala wyjaśnił, że Szpital nie został wyposażony w specjalistyczne drukarki i skanery służące do tworzenia i odczytu danych na opaskach identyfikacyjnych pacjentów. Poinformował ponadto, że *Istotą wszystkich działań Wojewódzkiego Szpitala Specjalistycznego im. Stefana Kardynała Wyszyńskiego SP ZOZ w Lublinie jest ochrona zdrowia i życia pacjentów. Dla pełni bezpieczeństwa pacjentów nieodzowna jest ich właściwa identyfikacja. W Szpitalu podjęto świadomą decyzję o zaopatrywaniu pacjenta w opaskę zawierającą imię i nazwisko, datę urodzenia oraz numer księgi głównej. Uwarunkowane to jest koniecznością niezwłocznej i jednoznacznej identyfikacji pacjenta przez personel Szpitala w celu udzielenia pomocy w przypadku nagłego pogorszenia się stanu zdrowia pacjenta. Nieoznaczenie opaski w powyższy sposób mogłoby skutkować zwiększeniem ryzyka pomyłki lub błędu medycznego i spowodować uszczerbek na zdrowiu. W Szpitalu dokonano oceny ryzyka naruszenia praw i wolności pacjentów pod kątem ochrony danych osobowych, w kontekście zakresu danych na opasce identyfikacyjnej stwierdzono niski poziom ryzyka, w wyniku czego podjęto decyzję o jego akceptacji. Sytuacja finansowa Szpitala powoduje, że nie wprowadzono systemu informatycznego do tworzenia opasek identyfikacyjnych i Szpital nie został wyposażony w specjalistyczne drukarki i skanery do tworzenia i odczytu danych na opaskach identyfikacyjnych. Mając na uwadze zasadę minimalizacji danych, wprowadzenie rozwiązania polegającego na wdrożeniu takiego systemu oraz wyposażenie w drukarki i przenośne skanery do odczytu danych, wiązałoby się z bardzo dużymi kosztami finansowymi, na których poniesienie Szpital nie posiada środków.*

   (akta kontroli str. 429-431)

3. Na trzech objętych oględzinami oddziałach szpitalnych karty przyłóżkowe zawierały niezasłonięte dane osobowe pacjentów. W Szpitalu funkcjonowało rozwiązanie, polegające na zastosowaniu ramek na karty przyłóżkowe, zasłaniających dane medyczne pacjentów, jednakże dane osobowe nie były zasłonięte. Dane te były widoczne dla wszystkich przebywających w sali, co było niezgodne z art. 24 ust. 1 RODO, w którym jako jeden z obowiązków ADO wskazano wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających ochronę danych osobowych.
   Dyrektor Szpitala wyjaśnił, że *wpisywanie nazwiska i imienia pacjenta wynika z potrzeby właściwego zabezpieczenia usług medycznych i bezpieczeństwa osobowego przy udzielaniu tych świadczeń, a w konsekwencji niezwłocznej identyfikacji pacjenta.*

   (akta kontroli str. 450)

[27] Tj. Oddziału Gastroenterologii, Oddziału Alergologii i Chorób Płuc oraz Oddziału Chorób Wewnętrznych, Endokrynologii i Diabetologii.
[28] Dz. U. z 2018 r. poz. 2190, ze zm.
[29] Dz. U. poz. 1098.

OCENA CZĄSTKOWA

NIK pozytywnie ocenia kontrolowany obszar. Wprowadzone rozwiązania techniczne i organizacyjne zapewniały na ogół ochronę danych osobowych pacjentów oraz poszanowanie ich prywatności. Jednak stwierdzone przypadki oznaczenia kart przyłóżkowych oraz opasek identyfikacyjnych pacjentów na oddziałach, które nie spełniały wymogów obowiązujących przepisów prawa oraz braku odpowiedniego zabezpieczenia jednego z gabinetów lekarskich podczas nieobecności lekarza, stwarzały ryzyko ujawnienia danych osobowych i medycznych pacjentów osobom nieuprawnionym.

IV. Wnioski/Uwagi i wnioski

Wnioski

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

1. Zapewnienie właściwego zabezpieczenia pomieszczeń gabinetów lekarskich podczas nieobecności osób uprawnionych pod kątem ochrony danych osobowych i medycznych.
2. Wprowadzenie rozwiązań w zakresie opasek identyfikacyjnych pacjentów i kart przyłóżkowych gwarantujących ochronę danych osobowych 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 Lublinie. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

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

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

Lublin, 19 kwietnia 2019 r.

Kontroler	Dyrektor
Sławomir Dąbrowski Doradca prawny	Delegatury Najwyższej Izby Kontroli w Lublinie Edward Lis
.....	.....
podpis	*podpis*