NAJWYŻSZA IZBA KONTROLI
Delegatura w Zielonej Górze

LZG.410.002.01.2019

Katarzyna Lebiotkowska
Lubuski Szpital Specjalistyczny
Pulmonologiczno-Kardiologiczny
w Torzymiu Sp. z o.o.

ul. Wojska Polskiego 52
66-235 Torzym

WYSTĄPIENIE POKONTROLNE

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

NAJWYŻSZA IZBA KONTROLI
Delegatura w Zielonej Górze
ul. Podgórna 9a, 65-213 Zielona Góra
T +48 68 410 66 00, F +48 68 410 66 39
lzg@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Lubuski Szpital Specjalistyczny Pulmonologiczno-Kardiologiczny w Torzymiu Sp. z o.o. (dalej: *Szpital* lub *Spółka*).
Kierownik jednostki kontrolowanej	Katarzyna Lebiotkowska, Prezes Zarządu[1] Spółki (Kierownik Szpitala) od 1 kwietnia 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. (data wejścia w życie przepisów RODO[2]) do dnia zakończenia czynności kontrolnych[3].
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[4]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Zielonej Górze
Kontroler	Mariusz Kniat, doradca prawny, upoważnienie do kontroli nr LZG/6/2019 z 7 stycznia 2019r.

(akta kontroli str. 1-5, 11-12)

1 Zarząd Spółki jest jednoosobowy.

2 Rozporządzenie 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 (Dz. Urz. UE L 119 z 2016 r., str. 1, ze zm.), dalej *RODO*.

3 Badania kontrolne mogą dotyczyć działań sprzed tego okresu, jeśli mają związek z zagadnieniami będącymi przedmiotem kontroli.

4 Dz. U. z 2019 r. poz. 489, dalej: *ustawa o NIK*.

II. Ocena ogólna[5] kontrolowanej działalności

OCENA OGÓLNA

Szpital terminowo opracował wymaganą dokumentację oraz procedury związane z ochroną przetwarzanych danych osobowych, jednak dane osobowe nie były w pełni prawidłowo chronione i przetwarzane.

Zgodnie z obowiązującymi wymogami wywiązano się z obowiązku opracowania i wdrożenia dokumentacji oraz procedur dotyczących ochrony danych osobowych, a także powołano na stanowisko Inspektora Ochrony Danych osobę posiadającą odpowiednie przygotowanie i kwalifikacje zawodowe oraz zgłoszono ten fakt Prezesowi Urzędu Ochrony Danych Osobowych. Opracowany terminowo rejestr czynności przetwarzania danych zawierał wymagane elementy. Rzetelnie przeprowadzono i udokumentowano analizę procesów przetwarzania danych. Nie w pełni zrealizowano natomiast obowiązek przeszkolenia pracowników Szpitala uczestniczących w procesie przetwarzania danych osobowych z zagadnień dotyczących bezpieczeństwa danych oraz obowiązywania przepisów RODO, gdyż blisko 60% tych pracowników nie zapoznano z regulacjami dotyczącymi ochrony danych osobowych.

W Szpitalu wdrożono rozwiązania organizacyjne i techniczne zmierzające do zapewnienia prawidłowej ochrony i przetwarzania danych osobowych, nie były one jednak w pełni przestrzegane.

Na ogół prawidłowo chroniono i przetwarzano dane osobowe w skontrolowanych oddziałach szpitalnych[6], poradniach specjalistycznych[7], a także w procesie rejestracji pacjentów[8]. Stwierdzone w tym obszarze nieprawidłowości dotyczyły zamieszczania na łóżkach szpitalnych w jednym z oddziałów[9] danych osobowych (imienia i nazwiska) pacjentów, a także niezapewnienia w procesie rejestracji pełnej ochrony tych danych[10]. Szpital zawierał umowy powierzenia przetwarzania danych w sytuacjach tego wymagających, a w pięciu analizowanych umowach zamieszczono postanowienia wymagane art. 28 RODO. Prawidłowo udostępniano również uprawnionym podmiotom dokumentację medyczną pacjentów oraz rzetelnie prowadzono wykaz dotyczący udostępnienia tych danych.

Wskutek braku bieżącej analizy wymaganych uprawnień personelu Szpitala w dostępie do danych medycznych pacjentów (badaniem objęto 30 pielęgniarek), stwierdzono aż 16 przypadków nadania zbyt szerokich uprawnień w systemie informatycznym[11]. Ponadto ze znacznym opóźnieniem (od 60 do 274 dni od daty rozwiązania stosunku pracy) odbierano możliwości dostępu do tych systemów byłym pracownikom Szpitala.

Prawidłowo zastosowano fizyczne zabezpieczenia serwerowni Szpitala, natomiast w przypadku pomieszczenia do przechowywania kopii zapasowych baz danych Szpitala przyjęte w nim rozwiązania i stwierdzony stan faktyczny nie zapewniały pełnego bezpieczeństwa przechowywanych danych. Sposób użytkowania i zabezpieczenia wykorzystywanych w Szpitalu komputerów stacjonarnych (badaniami objęto 30 komputerów) nie gwarantował pełnej ochrony przetwarzanych na tych komputerach danych osobowych pacjentów, wskutek m.in. nieprzestrzegania wymogów dotyczących obowiązujących haseł oraz praktyce logowania się do systemu operacyjnego z użyciem wspólnego loginu i hasła, a także nieodbierania uprawnień byłym pracownikom.

Podkreślenia wymaga, że jeszcze w toku kontroli podjęto lub zadeklarowano działania zmierzające do usunięcia stwierdzonych nieprawidłowości.

---

5 Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.

6 Oględzinami objęto trzy oddziały szpitalne (sale chorych, dyżurki pielęgniarskie, gabinety lekarskie) tj.: 1. rehabilitacji kardiologicznej, 2. onkologii pulmonologicznej i chemioterapii, 3. gruźlicy i chorób płuc.

7 Oględzinami objęto trzy poradnie: 1. geriatryczną, 2. gruźlicy i chorób płuc, 3. onkologiczną.

8 Oględzinami objęto dwie funkcjonujące w Szpitalu rejestracje, tj. Rejestrację Centralną oraz Rejestrację do poradni kardiologicznej i geriatrycznej.

9 Tj. Oddział gruźlicy i chorób płuc.

10 Z uwagi na usytuowanie trzech stanowisk rejestracyjnych w sposób umożliwiający wzajemne podsłuchanie informacji podawanych przez osoby rejestrujące się.

