NAJWYŻSZA IZBA KONTROLI

Delegatura w Poznaniu

LPO.410.002.01.2019

Pan
Rafał Szuca
Dyrektor Szpitala Specjalistycznego
im. Stanisława Staszica w Pile
ul. Rydygiera 15, 64-920 Piła

WYSTĄPIENIE POKONTROLNE

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

NAJWYŻSZA IZBA KONTROLI
Delegatura w Poznaniu
ul. Dożynkowa 9H, 61-662 Poznań
T +48 61 655 62 00, F +48 61 655 62 01
lpo@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Szpital Specjalistyczny im. Stanisława Staszica w Pile, ul. Rydygiera 1, 64-920 Piła, (dalej: Szpital albo ZOZ)
Kierownik jednostki kontrolowanej	Rafał Szuca, Dyrektor Szpitala, od 26 czerwca 2014 r.
Zakres przedmiotowy kontroli	1. Opracowanie wymaganej dokumentacji oraz procedur związanych z ochroną przetwarzanych danych osobowych. 2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych.
Okres objęty kontrolą	Od 25 maja 2018 r. do 1 marca 2019 r.[1]
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 Poznaniu
Kontrolerzy	1. Ryszard Kokociński, Główny specjalista kontroli państwowej, upoważnienie do kontroli nr LPO/4/2019 z 9 stycznia 2019 r. 2. Artur Pigłas, doradca ekonomiczny, upoważnienie do kontroli nr LPO/50/2019 z 4 kwietnia 2019 r. (akta kontroli str. 1-5, 636)

[1] Badania kontrolne objęły także działania sprzed tego okresu, które miały związek z zagadnieniami będącymi przedmiotem kontroli.
[2] Dz. U. z 2019 r. poz. 489, dalej: ustawa o NIK.

II. Ocena ogólna[3] kontrolowanej działalności

OCENA OGÓLNA

Dane osobowe przetwarzane przez Szpital w okresie od 25 maja 2018 r. do 1 marca 2019 r. były prawidłowo chronione, jednakże niektóre obowiązki wynikające z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.[4] (dalej: RODO) zostały zrealizowane z opóźnieniem.

Wprowadzone rozwiązania organizacyjne, zmierzające do zapewnienia ochrony danych osobowych pacjentów, gwarantowały poszanowanie ich prywatności. Przyjęty w ZOZ system zarządzania bezpieczeństwem informacji odpowiadał wymogom § 20 ust. 1 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r.[5]. Rzetelnie przeprowadzono analizę procesów przetwarzania danych osobowych i oceniono ich skutki oraz właściwie prowadzono związane z tym rejestry. Szkoleniami z zakresu znajomości przepisów RODO oraz zagadnień bezpieczeństwa danych objęto 98% personelu Szpitala. Na rok 2019 opracowano plan szkoleń pozostałej części personelu oraz działań audytowych z zakresu ochrony danych osobowych. Personel ZOZ posiadał dostęp do danych medycznych, adekwatny do zakresu wykonywanych przez poszczególne osoby czynności, a byłym pracownikom niezwłocznie odbierano uprawnienia do systemów informatycznych, w których przetwarzano dane osobowe. Prawidłowo zabezpieczano stacje robocze i stanowiska pracy podczas nieobecności pracowników oraz zgodnie z regulacjami wewnętrznymi uwierzytelniano poszczególnych użytkowników systemów informatycznych. Usługa opieki serwisowej nad tymi systemami była zlecona umową, w której zawarto odpowiednie postanowienia zabezpieczające przetwarzanie danych osobowych, a stosowane przy takim przetwarzaniu środki techniczne i organizacyjne zapewniały stopień bezpieczeństwa adekwatny do ryzyk związanych m.in. ze skalą i rodzajem takiego przetwarzania.

W skontrolowanym zakresie stwierdzono następujące nieprawidłowości:

1) przez kilkanaście miesięcy w Szpitalu nie wykorzystywano sprzętu służącego do drukowania znaków identyfikacyjnych, zakupionego za 23,3 tys. zł, co nie sprzyjało efektywnemu wykorzystaniu tych środków publicznych,
2) z 25 dniowym opóźnieniem zawiadomiono Prezesa Urzędu Ochrony Danych Osobowych (dalej: Prezes UODO) o powołaniu na stanowisko inspektora ochrony danych (dalej: IOD) dotychczasowego administratora bezpieczeństwa informacji (dalej: ABI),
3) z opóźnieniem w stosunku do obowiązujących od 25 maja 2018 r. przepisów RODO wynoszącym:
   - prawie pięć miesięcy - dostosowano do tych przepisów[6] politykę bezpieczeństwa informatycznego ZOZ,
   - od 14 dni do 2 miesięcy - zawarto 20 umów dotyczących powierzenia podmiotom zewnętrznym przetwarzania danych.

Nie stwierdzono jednak, aby nieprawidłowości te miały negatywny wpływ na bezpieczeństwo przetwarzania i ochronę danych osobowych w Szpitalu.

---

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

[4] W sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) - Dz. Urz. UE L 119 z 4 maja 2016 r., str. 1 ze zm., weszło w życie 24 maja 2016 r., znajduje zastosowanie od 25 maja 2018 r.

[5] W sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247, dalej: rozporządzenie KRI).

[6] A także przepisów ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000).

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

OBSZAR

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

Opis stanu faktycznego

1. Według stanu na dzień ogłoszenia ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[8], tj. 24 maja 2018 r., w Szpitalu pełnił funkcję administrator bezpieczeństwa informacji (dalej: ABI). Dyrektor Szpitala zarządzeniem z dnia 24 lipca 2018 r.[9] powołał dotychczasowego ABI, na stanowisko Inspektora Ochrony Danych (dalej: IOD) oraz określił regulamin jego pracy. Stosownie do wymogów art. 38 ust. 3 RODO, IOD umożliwiono wykonywanie obowiązków w sposób niezależny[10]. Informację o powołaniu IOD przekazano Prezesowi UODO 25 września 2018 r., tj. z 25 dniowym opóźnieniem[11]. Zgłoszenie to zawierało wszystkie elementy określone w art. 10 ust. 1 i 3 u.o.d.o.

(akta kontroli str. 6-16, 31-34)

Zgodnie z wymogami wskazanymi w art. 37 ust. 5 RODO, IOD posiadał właściwe przygotowanie, doświadczenie i kwalifikacje zawodowe do pełnienia swojej funkcji. Od 2017 r. zajmował on stanowisko ABI w Szpitalu, pełniąc uprzednio funkcje jego zastępcy. IOD odbył szkolenia i kursy z zakresu ochrony danych. Był zatrudniony na tym stanowisku w wymiarze ½ etatu oraz dodatkowo w takim samym wymiarze jako specjalista ds. obronności i archiwizacji. Ta forma zatrudnienia nie pociągała za sobą określania sposobów i celów przetwarzania danych osobowych, a w konsekwencji nie stwierdzono występowania konfliktu interesów, o którym mowa w art. 38 ust. 6 RODO.

Dane kontaktowe IOD opublikowane zostały na stronach internetowych Szpitala, zgodnie z art. 37 ust. 7 RODO i art. 11 u.o.d.o.

(akta kontroli str. 17-29, 35-36)

Ministerstwo Zdrowia powiadomiło Szpital o wszczęciu z urzędu postępowania administracyjnego w sprawie uznania tej placówki za operatora usługi kluczowej w zakresie udzielania świadczeń opieki zdrowotnej przez podmiot leczniczy oraz obrotu i dystrybucji produktów leczniczych. Minister Zdrowia pismem z dnia 20 listopada 2018 r. powiadomił Szpital o zakończeniu postępowania administracyjnego w ww. zakresie, jednak do zakończenia czynności kontrolnych w jednostce[12] nie wydał decyzji o uznaniu Szpitala za operatora usługi kluczowej, o którym mowa w art. 5 ust. 1 w zw. z art. 2 pkt 16 ustawy z dnia 5 lipca 2018 r. o krajowym rejestrze cyberbezpieczeństwa[13].