11 Ww. pielęgniarki oprócz dostępu do danych medycznych (w systemie InfoMedica) pacjentów w komórkach organizacyjnych, w których świadczyły pracę, posiadały również dostęp do danych pacjentów (obszarów – modułów w systemie InfoMedica) z innych oddziałów.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[12] kontrolowanej działalności

OBSZAR

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

Opis stanu faktycznego

1.1. Stosownie do art. 8 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[13] (dalej: *u.o.d.o.*), Prezes Zarząd Spółki powołała[14] z dniem 25 maja 2018 r. Inspektora Ochrony Danych Osobowych (dalej: *IOD*). W zarządzeniu powołującym IOD, a także w Regulaminie Organizacyjnym Szpitala[15] wskazano, że stanowisko to podlega bezpośrednio Prezesowi Zarządu (Administratorowi Danych Osobowych, dalej: *ADO*), co było zgodne z przepisem art. 38 ust. 3 RODO. Osoba wyznaczona na IOD nie pełniła przed wejściem w życie przepisów RODO funkcji Administratora Bezpieczeństwa Informacji Szpitala (dalej: *ABI*).

Do obowiązków IOD należało m.in.: informowanie Kierownika Szpitala, podmiotów przetwarzających dane osobowe oraz pracowników Szpitala o ich obowiązkach dotyczących ochrony danych osobowych, monitorowanie przestrzegania przepisów oraz wewnętrznej polityki w tym obszarze, szkolenie personelu, udzielanie zaleceń co do oceny skutków dla ochrony danych osobowych oraz monitorowanie ich wykonania, a także wykonywanie pozostałych czynności określonych w regulacjach RODO.

(akta kontroli: str. 23-27, 60, 68, 70-71)

Osoba powołana na stanowisko IOD równolegle (na podstawie odrębnej umowy) pełni funkcję Dyrektora do spraw ekonomicznych Szpitala podległego bezpośrednio Prezesowi Zarządu, który odpowiada m.in. za organizowanie pracy Spółki w sposób zapewniający wykonywanie świadczeń zdrowotnych w sposób ekonomicznie racjonalny, w warunkach zgodnych z obowiązującymi przepisami prawa, w celu uzyskania jak najlepszego wyniku ekonomicznego Spółki i nadzoruje prace Działu finansowo-kadrowego, Działu rozliczeń, analiz i sprzedaży oraz Działu usług komercyjnych. Dyrektor do spraw ekonomicznych Szpitala podległy jest bezpośrednio Prezesowi Zarządu.

(akta kontroli: str. 33-34, 70-71)

Prezes Zarządu wyjaśniła, że *Przed decyzją o wyznaczeniu na stanowisko IOD osoby wykonującej równolegle (na podstawie odrębnej umowy) funkcję Dyrektora do spraw ekonomicznych szczegółowo analizowaliśmy różne warianty usytuowania tego stanowiska (w tym również zlecenia usługi na zewnątrz) i uznaliśmy to rozwiązanie za optymalne. W mojej ocenie IOD jest w pełni niezależny w wykonywaniu swych zadań – podlega bezpośrednio Prezesowi Zarządu oraz nie zachodzi jakikolwiek konflikt interesu przy wykonywaniu obu tych zadań. Podkreślenia wymaga, że osoba powołana na to stanowisko jest doskonałym profesjonalistą, a z uwagi na równolegle wykonywanie funkcji Dyrektora ranga i możliwość egzekwowania przypisanych IOD zadań bardzo wzrosła.*

(akta kontroli: str. 245-246)

Zgodnie z wymogami art. 37 ust. 5 RODO, IOD miał należyte przygotowanie i kwalifikacje zawodowe[16] do pełnienia swojej funkcji. W szczególności uczestniczył w szkoleniach i kursach dotyczących tej problematyki[17], a także jest słuchaczem *studiów executive MBA* -

---

12 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.

13 Dz. U. poz. 1000 ze zm.

14 Zarządzeniem nr 14/2018 z dnia 25 maja 2018 r. Prezes Zarządu.

15 Załącznik nr 1 do uchwały nr 44/2018 Zarządu Spółki z dnia 4 października 2018 r. (tekst jednolity).

16 Mgr ekonomii.

17 M.in.: szkolenie z zagadnień dotyczących ochrony danych osobowych i bezpiecznych informacji w podmiotach ochrony zdrowia w ramach projektu "Kompetentni pracownicy systemu ochrony zdrowia" – w okresie od dnia 30.01.2018 do dnia 4.04.2018 r. (ogółem 112 godzin), szkolenie na temat „Vademecum ochrony danych osobowych po zmianie przepisów- najważniejsze aspekty RODO w przedsiębiorstwie - praktyczne szkolenie od podstaw" – w dniu 23 marca 2018 roku (ogółem 8 godzin).

Business Trends w latach 2018-2019, w ramach których problematyka RODO również była przedmiotem zajęć (panel wykładowy).

(akta kontroli: str. 72-75)

Szpital terminowo[18] wywiązał się z obowiązku zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych (dalej *PUODO*) o wyznaczeniu IOD, a przekazane zawiadomienie zawierało elementy wymagane przepisem art. 10 ust. 1 i 3 u.o.d.o.

Dane IOD oraz sposób i formę kontaktu udostępniono na stronie internetowej Szpitala – stosownie do wymogu określonego w przepisie art. 37 ust. 7 RODO.

(akta kontroli: str. 76-82)

Zarządzeniem nr 12/2018 z dnia 8 maja 2018 r. Prezes Zarządu Spółki powołała ośmioosobowy[19] Zespół ds. wdrożenia RODO w Szpitalu (dalej: *Zespół*), do zadań którego należała m.in.: współpraca z audytorem wybranym w celu weryfikacji stanu przetwarzania danych osobowych oraz przeprowadzenia prac konsultacyjnych przy wdrożeniu wymagań RODO (informacje o ww. audycie zamieszczono w pkt. 1.4. niniejszego wystąpienia).

(akta kontroli: str. 83-84)

Szpital nie został dotychczas[20] uznany (nie otrzymał decyzji administracyjnej od właściwego organu do spraw cyberpezpieczeństwa) za operatora usługi kluczowej, o którym mowa w art. 5 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[21].

(akta kontroli: str. 85)

1.2. W dniu wejścia w życie przepisów RODO oraz u.o.d.o. (25 maja 2018 r.) w Szpitalu została przyjęta i zatwierdzona przez Prezesa Zarządu Spółki, Polityka Bezpieczeństwa w zakresie przetwarzania danych osobowych w Szpitalu (dalej: *Polityka*), czym zrealizowano dyspozycję art. 24 ust. 1 i 2 RODO.

We wprowadzeniu do Polityki wskazano m.in., że realizacja postanowień tego dokumentu (obowiązującego wszystkich pracowników Szpitala) ma zapewnić ochronę danych osobowych, właściwą ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemach informatycznych.

Jako podstawę opracowania Polityki podano przepisy RODO, u.o.d.o., a także rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych[22].

W Polityce określono m.in. zadania ADO oraz IOD, a także określono zasady związane z przetwarzaniem danych osobowych, opis zdarzeń naruszających ochronę danych osobowych, wytyczne dotyczące zabezpieczenia danych osobowych, zasady i tryb kontroli przestrzegania zasad zabezpieczania danych osobowych oraz postępowanie w przypadku naruszenia danych osobowych. Integralną częścią Polityki były załączniki dotyczące zasad korzystania z komputerów przenośnych oraz instrukcji korzystania z komputerów przenośnych, na których przetwarzane są dane osobowe. Polityka nie przewidywała konieczności opracowania dodatkowych reguł i procedur uszczegóławiających te dokumenty, poza tymi które były jej załącznikami.

(akta kontroli: str. 86-110)

---

18 Zawiadomienie przekazano w dniu 7 czerwca 2018 r., tj. w terminie 14 dni od wyznaczenie IOD stosownie do wymogu określonego w przepisie art. 10 ust. 1 u.o.d.o.

19 W skład Zespołu weszli następujący pracownicy Szpitala: dyrektor ds. ekonomicznych, dyrektor ds. inwestycji, radca prawna, informatyk, naczelna pielęgniarka, kierownik działu rozliczeń, analiz i sprzedaży, kierownik działu kadr oraz kierownik Biura Zarządu.

20 Według stanu na 31 marca 2019 r.

21 Dz. U. poz. 1560.

22 Dz. U. Nr 100, poz. 1024.

Oprócz Polityki w Szpitalu opracowano i stosowano m.in. następujące dokumenty dotyczące ochrony danych osobowych: wzór umowy powierzenia przetwarzania danych osobowych, klauzula informacyjna o przetwarzaniu danych osobowych pracowników / zleceniobiorców / usługobiorców Szpitala wraz ze zgodą pracownika / zleceniobiorcy / usługobiorcy na utrwalanie i rozpowszechnianie wizerunku oraz wzór zobowiązania do zachowania tajemnicy informacji (poufności), wzór informacji o przetwarzaniu danych osobowych pacjentów (zamieszczony na stronie internetowej Szpitala oraz tablicach ogłoszeń), wzór indywidulanego potwierdzenia przez pacjenta (jego opiekuna prawnego) informacji o przetwarzaniu przez Szpital jego danych osobowych[23], a także wzór klauzuli informacyjnej na podstawie art. 13 RODO (dla wykonawców zamówień publicznych na rzecz Szpitala).

(akta kontroli: str. 111-125)

W okresie objętym kontrolą Szpital nie przeprowadzał aktualizacji Polityki. Od daty wejścia w życie Polityki uchylono jeden z aktów prawnych przywołanych w Polityce, jako stanowiący podstawę jej sporządzenia, tj. ww. rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych (…).

Ponadto w Szpitalu od wejścia w życie przepisów RODO nadal stosowane są wzory upoważnień do przetwarzania danych osobowych stanowiących załącznik do nieobowiązującej od 25 maja 2018 r. wcześniejszej Polityki, a w treści tych upoważnień, jako podstawę do ich wydania wskazano nieobowiązujący od dnia 25 maja 2018 r. przepis art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[24], co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli: str. 86-110, 126-128, 213, 243-244)

W dokumentacji Szpitala brak jest dowodów (potwierdzeń) o przekazaniu (udostępnieniu) pracownikom postanowień Polityki celem zapoznania się i stosowania. Natomiast od listopada 2018 r. pracownicy Szpitala[25] podpisywali dokument pn. *Zobowiązanie pracownika do zachowania tajemnicy informacji*, *których ujawnienie mogłoby narazić Pracodawcę na szkodę* (wg jednolitego wzoru), w którym wprowadzono postanowienie, że pracownik potwierdza, iż został pouczony przez pracodawcę o obowiązku i procedurach ochrony danych osobowych uzyskanych w związku ze świadczeniem pracy.

(akta kontroli: str. 126-128, 206-213)

IOD wyjaśniła, że: *Pracownicy Szpitala wraz z wejściem w życie nowej Polityki Bezpieczeństwa nie byli dotychczas formalnie (poprzez uzyskanie pisemnych potwierdzeń) zaznajamiani się z jej treścią. Nie mniej jednak w trakcie prowadzonych w Szpitalu szkoleń zbiorowych i indywidulanych każdorazowo informowaliśmy o zasadach i procedurach dotyczących ochrony danych osobowych obowiązujących w naszym Szpitalu. Jednocześnie deklaruję, że w najbliższym czasie zamierzamy zintensyfikować działalność szkoleniową i szczegółowo poinformować pracowników o wymogach wynikających z Polityki Bezpieczeństwa oraz zaznajomić ich z tym dokumentem.*

(akta kontroli: str. 126-128)

1.3. Rejestr czynności przetwarzania danych osobowych (dalej: *Rejestr*), o którym mowa w art. 30 RODO, został sporządzony w dniu 25 maja 2018 r. Zgodnie z wymogami art. 30 ust. 3 RODO, rejestr prowadzony był w formie pisemnej i elektronicznej oraz zawierał wszystkie wymagane elementy.

Według stanu na 31 marca 2019 r. w Rejestrze ujęto dziewięć czynności (procesów) przetwarzania danych, dla których dokonano identyfikacji oraz analizy zagrożeń w celu zabezpieczenia (ogólny opis technicznych i organizacyjnych środków bezpieczeństwa,

---

[23] Poprzez własnoręczny podpis na pieczątce zamieszczanej w dokumentacji medycznej pacjenta.

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

[25] Ustalono na podstawie analizy akt osobowych 30 pielęgniarek zatrudnionych w Szpitalu.

o których mowa w art. 32 ust. 1 RODO) danych osobowych adekwatnie do zidentyfikowanych zagrożeń.

(akta kontroli: str. 129-133)

1.4. W okresie objętym kontrolą IOD przeprowadził (ADO zatwierdził) jedną analizę procesów przetwarzania danych osobowych pacjentów Szpitala[26] (dalej: *Analiza*), o której mowa w art. 32 RODO. W opracowaniu Analizy uczestniczyli również członkowie Zespołu ds. wdrożenia RODO w Szpitalu (opisano w pkt. 1.1. niniejszego wystąpienia).