(akta kontroli str. 37-42)

2. W związku z rozpoczęciem stosowania RODO, po niespełna pięciu miesiącach[14], zarządzeniem z dnia 24 października 2018 r. w Szpitalu wprowadzono zaktualizowaną Politykę Bezpieczeństwa Przetwarzania Danych Osobowych (dalej:

[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, ze zm., dalej: u.o.d.o.
[9] Nr 80/2018.
[10] IOD podlegał bezpośrednio Dyrektorowi Szpitala.
[11] O czym szerzej w sekcji „Stwierdzone nieprawidłowości".
[12] Tj. do dnia 1 marca 2019 r.
[13] Dz. U. poz. 1560.
[14] O czym szerzej w sekcji „Stwierdzone nieprawidłowości".

PBD) oraz Instrukcję Zarządzania Systemami Informatycznymi (dalej: IZSI). Uprzednio w Szpitalu obowiązywała Polityka Bezpieczeństwa Informacji (dalej: PBI) wprowadzona w styczniu 2014 r., określająca min. cele polityki bezpieczeństwa danych, zasady polityki bezpieczeństwa oraz obowiązki w odniesieniu do zarządzania bezpieczeństwem informacji. Ponadto, zdefiniowano w niej wykazy zbiorów, opis ich struktury, sposób przepływu danych, a także środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych.
PBD uwzględniała podstawy prawne w postaci przepisów RODO oraz u.o.d.o i określała m.in: obszary przetwarzania danych osobowych, wykazy i strukturę zbiorów tych danych, środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych, ochronę danych osobowych pracowników i pacjentów, sposoby zapewnienia ich bezpieczeństwa podczas przetwarzania w formie papierowej oraz w systemach elektronicznych. Załącznikami do PBD były m.in.: wykazy zbiorów danych, w których przetwarza się te dane, opisy struktur ich zbiorów, ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych, instrukcja postępowania w przypadku naruszenia ich bezpieczeństwa oraz instrukcja w sprawie ich przetwarzania w celach innych niż świadczenie usług medycznych. Przywołane w PBD akty prawne były aktualne.
(akta kontroli str. 42-179)

IZSI[15] określała m.in.: zasady eksploatacji systemów teleinformatycznych, bezpieczeństwa sieci w tym sieci operacyjnych, procedury rozpoczęcia, przerwania i zakończenia pracy przy używaniu systemu, zarządzanie zmianami w systemie i wymiennymi nośnikami komputerowymi, reguły bezpieczeństwa wymiany danych, konserwacji i napraw oraz sposób zarządzania dostępem do systemów teleinformatycznych, ich monitorowanie i użycie oraz zabezpieczenie przed działalnością szkodliwego oprogramowania. Załącznikami do tej instrukcji były: rejestr kopii zapasowych, wniosek o wydanie służbowego wymiennego nośnika informacji (pendrive), wzór ewidencji bezpiecznych kopert, dziennik pracy systemu oraz procedura niszczenia nośników informacyjnych.

W rozdziale 5 IZSI dotyczącym bezpieczeństwa informatycznego określono m.in. procedury nadawania i odbierania upoważnień do przetwarzania danych lub uzyskania dostępu do systemów informatycznych. Nazwy użytkowników i hasła były nadawane przez Administratora Systemów Informatycznych[16] (dalej: ASI) na wniosek lokalnego administratora danych, złożony według wzoru stanowiącego załącznik do Instrukcji i zatwierdzony przez IOD. Rejestracji, wyrejestrowania lub zmiany uprawnień użytkownika w systemie informatycznym dokonywał ASI. Ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych prowadził IOD. Użytkownikom systemu HIS[17] nadawano jeden z możliwych zakresów dostępu: pełne prawa do zarządzania zbiorem danych, pełne prawa do ewidencji danych (wprowadzanie, zmienianie lub usuwanie), prawo do dodawania i modyfikacji danych lub prawo do przeglądania danych na ekranie. Wyrejestrowanie albo zmiana uprawnień użytkownika następowały na wniosek lokalnego administratora danych, za pośrednictwem IOD lub bezpośrednio na wniosek IOD. Wyrejestrowanie miało charakter stały albo czasowy i następowało poprzez zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (tzw. czasowe wyrejestrowanie użytkownika), albo poprzez usunięcie danych użytkownika z bazy użytkowników systemu informatycznego (wyrejestrowanie stałe). Czasowe

[15] Od 24 października 2018 r. na podstawie zarządzenia Dyrektora nr 109/2018.
[16] Kierownika Działu Informatyki.
[17] Hospital Information System – system informatyczny do obsługi Szpitala.

wyrejestrowanie użytkownika z systemu następowało w przypadku jego nieobecności w pracy przez okres dłuższy niż 35 dni, zawieszenia lub zwolnienia z pełnienia obowiązków służbowych. Stałe wyrejestrowanie użytkownika z systemu następowało w przypadku rozwiązania albo wygaśnięcia jego stosunku pracy, a także cofnięcia upoważnienia do przetwarzania danych osobowych. Hasła użytkowników posiadały odpowiednią złożoność i podlegały modyfikacji co 30 dni.

(akta kontroli str. 119-179)

Konserwacja i naprawa sprzętu informatycznego prowadzona była jedynie przez uprawnionych pracowników Szpitala lub podmiot zewnętrzny, świadczący usługi konserwacyjne na podstawie umowy lub w ramach gwarancji. W przypadku kiedy na nośnikach komputerowych, stanowiących integralną część sprzętu przekazanego do naprawy, znajdowały się informacje szczególnie chronione, sprzęt taki naprawiany był pod nadzorem ASI. W sytuacji gdy brak było możliwości sprawowania przez niego nadzoru, informacje takie - po zapewnieniu możliwości ich odtworzenia - były skutecznie usuwane z nośnika. Konserwacje i naprawy odnotowywano w dzienniku pracy danego sprzętu.

Gwarantowane zasilanie urządzeń informatycznych Szpitala uzyskiwano przez zastosowanie:
- dywersyfikacji zewnętrznych źródeł energii elektrycznej z samoczynnym załączaniem rezerwy,
- zasilaczy bezprzerwowych (UPS) oraz awaryjnych agregatów prądotwórczych.

Serwisowanie urządzeń zasilających prowadzone było wyłącznie przez autoryzowane podmioty zewnętrzne. Przeglądy, konserwacje i serwisowanie odnotowywano w dzienniku pracy systemu.

(akta kontroli str. 462-464, 466, 538,636)

Postanowienia obowiązujących PBD oraz IZSI nie wymagały aktualizacji. Pracowników zapoznano z tymi dokumentami podczas prowadzonych szkoleń oraz poprzez ich opublikowanie na stronach intranetowych Szpitala.

(akta kontroli str. 73-118, 146-179)

3. Zgodnie z art. 30 ust. 1 i 2 RODO, IOD od maja 2018 r. prowadził rejestr czynności przetwarzania danych osobowych oraz rejestr kategorii czynności przetwarzania dokonywanych w imieniu administratora. Rejestry te zawierały wszystkie wymagane informacje, o których mowa odpowiednio w art. 30 ust. 1 lit. a-g oraz ust. 2 lit. a-d RODO.