W ramach ww. Analizy zidentyfikowano 16 zagrożeń (ryzyk) związanych z ochroną danych osobowych. Dla każdego z nich oszacowano wartość ryzyka poprzez określenie parametrów dotyczących „Wpływu" (w skali od 0 do 5 punktów[27]) oraz „Prawdopodobieństwa" (w skali od 0 do 5 punktów[28]) określoną jako iloczyn ww. parametrów. Jako „ryzyka pomijalne" wskazano wartość ryzyka <2 pkt., „ryzyka, na które należy zwrócić szczególną uwagę" – od 3 do 6 pkt., „ryzyka, które należy monitorować" – od 7 do 14 pkt., „ryzyka niedopuszczalne" >15 pkt.

W rezultacie przeprowadzonej Analizy, jako stanowiące największe zagrożenie (poziom ryzyka – 9-12 punktów) wskazano kolejno następujące incydenty: [1] awaria serwerów; [2] brak możliwości przywrócenia kopii zapasowej baz danych; [3] pożar w pomieszczeniach serwerowni; [4] utrata papierowej dokumentacji archiwalnej w archiwum zakładowym [5] nie zachowanie tajemnicy służbowej przez zatrudniony personel. Pozostałe sytuacje (ryzyka) zostały zakwalifikowane do ryzyk, na które należy zwrócić szczególną uwagę (od 3 do 6 punktów).

(akta kontroli: str. 134-136)

W Analizie dla każdego z wyspecyfikowanych ryzyk wskazano także środki zabezpieczenia i środki do wdrożenia celem ograniczenia lub wyeliminowania ryzyka. Wg stanu na dzień 19 marca 2019 r. stan realizacji środków do wdrożenia dla czterech ww. incydentów (sytuacji) stanowiących największe zagrożenie (12 punktów) przedstawiał się następująco: [1] *awaria serwerów* – w Analizie przewidziano dwa środki do wdrożenia[29] – nie wykonano żadnego; [2] *brak możliwości przywrócenia kopii zapasowej baz danych* – w Analizie przewidziano dwa środki do wdrożenia[30] – nie wykonano żadnego; [3] *pożar w pomieszczeniach serwerowni* – w Analizie przewidziano trzy środki do wdrożenia[31] – nie wykonano żadnego; [4] utrata papierowej dokumentacji archiwalnej w archiwum zakładowym – w Analizie przewidziano jeden środek do wdrożenia[32] – nie został wykonany.

(akta kontroli: str. 126-128, 134-137, 245-246, 275-282)

IOD wyjaśniła, że: *Brak wdrożenia środków wskazanych w Analizie wynika przede wszystkim z kosztów ich realizacji. Priorytetem działalności Szpitala jest zapewnienie pacjentom najlepszej opieki medycznej, a to wymaga kierowania w pierwszej kolejności środków finansowych na poprawę tego obszaru. Znaczna część działań dotyczących poprawy funkcjonowania infrastruktury sieci informatycznej (komputerów, serwerów, baz danych) nastąpi po realizacji projektu Lubuskie e-Zdrowie, którego Szpital jest planowanym beneficjentem. Jednocześnie deklaruję, że przy sporządzaniu corocznych planów rzeczowo-finansowych szpitala weźmiemy pod uwagę możliwość wdrożenia środków wskazanych w analizie, przy uwzględnieniu sytuacji finansowej Szpitala.*

(akta kontroli: str. 126-128)

---

26 Dokument pn. Analiza i Ocena Ryzyka w *Lubuskim Szpitalu Specjalistycznym Pulmonologiczno-Kardiologicznym w Torzymiu Sp. z o.o.* z dnia 25 maja 2018 r.

27 Tj.: 0 – brak, 1 – pomijalny, 2 – mały, 3 – średni, 4 – duży, 5 – ekstremalny.

28 Tj.: 0 – brak, 1 – rzadko, 2 – nieprawdopodobne, 3 – możliwe, 4 – prawdopodobne, 5 – mało prawdopodobne.

29 Tj.: 1. Redundantne serwer pracujące w klastrze HA - w przypadku awarii jednego drugi przejmuje automatycznie działanie 2. Gwarancje na sprzęt serwerowy NBD (naprawa następnego dnia roboczego).

30 Tj.: 1. Poza sprawdzeniem sum kontrolnych brak możliwości sprawdzenia kopi zapasowej głównego systemu bazodanowego (testowe przywrócenie pełni danych) - obecnie wykorzystywany serwer bazodanowy ze względów zasobowych nie zezwala na taką operację bez kilkunastogodzinnego przestoju. 2. Zakup nowego serwera oraz licencji - konfiguracja serwera w postaci wirtualizacji ułatwiająca i przyśpieszająca proces przywracania nie tylko bazy danych ale całej maszyny wirtualnej.

31 Tj.: 1. Alarm ppoż.; 2. System gaszenia gazem; 3. Redundantne serwery w innej lokalizacji.

32 Tj.: 1. Wdrożenie systemów powiadamiających o pożarze, zalaniu, włamaniu.

Przy sporządzaniu ww. Analizy wykorzystano wyniki (raport) audytu przygotowania organizacji (Szpitala) do wymogów RODO przeprowadzonego w Szpitalu przez podmiot zewnętrzny (dalej: *Audytor*)[33], przed wejściem w życiu przepisów RODO (w dniach 14-15 maja 2018 r.).

W podsumowaniu wyników audytu zarekomendowano – w celu dostosowania Szpitala do wymagań RODO – m.in. następujący plan działania: - opracowanie rejestru czynności przetwarzania danych osobowych, - wykonanie analizy ryzyka, - podpisanie umów powierzenia z podwykonawcami, - realizację obowiązków informacyjnych, - przygotowanie polityki bezpieczeństwa, - przeszkolenie pracowników z przepisów RODO. Ponadto jako główne problemy, które należy wyeliminować wskazano ograniczenie dostępu do danych osobowych z poziomu współdzielonych kont, wyeliminowanie zagrożeń związanych z użytkowaniem systemu Windows XP oraz zapewnienie optymalnej temperatury w pomieszczeniu serwerowni.

Informacje dotyczące stanu zabezpieczenia pomieszczeń serwerowni oraz użytkowanych w Szpitalu komputerów przedstawiono w pkt. 2.9. niniejszego wystąpienia.

(akta kontroli: str. 138-148, 275-282, 287-292)

W dniu 4 czerwca 2018 r. w Szpitalu sporządzono (podpisany przez Prezes Zarządu) dokument pn. *Raport z analizy i oceny ryzyka w Szpitalu* (dalej *Raport*). W Raporcie podano m.in., że w oparciu o wyniki ww. Analizy, audytu wewnętrznego oraz praktyki z procesów biznesowych z lat poprzednich nie stwierdzono występowania w Szpitalu ryzyka niedopuszczalnego.

W części procesów biznesowych stwierdzono natomiast występowanie poważnych ryzyk w zakresie dostępności oraz utarty danych ze względu na brak dualnej serwerowni, przy czym wskazano, że niwelowanie tego ryzyka jest bardzo kosztochłonne i musi być rozłożone w czasie. Za niewystarczające uznano także zabezpieczenia wprowadzone w archiwum zakładowym. Wskazano także za konieczne sukcesywną wymianę niewspieranego oprogramowania komputerowego, gdyż ze względu na brak aktualizacji systemy te mają większą podatność na awarie oraz próby włamań informatycznych.

W Raporcie wskazano również, że poprawa stanu zabezpieczenia serwerowni oraz użytkowanego sprzętu komputerowego powinna nastąpić po realizacji projektu Lubuskie e-Zdrowie dofinansowanego ze środków unijnych, którego Szpital jest beneficjentem.

(akta kontroli: str. 149)

W Studium Wykonalności dla projektu Lubuskie e-Zdrowie[34] wskazano m.in., że w ramach tego projektu w przypadku Szpitala przewidywana jest rozbudowa istniejącego systemu HIS (system medyczny) oraz systemu ERP (system administracyjny), a także doposażenie Szpitala w infrastrukturę macierzowo-serwerową oraz w oprogramowanie i urządzenia końcowe. Do dnia zakończenia niniejszej kontroli ww. projekt był w trakcie przygotowania[35].

(akta kontroli: str. 150-167)

1.5. W Szpitalu dotychczas nie została wykonana ocena skutków dla ochrony danych (dalej: *DPIA*), o której mowa w art. 35 RODO (wykonanie DPIA w przypadku Szpitala jest fakultatywne). Obowiązek wykonania tej oceny dotyczy bowiem planowanych operacji przetwarzania dla ochrony danych osobowych przed rozpoczęciem ich przetwarzania, a Szpital, wraz z wejściem w życie RODO, nie rozpoczął przetwarzania nowych kategorii danych, w szczególności z użyciem nowych technologii.

(akta kontroli str. 126-128)

---

33 Na podstawie umowy nr ZP.381.TP.33.2018 z dnia 8 maja 2018 r.

34 Opracowanym na zlecenie Urzędu Marszałkowskiego Województwa Lubuskiego, wersja sierpień 2018 r.

35 http://bip.lubuskie.pl/zamowienia_publiczne/11/487/E2_80_9ESwiadczenie_uslugi_nadzoru_sprawowanego_w_imieniu_Zamawiajacego_w_zakresie_prawidlowosci_realizacji_Projektu_pod_nazwa__E2_80_9ELubuskie_e-Zdrowie_E2_80_9D_2C__0D_0Aw_charakterze_Inzyniera_Kontraktu__E2_80_9D_0D_0A/ - dostęp 21.03.2019 r.

IOD wyjaśniła, że: *Szpital w mojej ocenie nie jest zobowiązany do wykonania DPIA, jednak w najbliższym czasie rozważymy zasadność jej przeprowadzenia i w zależności od tej analizy podejmiemy decyzję o wykonaniu bądź odstąpieniu od wykonania tej oceny.*

(akta kontroli: str. 126-128)

1.6. Jednym z zadań IOD, w myśl art. 39 ust. 1 lit. b RODO, jest prowadzenie szkoleń personelu uczestniczącego w operacjach przetwarzania danych. Kwestie przeprowadzania szkoleń zostały również określone w Regulaminie Organizacyjnym Szpitala (§ 15 pkt 38) oraz w Zarządzeniu kierownika Szpitala w sprawie powołania IOD, gdzie wskazano, że do zadań IOD należy m.in. podnoszenie świadomości personelu Szpitala oraz szkolenie personelu uczestniczącego w procesie przetwarzania danych osobowych. Również w ww. Analizie, Raporcie oraz wynikach audytu (opisanych w pkt. 1.6. niniejszego wystąpienia) zadanie dotyczące szkolenia pracowników wskazano jako jeden z kluczowych środków do wdrożenia.

(akta kontroli str. 26, 60, 71, 148-149)

W Szpitalu opracowano Terminarz planowanych w 2018 r. i w 2019 r. szkoleń wewnętrznych (po jednym w każdym półroczu, bez wskazywania konkretnych dat i grup/pracowników do przeszkolenia).

(akta kontroli str. 168)

Ustalono, że do dnia 21 marca 2019 r. przeszkolonych zostało ogółem 92 spośród 219[36] pracowników Szpitala (tj. 42%), z tego 62 na szkoleniu zbiorowym zorganizowanym w dniu 11 grudnia 2018 r. w Szpitalu (Zespół szkoleniowy w składzie: IOD, radca prawna, informatyk, naczelna pielęgniarka), a 30 pracowników w drodze indywidulanych szkoleń.

Udział osób przeszkolonych w poszczególnych grupach pracowników Szpitala przedstawiał się następująco: lekarze (20%), pielęgniarki (61,5%), ratownicy medyczni (18,2%), sekretarki medyczne i rejestratorki (50%), technicy RTG (100%), fizjoterapeuci (11%), opiekunowie medyczni (13%), administracja (29%), personel pomocniczy (39%).

Z analizy ww. danych wynika, że prawie 60% pracowników Szpitala nie zostało dotychczas przeszkolonych z zakresu RODO, co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str. 126-128, 169-175)

Badanie w zakresie przeszkolenia z przepisów RODO 30 pracowników Szpitala[37] zaangażowanych w proces przetwarzania danych medycznych pacjentów wykazało, że:

- wszyscy posiadali udokumentowany fakt zapoznania się z regulacjami wewnętrznymi Szpitala w zakresie ochrony danych osobowych oraz złożyli oświadczenie o poufności – na obowiązującym w Szpitalu wzorze, przy czym oświadczenia takie składano od listopada 2018 r. (tj. po upływie blisko pół roku od wejścia w życie przepisów RODO),
- jedenastu uczestniczyło w zorganizowanym przez IOD (Zespół szkoleniowy) wewnętrznym zbiorowym szkoleniu,
- czterech przeszkolono indywidualnie (wg oświadczeń IOD i Naczelnej Pielęgniarki), przy czym faktu tego nie potwierdzono w dokumentacji Szpitala (brak pisemnych potwierdzeń).

(akta kontroli str. 170-175)

1.7. Szpital nie zobowiązał się formalnie (np. poprzez deklarację stosowania) do przestrzegania regulacji zawartych w *Kodeksie postępowania dla sektora ochrony zdrowia*[38], dla którego wniosek o przyjęcie został 13 listopada 2018 r. przedłożony PUODO lub pozostałych opracowań związanych z ochroną danych osobowych, takich jak

[36] Wg stanu na 31.12.2018 r.
[37] W próbie wskazanej w pkt. 2.3. niniejszego wystąpienia.
[38] Treść kodeksu została opublikowana na stronie internetowej: www.rodowzdrowiu.pl.