(akta kontroli str. 228-251)

4. W Szpitalu wyodrębniono siedem procesów przetwarzania danych osobowych[18]. Dla każdego z tych procesów dokonano identyfikacji zagrożeń na podstawie mapy ryzyka oraz tabeli akceptowalności. Poziom ryzyka dla danego procesu obliczono ustalając odsetek sumy obliczonych ocen zagrożeń względem sumy maksymalnych ryzyk zagrożenia dla całego poziomu. Przyjęto następujące poziomy ryzyk: niski do 33%, średni w przedziale 34-66% oraz wysoki: 67-100%. Wskazano cztery warianty postępowania z ryzykiem, tj. jego: redukcję, zatrzymanie, unikanie oraz przeniesienie. Do zagrożeń o najwyższym poziomie ryzyka zaliczono: awarię serwera, celowe niszczenie urządzeń, nieautoryzowane działania, podrabianie dokumentacji w wersji elektronicznej, awarię oprogramowania aplikacyjnego, przerwę w dostawie prądu.

(akta kontroli str. 180-201)

[18] Opieka szpitalna, rekrutacja i zatrudnienie, informatyka, zarzadzanie finansowe, zarządzanie i organizacja szpitala, monitoring oraz przechowywanie dokumentacji zawierającej dane osobowe.

Stosownie do wymogów określonych w art. 35 ust. 7 RODO, już w czerwcu 2018 r., dokonano oceny skutków naruszenia praw i wolności osób fizycznych. Określając poziom skutków, oceniono prawdopodobieństwa ich wystąpienia i urzeczywistnienia się, dokonano oceny powagi ryzyka oraz poziomu akceptacji. Oceniając skutki przetwarzania danych zidentyfikowano: zagrożenia, podatność, możliwe skutki, określono wagę, prawdopodobieństwo i ryzyko oraz wskazano rekomendacje.
Ustalono dwa poziomy ryzyka podczas przetwarzania danych. Średni: 40% - dla procesu przechowywania dokumentacji zawierającej dane osobowe oraz niski: 19,3% - dla zarządzania i organizacji szpitala, 17,5% - dla zarządzania finansowego, 20% - dla monitoringu, 26% - dla informatyki, 17,5% - dla rekrutacji i zatrudnienia, 25% - dla leczenia szpitalnego i ambulatoryjnego.

(akta kontroli str. 180-201)

Ocena skutków przetwarzania danych osobowych poprzedzona została analizą listy procesów dokonaną przez IOD i ASI. Przy opracowywaniu tej oceny wykorzystano m.in. ocenę ryzyka przyjętą według wymogów ISO z czerwca 2017 r. oraz ocenę weryfikującą ISO z listopada 2018 r. Na podstawie weryfikacji oceny ryzyka z 2018 r. ustalono, że nie wystąpiły nowe zagrożenia dla przetwarzania danych osobowych. Zidentyfikowano trzy grupy ryzyka: naturalne, przypadkowe, umyślne. Dla każdego z 42 zidentyfikowanych ryzyk określono poziom skutków oraz oceniono prawdopodobieństwo zagrożenia, powagę i poziom akceptacji z mapą ryzyka dla prywatności. Dla każdego procesu przetwarzania danych osobowych, w tym danych szczególnych, zidentyfikowano zagrożenia mogące wystąpić przy ich przetwarzaniu oraz określono poziom akceptowalności ryzyka. W zakresie przechowywania dokumentacji medycznej wskazano na możliwość naruszenia praw i wolności pacjentów na skutek zaginięcia, kradzieży lub zdekompletowania akt w komórce organizacyjnej albo składnicy akt. W odpowiedzi na to zagrożenie PBD wprowadzała instrukcję w sprawie organizacji i zakresu działania składnicy akt oraz instrukcję udostępniania dokumentacji medycznej. W przypadku ryzyka ujawnienia danych szczególnych osobom nieuprawnionym PBD rekomendowała stosowanie zasady czystego biurka, instrukcji udostępniania dokumentacji medycznej, a także sprawdzanie tożsamości osoby wnioskującej o wydanie dokumentacji i weryfikację jej uprawnień. Powyższe rekomendacje zostały przez Szpital zrealizowane.

(akta kontroli str. 180-209)

Lista procesów związanych z przetwarzaniem danych osobowych obejmowała całość procesów zachodzących w Szpitalu. Każdemu procesowi przypisano wywoływanie określonych skutków.

(akta kontroli str. 180-201)

5. Na dzień 1 stycznia 2019 r., Szpital zatrudniał 1.284 pracowników. W okresie od maja 2018 r. do marca 2019 r. w ramach planowych szkoleń dotyczących znajomości przepisów ochrony danych osobowych, przeszkolono 1.260 z nich, tj. 98% ogółu zatrudnionych. Ponadto, każdy nowo przyjmowany pracownik odbywał, prowadzone przez IOD, przeszkolenie wstępne z przepisów RODO i ochrony danych osobowych, co było potwierdzane podpisem pracownika na „Upoważnieniu do przetwarzania danych osobowych" oraz na „Zgodzie do przebywania w obszarach przetwarzania danych osobowych Szpitala". Przeprowadzone planowe szkolenia dotyczyły m.in.: zasad przetwarzania danych osobowych z uwzględnieniem przepisów RODO, ochrony danych osobowych w podmiotach leczniczych, zmiany w przepisach wewnętrznych Szpitala związanych z RODO, tj. polityki bezpieczeństwa przetwarzania danych osobowych oraz instrukcji sposobu zarzadzania systemami informatycznymi. Powyższymi szkoleniami objęto dyrekcję Szpitala, kierowników oddziałów, lekarzy, pielęgniarki i sekretarki medyczne, kierowników komórek organizacyjnych, asystentów,

rehabilitantów, oraz sanitariuszy i personel sprzątający. IOD opracował na 2019 r. program szkoleń w zakresie przestrzegania zasad przetwarzania danych osobowych z uwzględnieniem przepisów RODO, plan audytu w zakresie zabezpieczenia komputerów, terminali oraz pomieszczeń, w których przetwarzane są dane osobowe, zabezpieczenia dokumentacji papierowej i elektronicznej przed dostępem osób nieupoważnionych a także testy wśród pracowników audytowanych komórek organizacyjnych, ze znajomości przepisów dotyczących ochrony danych osobowych. Szkoleniami zaplanowano objąć pracowników pięciu oddziałów, dwóch zakładów, Szpitalnego Oddziału Ratunkowego, Sekcji Statystyki Medycznej i Rozliczeń oraz Działu Ekonomiczno-Finansowego Szpitala.

(akta kontroli str. 252-330, 642)

6. W Szpitalu wykorzystywano „Przewodnik po RODO w służbie zdrowia", z którego treścią m.in. zapoznano kierowniczą kadrę pielęgniarską z 27 komórek organizacyjnych. Przeszkolone osoby otrzymały kopię przewodnika, a jego treść udostępniona została w wewnątrzszpitalnej wersji elektronicznej. Do opracowania rejestrów i wdrożenia procedur dotyczących wykorzystania monitoringu wizyjnego wykorzystano publikacje zamieszczone na stronach internetowych Urzędu Ochrony Danych Osobowych[19]. Przy realizacji wytycznych RODO, wykorzystywano publikacje zamieszczone na portalu dot. ochrony danych osobowych[20]. We wrześniu 2018 r. IOD przeprowadził w Dziale Służb Pracowniczych audyt zgodności przetwarzanych danych osobowych z obowiązującymi przepisami i uregulowaniami wewnętrznymi.

IOD wyjaśnił, że po zatwierdzeniu przez Prezesa UODO ostatecznej wersji Kodeksu Postępowania dla sektora ochrony zdrowia, zostanie on w Szpitalu wdrożony.