Przewodnik po RODO w służbie zdrowia[39] i *Wytyczne dotyczące inspektorów ochrony danych*[40].

IOD poinformowała, że: (…) *w znacznej mierze postępowanie Szpitala dostosowane jest do zasad określonych projektem Kodeksu Branżowego w Ochronie Zdrowia przygotowanego przez Polską Federację Szpitali i złożonego do zatwierdzenia Prezesowi UODO wnioskiem z dnia 13.11.2018 r. (np. w zakresie zasad przetwarzania danych pacjentów, dostępu do danych pacjenta i nadawania uprawnień, udostępnianiu danych dotyczących pacjenta zgodnie z ustawą z dnia 6 listopada 2008 roku o prawach pacjenta i Rzeczniku Praw Pacjenta, spełniania obowiązków informacyjnych wobec Pacjentów, zbierania tylko tych danych, które są wystarczające do identyfikacji pacjentów).*

(akta kontroli str. 176)

Stwierdzone nieprawidłowości

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

1. Obowiązująca w Szpitalu Polityka Bezpieczeństwa nie była dotychczas aktualizowana, pomimo że od jej wejścia w życie (tj. 25 maja 2018 r.) uchylono jeden z aktów prawnych stanowiących podstawę jej opracowania, tj. ww. rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, a w Szpitalu nadal stosowane są wzory upoważnień do przetwarzania danych osobowych stanowiących załącznik do nieobowiązującej od 25 maja 2018 r. wcześniejszej Polityki, przy czym w treści tych upoważnień, jako podstawę do ich wydania wskazano nieobowiązujący od dnia 25 maja 2018 r. przepis art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[41].

   (akta kontroli: str. 86-110, 126-128, 213, 243-244)

   IOD wyjaśniła, że: *Faktycznie dotychczas nie przeprowadzaliśmy aktualizacji obowiązującej w Szpitalu Polityki Bezpieczeństwa ochrony danych osobowych, co wynikało przede wszystkim z ogromu realizowanych przeze mnie zadań, jednak w mojej ocenie taka aktualizacja w najbliższym czasie powinna zostać dokonana. Pozwoli to na dostosowanie Polityki i przyjętych w zakresie ochrony danych osobowych dokumentów (w tym wzorów stosowanych upoważnień) do aktualnie obowiązujących wymogów. Przy dokonywaniu aktualizacji skorzystamy również z ustaleń i uwag poczynionych w trakcie kontroli NIK.*

   (akta kontroli str. 126-128)

2. IOD nie wywiązała się w pełni z obowiązku prowadzenia szkoleń personelu uczestniczącego w operacjach przetwarzania danych, wynikającego z art. 39 ust. 1 lit. b RODO. Szkoleniami w zakresie obowiązywania przepisów RODO dotychczas nie zostało bowiem objętych 58% pracowników Szpitala, a w niektórych grupach zawodowych uczestniczących w procesie przetwarzania danych odsetek osób nieprzeszkolonych był jeszcze wyższy i wynosił: lekarze (80%), ratownicy medyczni (81,8%), fizjoterapeuci (89%), opiekunowie medyczni (87%), administracja (71%). Ponadto w przypadku szkoleń indywidulanych fakt ich przeprowadzenia nie był potwierdzany w dokumentacji Szpitala, co nie pozwala na rzetelne ustalenie m.in. liczby osób przeszkolonych i terminu przeprowadzenia szkolenia.

   (akta kontroli str. 126-128, 168-175)

   IOD wyjaśniła, że *Brak przeszkolenia tak znacznej liczby pracowników wynikał w znacznej mierze z trudności w jednoczesnym zebraniu pracowników wykonujących podstawowe obowiązki dotyczące opieki medycznej nad pacjentami również w systemie zmianowym. Ponadto z uwagi na początkowy okres obowiązywania tych przepisów i związany z tym brak wypracowanych praktyk, orzeczeń sądowych czy praktycznych komentarzy, intensyfikacja tych szkoleń miała nastąpić w czasie, gdy zagadnienia te już będą bardziej znajome. Jednocześnie deklarują, że do końca I połowy br.*

[39] Opublikowany 24 września 2018 r. na stronie internetowej Ministerstwa Cyfryzacji.
[40] Opublikowane 10 maja 2018 r. na stronie internetowej Urzędu Ochrony Danych Osobowych.
[41] Dz. U. z 2016 r. poz. 922, ze zm.

przeszkoleni zostaną wszyscy pracownicy przetwarzający dane osobowe. Natomiast błąd dotyczący niepotwierdzania udziału pracownika w szkoleniu indywidulanym zostanie wyeliminowany przez wprowadzenie wzoru dokumentu potwierdzającego m.in. termin i zakres tego szkolenia.

(akta kontroli str. 126-128)

W toku kontroli NIK[42] w Szpitalu wprowadzono do stosowania wzór protokołu potwierdzającego przeprowadzenie indywidulanego szkolenia pracownika z zakresu RODO.

(akta kontroli str. 177)

OCENA CZĄSTKOWA

Szpital terminowo wywiązał się z obowiązku opracowania i wdrożenia dokumentacji oraz procedur dotyczących ochrony danych osobowych, jednak dokumentacja ta wymaga aktualizacji. Wywiązano się również z obowiązku powołania na stanowisko IOD osoby posiadającej odpowiednie przygotowanie i kwalifikacje zawodowe oraz terminowo zawiadomiono o tym fakcie PUODO.

Opracowany terminowo rejestr czynności przetwarzania danych zawierał wymagane elementy. Rzetelnie przeprowadzono i udokumentowano analizę procesów przetwarzania danych oraz zidentyfikowano ryzyka wraz z określeniem środków do wdrożenia (działań) celem eliminacji lub ograniczenia tych ryzyk, przy czym dotychczas – wskutek ograniczonych środków finansowych Szpitala – nie wdrożono tych działań.

Nie w pełni zrealizowano obowiązek przeszkolenia pracowników Szpitala uczestniczących w procesie przetwarzania danych osobowych z zagadnień dotyczących bezpieczeństwa danych oraz obowiązywania przepisów RODO. Blisko 60% tych pracowników nie zostało bowiem objętych takimi szkoleniami, a w niektórych grupach zawodowych odsetek osób nieprzeszkolonych przekraczał 80%.