(akta kontroli str. 331-341)

Stwierdzone nieprawidłowości

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

1. Szpital zawiadomił Prezesa UODO o powołaniu dotychczasowego ABI na stanowisko IOD w dniu 25 września 2018 r., tj. 25 dni po terminie zakreślonym w art. 158 ust. 2 u.o.d.o. Zgodnie z tym przepisem, osoba która stała się IOD na podstawie ust. 1 tego artykułu pełni swoją funkcję także po 1 września 2018 r., jeżeli do tego dnia administrator zawiadomi Prezesa UODO o jej wyznaczeniu w sposób określony w art. 10 ust. 1 u.o.d.o.

Dyrektor Szpitala wyjaśnił, że wysłanie z opóźnieniem do Prezesa UODO zawiadomienia o powołaniu IOD wynikało z błędnego założenia, że termin zgłoszenia ubiega 30. – a nie 1. – września 2018 r. Ponadto wskazał, że po powzięciu informacji o pomyłce bezzwłocznie zgłoszono powołanie IOD w sposób określony art. 10 ust. 1 u.o.d.o.

Prezes UODO nie zakwestionował prawidłowości dokonanego zawiadomienia i powołania IOD.

(akta kontroli str. 31-34, 633)

2. Pomimo rozpoczęcia stosowania RODO od 25 maja 2018 r. oraz wejścia w życie w tym samym dniu przepisów u.o.d.o., PBD i IZSI, uwzględniające rozwiązania przyjęte w tych aktach prawnych wprowadzono 24 października 2018 r., tj. po upływie niespełna pięciu miesięcy. W tym okresie w PBI nadal odnoszono się do nieobowiązującego stanu prawnego oraz ustanowionego ABI, pomimo że

[19] „Wskazówki i wyjaśnienia dotyczące obowiązku rejestracji czynności i kategorii czynności przetwarzania określone w art. 30 ust. 1 i 2 RODO", które stosuje się od października 2018 r. „Wskazówki Prezesa Urzędu Ochrony Danych Osobowych dotyczące wykorzystywania monitoringu wizyjnego".

[20] www.poradyodo.pl

podstawa prawna jego wyznaczenia, tj. art. 36a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[21] utraciła moc, a w miejsce ABI 24 lipca 2018 r. powołano IOD. Obowiązująca do 23 października 2018 r. PBI nie uwzględniała części wymogów przewidzianych w RODO oraz w przepisach krajowych obowiązujących po 25 maja 2018 r., w tym m.in. obowiązków: zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu (art. 33 RODO), powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania (art. 19 RODO), informowania pracowników o wprowadzeniu monitoringu terenu Szpitala oraz monitoringu poczty elektronicznej (art. 22^2 oraz art. 22^3 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy[22]) a także praw do sprostowania danych (art. 16 RODO), usunięcia danych (art. 17 RODO), ograniczenia przetwarzania (art. 18 RODO).

Dokonanie aktualizacji regulacji wewnętrznych Szpitala po blisko pięciu miesiącach nie spełniało wymogów z art. 24 ust. 1 i 2 RODO, w myśl których obowiązkiem ADO było m.in. wdrożenie odpowiednich środków organizacyjnych, w tym polityk ochrony danych, poddawanych w razie potrzeby przeglądom i uaktualnianiu, tak aby przetwarzanie odbywało się zgodnie z ww. rozporządzeniem i aby móc to wykazać. NIK podkreśla, że jakkolwiek RODO stosowane było od 25 maja 2018 r., to weszło w życie już 24 maja 2016 r. (art. 99 RODO), a co za tym idzie, czas na niezwłoczne dostosowanie regulacji wewnętrznych Szpitala do jego przepisów był wystarczający.

Dyrektor wyjaśnił, że opóźnienie wprowadzenia w Szpitalu zaktualizowanej PBD oraz IZSI wynikło z oczekiwania na dalsze wytyczne z Urzędu Ochrony Danych Osobowych, co do przetwarzania danych osobowych w jednostkach ochrony zdrowia, a zwłaszcza z oczekiwania na Kodeks Branżowy w Ochronie Zdrowia. Dyrektor podkreślił, że Szpital posiadał zaktualizowane teksty ww. dokumentów według stanu na dzień obowiązywania RODO. Po stwierdzeniu, że wspomniany Kodeks nie wejdzie w życie w najbliższym czasie, w październiku 2018 r. Szpital wprowadził zaktualizowane przepisy dotyczące przetwarzania danych osobowych. Dyrektor dodał, że w okresie do wprowadzenia zaktualizowanych dokumentów funkcję IOD pełnił dotychczasowy ABI.

(akta kontroli str. 42-179, 639-640)

OCENA CZĄSTKOWA

Szpital wywiązał się z obowiązku opracowania i wdrożenia dokumentacji oraz procedur dotyczących ochrony danych osobowych, chociaż miało to miejsce po upływie prawie pięciu miesiącyh od rozpoczęcia stosowania RODO. Przyjęty system zarządzania bezpieczeństwem informacji w pełni odpowiadał wymogom § 20 ust. 1 rozporządzenia KRI. Rzetelnie przeprowadzono analizę procesów przetwarzania danych osobowych oraz ocenę skutków ich przetwarzania, jak również prawidłowo prowadzono rejestr czynności i kategorii czynności przetwarzania tych danych. Z przepisami RODO oraz zagadnieniami dotyczącymi bezpieczeństwa danych zapoznano 98% personelu Szpitala, a IOD opracował na 2019 r. plan kolejnych szkoleń oraz plan działań audytowych w zakresie ochrony danych osobowych. Nie stwierdzono by - relatywnie niewielkie - opóźnienie w powiadomieniu Prezesa UODO o powołaniu dotychczasowego ADO na IOD oraz opóźniona aktualizacja PBI wpłynęły negatywnie na realizację zadań w badanym obszarze.

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

[22] Dz. U. z 2018 r. poz. 917, ze zm.

OBSZAR

2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych

Opis stanu faktycznego

1. W poddanych badaniom salach chorych oddziałów: Dziecięcego, Reumatologicznego oraz Nefrologii i Chorób Wewnętrznych nie stwierdzono na łóżkach szpitalnych obecności kart pacjentów zawierających informacje o ich stanie zdrowia. Pacjenci tych oddziałów zgodnie z wymogami art. 36 ust. 3 ustawy z 15 kwietnia 2011 r. o działalności leczniczej[23], zostali zaopatrzeni w opaski identyfikacyjne. Na oddziałach Reumatologii oraz Nefrologii i Chorób Wewnętrznych opaski posiadały wypisany ręcznie numer z księgi głównej przyjęć i wypisów, natomiast na Oddziale Dziecięcym opaski były zadrukowane numerem księgi głównej, imieniem i pierwszą literą nazwiska pacjenta oraz kodem identyfikacyjnym.

Dane osobowe i medyczne pacjentów z ww. oddziałów przechowywano w zamykanych szafach lub szufladach znajdujących się w dyżurkach pielęgniarskich oraz gabinetach lekarskich. Nie ujawniono przypadków pozostawienia dokumentacji bez nadzoru uprawnionego personelu. Tablice z ruchem chorych na tych oddziałach znajdowały się w miejscu do którego dostęp był ograniczony (w pomieszczeniu zamkniętym za dyżurką lub w niewidocznej wnęce), a dane na nich umieszczone zawierały imię i pierwszą literę nazwiska pacjenta.

Komputery w dyżurkach pielęgniarskich oraz w pokojach lekarzy pełniących dyżur na tych oddziałach były zabezpieczone przed nieuprawnionym dostępem. Ich uruchomienie wymagało podania indywidualnego loginu oraz hasła posiadającego odpowiednią złożoność.

(akta kontroli str. 342-347)

W grudniu 2017 r. Szpital zakupił dziesięć drukarek znaków identyfikacyjnych za kwotę 23 298,29 zł z przeznaczeniem na wyposażenie Szpitalnego Oddziału Ratunkowego. Do zakończenia czynności kontrolnych w jednostce drukarek tych nie uruchomiono[24].

(akta kontroli str. 348)

2. W Szpitalu wprowadzono nw. rozwiązania techniczne i organizacyjne mające na celu zapewnienie właściwej ochrony danych osobowych pacjentów.

(akta kontroli str. 342-347, 350-356)

Punkty rejestracji pacjentów[25], w odległości od 1,5 do 1,8 m przed okienkami, posiadały oznaczenie na posadzce strefy, w której mogli przebywać jedynie pacjenci obsługiwani przez personel szpitalny. Pojedyncze stanowiska w rejestracji ogólnej i rejestracji laboratorium oraz trzy stanowiska w rejestracji przyjęć planowych[26] znajdowały się w odległości uniemożliwiającej usłyszenie danych osobowych lub wgląd w dokumentację osoby obsługiwanej na sąsiednim stanowisku. Przy okienkach umieszczono informację o możliwości przebywania przed nimi podczas rejestracji wyłącznie jednej osoby oraz uwidoczniona była klauzula informacyjna o przetwarzaniu danych osobowych. Każde stanowisko rejestracji wyposażone było w terminal, którego monitor był niewidoczny dla pacjenta obsługiwanego przy sąsiednim stanowisku. Obsługiwany pacjent okazywał personelowi skierowanie oraz dowód osobisty.

Kolejność wizyty do poradni lub laboratorium ustalana była według wydanych numerów lub kolejności rejestracji. Pacjentów wywoływano bez podawania ich

[23] Dz. U. z 2018 r. poz. 2190.
[24] O czym szerzej w sekcji „Stwierdzone nieprawidłowości".
[25] Rejestracja ogólna, rejestracja do laboratorium oraz rejestracja przyjęć planowych.
[26] Objęte szczegółowymi oględzinami.

danych osobowych. Dokumentacja medyczna w tych punktach rejestracji pacjentów przechowywana była w regałach z zamykanymi na klucz szufladami. Nie ujawniono przypadków aby w obrębie wzroku osoby rejestrowanej znajdowały się dane osobowe lub dokumentacja medyczna innych pacjentów.

(akta kontroli str. 350-354)

Osoby oczekujące na przyjęcie do lekarza w poradni ginekologicznej, onkologicznej oraz okulistycznej wzywano do gabinetu lekarskiego bez użycia nazwisk. Pacjentów wzywano przy użyciu sformułowań grzecznościowych np. „proszę następny pacjent" lub po imieniu. Karty pacjentów w ww. poradniach przechowywano w szufladach szafek zamykanych na klucz. Na biurku lekarza znajdowała się wyłącznie dokumentacja pacjenta aktualnie wzywanego do gabinetu. Nie ujawniono pozostawienia gabinetu lekarskiego bez nadzoru. Opuszczająca poradnię onkologiczną pielęgniarka, pod nieobecność pacjentów i lekarza zamknęła na klucz pomieszczenie poradni. Komputer znajdujący się w tej poradni był zablokowany i po powrocie pielęgniarki wymagał ponownego podania danych umożliwiających zalogowanie komputera i systemu informatycznego. Na biurku nie stwierdzono pozostawienia dokumentacji medycznej.

(akta kontroli str. 355-356)

Funkcjonujący w Szpitalu system monitoringu wizyjnego obejmował monitoring zewnętrzny, tj. wjazd i wyjazd na SOR, wejście główne, bramę wjazdową znajdującą się z tyłu szpitala, a także parking pracowniczy i parking dla pacjentów wraz z wyjazdem z tego parkingu. Ponadto system ten tworzyła kamera obrotowa, która obejmowała budynki zaopatrzenia, patomorfologię, kuchnię oraz pralnię. Monitoring wewnętrzny obejmował: wejście główne, punkt przyjęć planowych, korytarz prowadzący do działu informatyki i sekcji statystyki medycznej, hol i korytarz budynku, aptekę szpitalną, rejestrację RTG. System ten obejmował również: kaplicę na drugim piętrze znajdującą się w budynku „E", korytarze budynku „A" wraz z windami na wysokim parterze i pierwszym piętrze oraz korytarz i rejestrację przy SOR znajdujące się w budynku „C". Dane z monitoringu przechowywano przez okres 14 dni, a po tym okresie były one samoistnie kasowane.

Informację o funkcjonującym monitoringu umieszczono przy wejściu głównym do Szpitala, a do wiadomości publicznej podano regulamin funkcjonowania monitoringu. Urządzenia służące do zapisu danych z monitoringu oraz monitory znajdowały się w pomieszczeniu pracowników ochrony, a nadzór nad nimi sprawowali upoważnieni pracownicy. Pracownicy Szpitala złożyli stosowne oświadczenia o udostępnieniu ich wizerunków do celów służbowych.

(akta kontroli str. 357-370)

Spośród 88 pracowników administracyjnych Szpitala[27], dostęp do systemu informatycznego klasy HIS posiadało 27 z nich, w tym pełen dostęp do systemu, pięciu pracowników Działu Informatyki oraz Dyrektor Szpitala i jego dwóch zastępców. Ograniczony dostęp do systemu HIS miało: dziesięciu pracowników Działu Organizacji w zakresie modułu „Statystyka i Rozliczenia", sześciu pracowników Działu Ekonomiczno – Finansowego, kierownik ww. działu oraz IOD w zakresie danych o ruchu chorych (informacje o zwrotach historii chorób i użytkownikach) a także Inspektor ds. transportu w zakresie danych dot. zespołów wyjazdowych. Osoby te posiadały upoważnienie ADO do przetwarzania danych osobowych, stosownie do zakresu zadań, obowiązków i kompetencji określonych dla zajmowanego stanowiska. Na podstawie udzielonego upoważnienia ASI

[27] Kontrolą objęto wszystkich takich pracowników.

przyznawał uprawnienia dostępu do systemu. Uprawnienia tych pracowników były adekwatne do zakresu obowiązków i udzielonego przez ADO upoważnienia.

(akta kontroli str. 371-381)

3. Zarzadzanie siecią informatyczną odbywało się centralnie przez administratora infrastruktury informatycznej Szpitala (tzw. usługa Active Directory). O zakresie dostępu do danych pacjentów w informatycznym systemie obsługi Szpitala decydowały tzw. schematy uprawnień, które określały moduły systemu i zakres jaki mógł uzyskać użytkownik. Schematy uprawnień tworzone były w miarę potrzeb przez ASI. Zdefiniowane schematy uprawnień były przypisywane do personelu medycznego szpitala. Poszczególnym pracownikom określano w pierwszej kolejności komórkę organizacyjną, do której mieli uzyskać dostęp, a następnie w ramach tej komórki określano schemat uprawnień. Spośród 518 pielęgniarek i położnych posiadających różny zakres uprawnień do przetwarzania danych osobowych pacjentów, analizie poddano 32 uprawnienia. W zbadanej grupie personelu medycznego ASI przydzielił uprawnienia zgodne z przyznanymi przez ADO.