Podkreślenia wymaga, że jeszcze w toku kontroli podjęto lub zadeklarowano działania zmierzające do usunięcia stwierdzonych nieprawidłowości.

OBSZAR

2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych.

Opis stanu faktycznego

2.1. Przeprowadzone oględziny wszystkich (dwóch) funkcjonujących w Szpitalu rejestracji[43] wykazały, że w celu właściwej ochrony danych osobowych pacjentów funkcjonowały poniżej wymienione rozwiązania:

- w każdej rejestracji umieszczono klauzule informacyjne RODO (w formie wydruku) ogólnodostępne dla osób rejestrujących się;
- zapewniono aby w obrębie wzroku pacjenta znajdującego się przy stanowisku rejestracji nie znajdowały się dokumenty zawierających dane osobowe innych pacjentów. Dokumenty osób już zarejestrowanych były na bieżąco przenoszone do gabinetów zabiegowych lub poradni Szpitala;
- wszystkie komputery (cztery) znajdujące się w rejestracjach było ustawione w sposób uniemożliwiający wgląd w treści na nich wyświetlane osobom rejestrującym się;
- pacjenci po zarejestrowaniu otrzymywali specjalnie przygotowane karteczki, na których podawano datę i godzinę wizyty oraz numer właściwego gabinetu;
- pracownicy rejestracji nie wypowiadali na głos informacji zawierających dane osobowe, przekazując jedynie dane dotyczące dalszego procesu postępowania po zarejestrowaniu się do danej poradni lub gabinetu;
- identyfikacja pacjentów odbywała się na podstawie okazanych rejestratorce dowodów tożsamości wg kolejności przyjścia do rejestracji (brak urządzeń elektronicznych wspomagających proces rejestracji);
- w każdej z rejestracji znajdowały się szafki zamykane na klucz na przechowywania dokumentacji pacjentów;

---

42 Tj. z dniem 21 marca 2019 r.

43 Tj.: 1. Rejestracji Centralnej Szpitala zlokalizowanej w budynku głównym, segment II, 2. Rejestracji do poradni kardiologicznej i geriatrycznej, zlokalizowanej w tzw. „budynku w lesie", pomieszczenie 01/09.

- w przypadku jednej rejestracji (Rejestracja Centralna) usytuowanie trzech stanowisk rejestracyjnych bezpośrednio obok siebie z uwagi na bardzo małą odległość między nimi oraz brak przesłon (barier) między stanowiskami może powodować, że osoba znajdująca się przy stanowisku słyszy informacje podawane przez osobę rejestrującą się przy drugim stanowisku. Ponadto poza zamieszczeniem przy stanowiskach informacji o treści „Prosimy o przebywanie przy stanowisko recepcyjnym tylko jednego pacjenta" nie wprowadzono innych rozwiązań (np. poziomych linii) zapewniających odstęp pomiędzy osobami przy okienku, a kolejnymi osobami w kolejce, a odległość usytuowanych przed stanowiskami miejsc siedzących dla osób oczekujących na rejestrację nie uniemożliwiała podsłuchanie informacji podawanych przez osoby rejestrujące się. Powyższe ustalenia wraz z wyjaśnieniem szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str. 178-185)

We wszystkich trzech objętych oględzinami gabinetach poradni specjalistycznych Szpitala[44], dokumentację pacjentów przechowywano we właściwy sposób, tj. pacjent wchodzący do gabinetu nie miał możliwości zapoznania się z danymi osobowymi innych osób oczekujących w kolejce lub tych, którzy odbyli już wizytę. Ponadto w trakcie oględzin, nie zaobserwowano, aby którykolwiek gabinet został pozostawiony bez opieki oraz nie stwierdzono przypadków pozostawienia klucza w drzwiach i opuszczenia przez personel gabinetu poradni. Wywoływanie pacjentów wszystkich poradni odbywało się w sposób gwarantujący im anonimowość, tj. pacjenci wchodzili do gabinetu poradni wg kolejności zapisów na wizytę (numer i godzina wizyty wskazana w procesie rejestracji).

(akta kontroli str. 186-189)

Przeprowadzone oględziny dyżurek pielęgniarskich, sal chorych oraz gabinetów lekarskich na trzech oddziałach szpitalnych[45] wykazały m.in., że:

- na oddziałach znajdowało się łącznie: 57 sal chorych (161 łóżek), dziewięć gabinetów lekarskich oraz siedem dyżurek pielęgniarskich;
- w przypadku wszystkich 129 zaobserwowanych pacjentów nie stwierdzono braku na nadgarstku opaski informacyjnej zawierającej numer pacjenta[46];
- na dwóch oddziałach[47] nie stwierdzono umieszczania kart z danymi pacjentów na lub przy łóżkach pacjentów, natomiast na zajętych łóżkach (57) na Oddziale gruźlicy i chorób płuc zamieszczono karty z imieniem i nazwiskiem pacjentów w sposób umożliwiający odczytanie tych danych dla osób przebywających w tych salach (w tym osób postronnych np. odwiedzających chorych). Powyższe szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości";
- ruch chorych[48] prowadzony był w dyżurkach pielęgniarskich w miejscu niewidocznym dla osób postronnych;
- we wszystkich dyżurkach pielęgniarskich podręczna dokumentacja pielęgniarska przechowywana była w zamykanych na klucz szafkach, nie stwierdzono nieprawidłowości w zakresie sposobu użytkowania i zabezpieczenia komputerów w dyżurkach (ogółem siedem);

---

44 Oględzinami objęto trzy poradnie: 1. Poradnia geriatryczna – pomieszczenie 01/04 w tzw. „budynku w lesie", 2. Poradnia gruźlicy i chorób płuc, pomieszczenie 007, budynek główny, segment II, 3. Poradnia onkologiczna, pomieszczenie 007, budynek główny, segment II.

45 Oględzin objęto trzy oddziały szpitalne (sale chorych, dyżurki pielęgniarskie, gabinety lekarskie) tj.: 1. Oddział rehabilitacji kardiologicznej, tzw. „budynek w lesie, 2. Oddział onkologii pulmonologicznej i chemioterapii, budynek główny, segment I, 3. Oddział gruźlicy i chorób płuc, budynek główny, segment II oraz III.

46 Opaski wypisywane byłe ręcznie i zawierały wyłącznie numer pacjenta (Medyczny Identyfikator Pacjenta) z systemu InfoMedica, po którym można było zidentyfikować dane pacjenta (historię choroby).

47 Tj.: Oddział rehabilitacji kardiologicznej, Oddział onkologii pulmonologicznej i chemioterapii.

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

- w gabinetach lekarskich dokumentacja medyczna przechowywana była w zamykanych na klucz szafkach, nie stwierdzono nieprawidłowości w zakresie sposobu użytkowania i zabezpieczenia komputerów w gabinetach.