Personel medyczny w sposób adekwatny do realizowanych zadań i obowiązków uczestniczył w procesie przetwarzania danych osobowych pacjentów, a przyznany dostęp do danych medycznych pacjentów był zgodny z miejscem pracy w oddziale lub przychodni. Pracownikom niewykonującym działalności medycznej, m.in. pracownikom sprzątającym, nie wydawano upoważnień do przetwarzania danych osobowych. Osobom takim wydano zgodę na przebywanie w obszarach przetwarzania danych osobowych bez prawa wglądu do danych osobowych pacjentów, w tym bez uprawnień wstępu do systemów informatycznych.

(akta kontroli str. 382-411)

4. W myśl § 20 ust. 2 pkt 4 rozporządzenia KRI, zarządzanie bezpieczeństwem informacji wymaga podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji. Obowiązująca w Szpitalu PBD nakładała na IOD oraz ASI obowiązek wyrejestrowania z systemu informatycznego wszystkich pracowników, którym kończyła się umowa o pracę (kontrakt, a także w zw. z przejściem na emeryturę) lub wystąpiła absencja pracownika w pracy trwająca powyżej 35 dni. Informację taką dział służb pracowniczych przekazywał IOD, który następnie sporządzał wniosek o wyrejestrowanie danego pracownika z systemu informatycznego oraz przekazywał ten wniosek ASI dzień po zakończeniu umowy o pracę. W dniu otrzymania tego wniosku ASI wyrejestrowywał użytkownika z systemu informatycznego.

W okresie od 25 maja 2018 r. do 31 stycznia 2019 r. 82 osoby zakończyły zatrudnienie w Szpitalu. W dniu następującym po dniu zakończenia świadczenia pracy, ASI odebrał każdej z tych osób uprawnienia dostępu do systemu informatycznego do obsługi Szpitala.

(akta kontroli str. 422-430)

5. W wyniku postępowania w trybie przetargu nieograniczonego, w okresie od 31 sierpnia 2015 r. do 8 listopada 2018 r. obowiązywała umowa[28] zawarta pomiędzy Szpitalem a podmiotem gospodarczym na dostawę m.in. dodatkowych bezterminowych licencji oprogramowania medycznego, licencji modułów medycznego oprogramowania aplikacyjnego, usług serwisowych i szkoleniowych oraz 300 terminali dla wszystkich modułów oprogramowania medycznego. Kolejna

[28] Nr 144/2015/ZP z 31 sierpnia 2015 r.

umowa z 9 listopada 2018 r.[29] dotyczyła świadczenia usług opieki serwisowej wraz z dostępem do nowych wersji i nadzorem autorskim nad systemem informatycznym do obsługi Szpitala. Usługi te świadczone były drogą elektroniczną z wykorzystaniem technologii SSL VPN[30]. Każdorazowe zestawienie połączeń Dział Informatyki Szpitala ujmował w ewidencji zdalnych połączeń.

Stosowane środki techniczne i organizacyjne zapewniały zabezpieczenie danych osobowych przed: udostępnieniem ich osobom nieupoważnionym, przetwarzaniem z naruszeniem RODO, zmianą, utratą, uszkodzeniem lub zniszczeniem. Serwisujący zobowiązany był do usunięcia wszelkich danych osobowych z nośników elektronicznych pozostających w jego dyspozycji po wykonaniu usługi.

(akta kontroli str. 431-461, 467-469, 644-649)

Kierownik Działu Informatyki Szpitala (ASI) wyjaśnił, że instalację nowych wersji oraz zmian w oprogramowaniu dokonywali pracownicy podmiotu gospodarczego poprzez udostępnienie im połączenia VPN SSL. ASI był w posiadaniu wykazu tego typu połączeń będących zbiorem protokołów służących implementacji bezpiecznych połączeń oraz wymiany kluczy szyfrowania pomiędzy komputerami. Składający wyjaśnienia dodał, że Szpital nie prowadził prac programistycznych, a instalowane systemy były wcześniej sprawdzone i przetestowane.

(akta kontroli str. 466)

Zgłoszenia dotyczące problemów z system informatycznym do obsługi ZOZ były umieszczane w systemie HELPDESK firmy świadczącej usługi serwisowe nad systemem HIS. Analiza 50 zgłoszeń problemów informatycznych w systemie HELPDESK wykazała, że Szpital nie przekazywał temu podmiotowi danych osobowych lub dokumentacji medycznej pacjentów.

(akta kontroli str. 461, 465, 470-515, 650-699)

6. Szpital zawarł 28 umów powierzenia przetwarzania danych osobowych z podmiotami świadczącymi na jego rzecz usługi m.in. medyczne i informatyczne. Umowy te zawarto w okresie od 19 lutego 2018 r. do 27 sierpnia 2018 r., z czego 20 z nich po 25 maja[31].

Pięć skontrolowanych umów zawierało wszystkie wymagane postanowienia, o których mowa w art. 28 ust. 3 RODO. Zgodnie z ich treścią, przetwarzanie danych osobowych przez zleceniobiorców prowadzone będzie wyłącznie w celu realizacji ich postanowień. Przetwarzający dane zobowiązali się m.in. do podjęcia środków zabezpieczających wymaganych art. 32 w zw. z art. 28 ust. 3 lit. c RODO oraz do realizacji obowiązku określonego art. 33 w zw. z art. 28 ust. 3 lit. f RODO, w szczególności do niezwłocznego (nie później niż w ciągu 24 godzin) poinformowania IOD zleceniodawcy o jakichkolwiek przypadkach naruszenia ochrony danych osobowych.

W celu zabezpieczenia przetwarzanych danych osobowych, przetwarzający zobowiązani byli do prowadzenia dokumentacji opisującej sposób przetwarzania tych danych, a posiadane przez nich urządzenia i systemy informatyczne służące do ich przetwarzania zabezpieczone były zgodnie z obowiązującymi dobrymi praktykami i przepisami prawa w zakresie ochrony infrastruktury i zasobów teleinformatycznych, m.in. poprzez szyfrowanie powierzonych danych.

[29] Nr 285/2018/ZP.

[30] Technologia ta opiera się na zasadzie wykorzystania mechanizmów szyfrowania i uwierzytelniania transmisji danych zawartych w przeglądarkach Web. Jej zaletą jest dostępność sieci VPN ze zwykłego komputera PC, na którym nie ma potrzeby instalowania i konfigurowania dodatkowego oprogramowania.

[31] O czym szerzej w sekcji „Stwierdzone nieprawidłowości".

Przetwarzanie danych wrażliwych w bazach danych odbywało się wyłącznie w Szpitalu, na serwerach szpitalnych

(akta kontroli str. 439-447, 643-649, 704-705)

7. Załącznikiem do PBD była Instrukcja postępowania w przypadku naruszenia bezpieczeństwa danych osobowych. Prowadzony od 15 sierpnia 2018 r. Rejestr naruszeń danych osobowych, zawierał informację o jednym naruszeniu zasad ochrony danych osobowych pracowników Szpitala. Wstępną, telefoniczną informację o ujawnieniu w BIP danych osobowych pracowników (opublikowanych w pliku zamówienia publicznego na grupowe ubezpieczenie pracowników) Szpital powziął 18 września 2018 r. W tym samym dniu usunięto błędny załącznik. Dzień później do ZOZ wpłynął drogą elektroniczną oficjalny komunikat w tym zakresie. W dniach od 19-21 września 2018 r. IOD wszczął i prowadził postępowanie wyjaśniające. Ze względu na nieobecność w dniu 21 września 2018 r. (piątek) Dyrektora Szpitala, który posiadał profil zaufany e-PUAP z uprawnieniem reprezentowania Szpitala, zgłoszenie zdarzenia Prezesowi Urzędu, nastąpiło w poniedziałek 24 września 2018 r., tj. po upływie ponad 72 godzin, o których mowa w art. 33 ust. 1 in fine RODO[32]. ADO powiadamiając Prezesa Urzędu, wyjaśnił przyczynę tego opóźnienia.

Rejestr skarg i wniosków w kontrolowanym okresie nie zawierał skarg dotyczących ujawnienia danych osobowych.

(akta kontroli str. 111-118, 516-537)

8. Instrukcja w sprawie udostępniania dokumentacji medycznej określała m.in.: zakres stosowania, odpowiedzialność i uprawnienia, formy udostępniania[33], w tym również na zewnątrz Szpitala, przechowywanie oraz zasady odpłatności. W instrukcji tej przywołano aktualnie obowiązujące przepisy prawa.

Załącznikami do ww. instrukcji były wzory: wniosku o udostępnienie, upoważnienia do odbioru dokumentacji medycznej, wniosku o wydanie oryginału dokumentacji medycznej, upoważnienia do odbioru wyniku badania, protokołu przekazania dokumentacji medycznej. Udostępnienie dokumentacji medycznej przedstawicielowi ustawowemu lub osobie upoważnionej przez pacjenta następowało po złożeniu wniosku o jej udostępnienie. Odbiór dokumentacji przez osobę upoważnioną następował po złożeniu upoważnienia do odbioru dokumentacji medycznej. Udostępnianie dokumentacji medycznej pacjenta na zewnątrz Szpitala organom i podmiotom uprawnionym następowało na podstawie wniosku skierowanego do Dyrektora Szpitala. Kierownik sekcji Statystyki Medycznej i Rozliczeń Szpitala posiadał stałe pełnomocnictwo, udzielone przez Dyrektora, do podpisywania korespondencji związanej z udostępnianiem dokumentacji medycznej jednostkom publicznym i osobom prywatnym.

Uprawnionymi i odpowiedzialnymi za udostępnianie dokumentacji medycznej zgodnie z ww. instrukcją byli:

- ordynatorzy i kierownicy komórek organizacyjnych w sytuacji, kiedy było to niezbędne do zapewnienia dalszego leczenia, a zwłoka w wydaniu dokumentacji mogłaby narazić pacjenta na szkodę na zdrowiu. O fakcie wydania historii, ordynator winien był pisemnie informować Dyrektora. W kontrolowanym okresie powyższe sytuacje nie wystąpiły.

---

[32] W wytycznych Grupy Roboczej art. 29 dotyczących zgłaszania naruszenia ochrony danych osobowych na mocy rozporządzenia 2016/679 wskazano m.in., że po stwierdzeniu naruszenia przez administratora, zgłoszenie - w przypadku naruszenia wymagającego zgłoszenia - musi nastąpić bez zbędnej zwłoki, a jeżeli to możliwe, nie później niż w ciągu 72 godzin.

[33] Do wglądu, poprzez sporządzenie wyciągu, wydanie oryginału za pokwitowaniem z zastrzeżeniem zwrotu po wykorzystaniu, drogą elektroniczną innemu podmiotowi leczniczemu w celu konsultacji, za pośrednictwem poczty zaszyfrowanej.

- lekarze prowadzący leczenie w zakresie udostępniania w ich obecności dokumentacji medycznej do wglądu na prośbę pacjenta,

- pracownicy Sekcji Statystyki Medycznej i Rozliczeń przygotowujący kopie dokumentów, realizujący wydanie oraz wysyłanie dokumentacji uprawnionym organom i podmiotom, a także poświadczanie kopii za zgodność z oryginałem,

- pracownicy Sekcji ds. Obronności i Archiwizacji prowadzący składnicę akt odpowiedzialni w zakresie przygotowania i wydania kopii dokumentów takich jak: karta informacyjna leczenia-wypis, wyniki badań, protokół operacyjny, historie chorób z poradni specjalistycznych.

Wydanie kopii dokumentacji medycznej następowało na wniosek złożony przez pacjenta albo osoby upoważnione, po uprzednim sprawdzeniu tożsamości osoby wnioskującej. Rejestrowano je w „Wykazie udostępnionej dokumentacji medycznej", zgodnym z wymogami art. 27 ust. 4 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta[34]. W okresie od 25 maja 2018 r. do 31 stycznia 2019 r. udostępniono dokumentację medyczną 48 osób, w tym 34 pacjentom oraz 14 upoważnionym osobom fizycznym.

(akta kontroli str. 311-327, 605-607, 631)

W okresie od 25 maja 2018 r. do 31 stycznia 2019 r., do Szpitala wpłynęło 767 wniosków o udostępnienie danych dokumentacji medycznych pacjentów. W wyniku przeprowadzonej procedury weryfikacji poszczególnych wniosków, w 758 przypadkach nastąpiło jej udostępnienie, a w dziewięciu odmówiono go. Powodem odmowy udostępnienia było to że: upłynął termin przechowywania dokumentacji medycznej, wnioskodawca nie był osobą upoważnioną przez pacjenta, wnioskodawca zrezygnował z wniosku lub osoba wymieniona we wniosku nie była hospitalizowana w szpitalu bądź cel wydania dokumentacji medycznej przez podmiot wnioskujący nie podlegał przepisom ustawy. Analiza 30 przypadków udostępnienia dokumentacji medycznej zakładom ubezpieczeń[35] oraz 30 udostępnień dokumentacji innej osobie niż pacjent wykazała, że dokumentację tę udostępniano wyłącznie podmiotom, które występowały ze stosownym wnioskiem oraz posiadały pisemne upoważnienie w tym zakresie. Udostępnienie organom i podmiotom uprawnionym następowało za zgodą Dyrektora Szpitala.

(akta kontroli str. 609-630)

9. Dostęp do pomieszczenia serwerowni był zabezpieczony przed dostępem osób nieuprawnionych. Pomieszczenie to wyposażone w systemy m.in. kontroli dostępu oraz wykrywania pożaru, włamania, zalania. Ponadto serwerownię wyposażono m.in. w urządzenia podtrzymywania napięcia, gaśnice przeciwpożarowe, urządzenia i systemy regulacji temperatury.

(akta kontroli str. 538-542)

Lekarze, pielęgniarki oraz pracownicy administracji Szpitala[36], przetwarzający dane osobowe pacjentów, posiadali uprawnienia w systemie operacyjnym zgodne z przyznanymi przez ADO upoważnieniami do przetwarzania danych osobowych. Dostęp poszczególnych użytkowników do systemu operacyjnego wymagał podwójnego uwierzytelnienia, pierwszego po włączeniu terminala oraz drugiego przy wejściu do systemu informatycznego do obsługi Szpitala. Długość hasła odpowiadała wymogom obowiązującej IZSI. Użytkownicy systemu nie mieli możliwości zainstalowania dowolnego oprogramowania ze względu na charakter terminala bezsystemowego, który nie posiadał dysku twardego. Port USB

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

[35] W rozumieniu ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz. U. z 2019 r. poz. 381).

[36] Próbę wykonano na 30 komputerach po 10 komputerów w każdej grupie

w terminalu nie pozwalał na odczyt zewnętrznych nośników danych. Na serwerach, do których łączyły się terminale zainstalowano oprogramowanie zabezpieczające wraz z aktualną bazą sygnatur wirusów.

(akta kontroli str. 543-603)

Użytkowane przez lekarzy, pielęgniarki, położne oraz pracowników administracji 12laptopów, posiadało aktualne programy antywirusowe. Nie ujawniono komputerów, które posiadałyby zainstalowane starsze wersje systemów operacyjnych, niewspieranych już przez producenta.

(akta kontroli str. 462, 604)

Kierownik Działu Informatyki wyjaśnił, że kopie systemu informatycznego do obsługi Szpitala były wykonywane na bieżąco i przenoszone na nośniki danych. Kopie te przechowywane były poza serwerownią, w odrębnym pomieszczeniu, w specjalnej szafie zamykanej na klucz. Według składającego wyjaśnienia w Szpitalu wykorzystywanych było 12 laptopów, z których tylko jeden służył do przetwarzania danych osobowych[37]. Laptop ten miał zainstalowany system pozwalający na monitorowanie i ochronę danych oraz uniemożliwiał używanie zewnętrznych nośników danych (wyłączone porty USB). W części medycznej szpitala działało 230, a docelowo zaplanowano zainstalowanie 300 bezsystemowych terminali. Ponadto szpital dysponował szyfrowanymi nośnikami danych, które po akceptacji ADO były przez IOD wydawane pracownikom Szpitala.

(akta kontroli str. 462- 464, 466)

Stwierdzone nieprawidłowości

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

1. Od grudnia 2017 r. do dnia zakończenia czynności kontrolnych NIK, tj. przez ponad 14 miesięcy, nie uruchomiono zakupionych za kwotę 23.298,29 zł dziesięciu drukarek opasek.

Dyrektor Szpitala wyjaśnił m.in., że drukarki opasek były jednym z elementów przetargu pod nazwą „Dostawa sprzętu komputerowego, rozbudowa zintegrowanego systemu informatycznego oraz modernizacja sieci komputerowej wraz z niezbędnymi pracami budowlanymi, w celu dostosowania infrastruktury informatycznej szpitala do wdrożenia Elektronicznej Dokumentacji Medycznej", którego realizację przeprowadzano w ciągu trzech lat, tj. w okresie od 31 sierpnia 2015 r. do 31 sierpnia 2018 r. Dodał, że w momencie rozpoczęcia realizacji tego przetargu nie przewidywano remontu SOR i planowano wcześniejsze uruchomienie drukarek (zgodnie z harmonogramem miało to nastąpić w pierwszej połowie 2018 r.). Ze względu na podjęty remont SOR, termin uruchomienia drukarek został przesunięty do końca czerwca 2019 r. Dyrektor Szpitala podkreślił, że po zakończenia tego remontu nastąpi kompleksowe rozmieszczenie i uruchomienie 10 drukarek opasek, uwzględniając Dziecięcą Izbę Przyjęć i Punkt Przyjęć Planowych.

(akta kontroli str. 348, 633-634)

IOD wyjaśnił, że po zakończeniu kompleksowego remontu SOR, zainstalowane zostaną drukarki do wydruku opasek i dalszego ich odczytu przy użyciu skanera. Ponadto wskazał, że stosowany będzie nowy wzór opasek zawierających kod kreskowy (kod QR), numer z księgi głównej pacjenta, nazwę oddziału oraz imię i pierwszą literę nazwiska pacjenta. Po wprowadzeniu systemu kodów z opasek, jak podał IOD, wprowadzone zostaną etapowo tablety na oddziałach, które będą

[37] Laptop ten jest na wyposażeniu Z-cy Dyrektora ds. ekonomicznych i nie jest wykorzystywany poza Szpitalem oraz służy wyłącznie jako stanowisko pracy w gabinecie tej osoby.

zintegrowane z systemem i pozwolą m.in. wyeliminować karty gorączkowe oraz ułatwią wgląd do dokumentacji pacjenta w systemie informatycznym.

(akta kontroli str. 349)

NIK wskazuje, że zgodnie z art. 44 ust. 3 pkt 1 lit. a ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych[38], wydatki publiczne powinny być dokonywane w sposób m.in. oszczędny, z zachowaniem zasady uzyskiwania najlepszych efektów z danych nakładów. Dokonanie zakupu sprzętu, który następnie przez kilkanaście miesięcy stał nieużywany - i to mimo że był w Szpitalu potrzebny, gdyż wpisów na opaskach w części oddziałów dokonywano ręcznie - nie sprzyjało efektywnemu wykorzystaniu środków publicznych, chociażby z uwagi na upływ terminów rękojmi i ewentualnych gwarancji, o których mowa w art. 556 i 577 ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny[39].

2. Pomimo rozpoczęcia z dniem 25 maja 2018 r. stosowania przepisów RODO, 20 umów powierzenia przetwarzania danych osobowych, o których mowa w art. 28 ust. 3 tego rozporządzenia Szpital zawarł dopiero w dniach od 8 czerwca do 27 sierpnia 2018 r. Zgodnie z przywołanym przepisem, przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

IOD wyjaśnił, że Szpital zawierał wszystkie wymagane umowy powierzenia przetwarzania danych osobowych sukcesywnie, w miarę możliwości organizacyjnych ZOZ. Ponadto wskazał, że umowy te wymagały uzgodnienia i akceptacji ze strony podmiotów współpracujących ze Szpitalem. IOD podkreślił, że daty umów powierzenia odzwierciedlały faktyczny czas ich zawarcia.

(akta kontroli str.706-707)

NIK ponownie wskazuje, że jakkolwiek RODO stosowane było od 25 maja 2018 r., to weszło w życie już 24 maja 2016 r. (art. 99 RODO), a co za tym idzie, czas na uprzednie przygotowanie i zawarcie ww. umów był wystarczający.

OCENA CZĄSTKOWA

W Szpitalu wprowadzono rozwiązania organizacyjne zmierzające do zapewnienia ochrony danych osobowych pacjentów oraz poszanowania ich prywatności. Wielokierunkowe działania realizowane przez ZOZ ograniczały ryzyko utraty tych danych osobowych pacjentów w wyniku awarii, błędów lub nieuprawnionej modyfikacji. Personelowi Szpitala zapewniono odpowiedni, zgodny z zakresem wykonywanych czynności dostęp do danych medycznych, a byłym pracownikom niezwłocznie odbierano uprawnienia do korzystania z systemów informatycznych. Prawidłowo stosowano, regularnie zmieniane loginy i hasła, a na czas nieobecności pracowników na stanowiskach pracy blokowano stacje robocze. Usługa opieki serwisowej nad szpitalnym systemem informatycznym została zlecona umową, w której zawarto odpowiednie postanowienia zabezpieczające przetwarzanie danych osobowych, a stosowane przy takim przetwarzaniu środki techniczne i organizacyjne zapewniały stopień bezpieczeństwa adekwatny do ryzyk związanych m.in. ze skalą i rodzajem takiego przetwarzania.

Przez kilkanaście miesięcy nie używano jednak części sprzętu służącego do drukowania znaków identyfikacyjnych, co nie sprzyjało efektywnemu wykorzystaniu środków publicznych przeznaczonych uprzednio na jego zakup. Ponadto 20 z 28

[38] Dz. U. z 2017 r. poz. 2077, ze zm.
[39] Dz. U. z 2018 r. poz. 1025, ze zm.

zawartych umów powierzenia przetwarzania danych zawarto po upływie od dwóch tygodni do dwóch miesięcy od rozpoczęcia stosowania RODO.

IV. Wnioski

W związku ze stwierdzonymi nieprawidłowościami, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK, wnosi o podjęcie działań mających na celu możliwie niezwłoczne rozpoczęcie wykorzystywania w Szpitalu 10 drukarek opasek zakupionych w grudniu 2017 r.

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 7 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do dyrektora Delegatury NIK w Poznaniu. 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 wniosku pokontrolnego oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

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

Poznań, 18 kwietnia 2019 r.

Najwyższa Izba Kontroli
Delegatura w Poznaniu

Kontroler	Dyrektor
Artur Pigłas	z up. Tomasz Nowiński
doradca ekonomiczny	p.o. Wicedyrektora
.....	.....
podpis	*podpis*