(akta kontroli str. 190-197)

Ponadto w ramach przeprowadzonych oględzin stwierdzono, że w Szpitalu (na żadnym z oddziałów, rejestracji, poradni) nie funkcjonował monitoring wizyjny.

(akta kontroli str. 178-183, 186-197)

2.2. Według stanu na 11 marca 2019 r. personel działów administracyjnych[49] Szpitala liczył 23 osoby[50]. Analiza uprawnień w systemie InfoMedica[51], jakie zostały nadane wszystkim osobom z tej grupy wykazała, że odpowiadały one zakresom zadań i obowiązków realizowanych przez tych pracowników. I tak:

– 12 osób nie posiadało dostępu do systemu InfoMedica, co wynikało z ich zakresów obowiązków (nie realizowali oni zadań wymagających dostępu do danych medycznych pacjentów Szpitala);

– pięć osób posiadło nadane uprawnienia w tym systemie, które pozwalały im na dostęp do danych medycznych niezbędny z punktu widzenia realizowanych przez nich zadań, a także pisemne upoważnienia do przetwarzania danych osobowych[52];

– sześć osób posiadło ograniczony dostęp do danych w systemie InfoMedica (np. tylko do danych księgowych lub kadrowych).

(akta kontroli str. 200-205)

2.3. Analiza przeprowadzona na próbie 30 (z 84) pielęgniarek[53] zatrudnionych w Szpitalu[54] wykazała, m.in. że:

– wszystkie posiadały dostęp w systemie InfoMedica do danych medycznych pacjentów w komórkach organizacyjnych (oddziały, izba przyjęć), na których świadczyły pracę, a także pisemne upoważnienia do przetwarzania danych osobowych,

– 16 spośród nich (tj. 53,3%), oprócz ww. dostępu do danych medycznych pacjentów w komórkach organizacyjnych, na których świadczyły pracę, posiadały również dostęp do danych pacjentów (obszarów – modułów w systemie InfoMedica) z innych oddziałów, co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str. 206-215)

Ustalono, że żadnej z osób zatrudnionych lub wykonujących na podstawie umów cywilnoprawnych[55] zadania salowej lub sprzątaczki nie nadano uprawnień w systemie InfoMedica do przetwarzania danych osobowych pacjentów, a także upoważnień do przetwarzania danych osobowych, co było działaniem prawidłowym.

(akta kontroli str. 216)

2.4. W okresie od 25 maja 2018 r. do 28 lutego 2019 r. Szpital rozwiązał stosunek pracy/umowę cywilnoprawną z 23 osobami. Spośród nich, osiem osób w trakcie zatrudnienia/świadczenia zadań miało przyznany dostęp do systemów informatycznych, w tym systemu InfoMedica. Przeprowadzona analiza terminu odebrania uprawnień wszystkim ośmiu ww. osobom wykazała, że:

– w przypadku pięciu osób dostęp do systemów informatycznych dotyczył danych medycznych, natomiast w trzech przypadkach danych administracyjnych;

---

49 Biuro Zarządu, Dział Finansowo-Kadrowy, Dział Administracyjno-Gospodarczy, Dział Administracyjno-Eksploatacyjny, Dział Rozliczeń i Analiz, stanowiska samodzielne w Administracji Szpitala.

50 Stan na 28 luty 2019 r.

51 System typu HIS (*Hospital Information System* – rodzaj oprogramowania do obsługi ruchu pacjentów wewnątrz podmiotu leczniczego).

52 Pracownicy Działu Rozliczeń i Analiz oraz Administrator systemów informatycznych (informatyk).

53 Szpital nie zatrudniał położnych.

54 Na umowę o pracę oraz umowy cywilnoprawne (zlecenie) - stan na 13 marca 2019 r.

55 Ogółem 33 osoby - stan na 13 marca 2019 r.

– we wszystkich przypadkach dostęp do systemu InfoMedica został zablokowany w toku kontroli NIK (w dniu 1 marca 2019 r.), tj. po upływie od 60 do 274 dni od daty rozwiązania stosunku pracy/umowy cywilnoprawnej; przy czym w jednym przypadku administrator systemów informatycznych Szpitala dokonał zmiany hasła dostępu (po upływie 124 dni po zakończeniu zatrudnienia, dostęp zblokowano po upływie 274 po zakończeniu zatrudnienia), co szerzej opisano w dalszej części wystąpienia, w sekcji *„Stwierdzone nieprawidłowości”*.

(akta kontroli str. 217-221)

2.5. W myśl postanowień umowy serwisowej Szpital obowiązany był do zgłaszania błędów w działaniu systemu InfoMedica poprzez witrynę internetową help-desk'u wykonawcy znajdującą się pod adresem www.hd.asseco.pl lub poprzez strony autoryzowanych przedstawicieli serwisowych wykonawcy (wskazanych przez wykonawcę).

(akta kontroli str. 222-237)

Do przesyłania zgłoszeń związanych z błędami lub wadliwym działaniem systemu informatycznego InfoMedica wykorzystywano serwisy internetowe znajdujące się pod adresem: https://hd.asseco.pl (ogólne błędy dotyczące aktualizacji), http://serwis.jts.pl (błędy związane z działaniem modułów administracyjnych), http://infobud.eu/ (błędy związane z działaniem modłów medycznych).

Przeprowadzone oględziny sposobu przekazania 11 (100%) zgłoszeń serwisowych z okresu od 25 maja 2018 do 1 marca 2019 r. związanych z błędami lub wadliwym działaniem systemu informatycznego InfoMedica wykazały m.in., że:

– wszystkie zgłoszenia serwisowe były przekazywane przez administratora systemów informatycznych Szpitala, przy czym w dniu oględzin dziewięć zgłoszeń miało status „zamknięty”, a dwa zgłoszenia (przekazane w dniu 26 oraz 27 lutego 2019 r.) status „otwarte”,

– wszystkie zgłoszenia zrealizowano drogą elektroniczną z wykorzystaniem ww. serwisów internetowych, przy czym w przypadku żadnego ze zgłoszeń nie przekazywano danych osobowych (w tym danych medycznych) pacjenta.

(akta kontroli str. 238-239)

2.6. Szpital w okresie objętym kontrolą posiadał 16 umów dotyczących powierzenia przetwarzania danych osobowych, w których wystąpił jako podmiot powierzający przetwarzanie danych oraz 8 umów gdzie wskazano go jako podmiot przetwarzający dane osobowe.

(akta kontroli str. 240)

Ustalono, że umowy dotyczące powierzenia przetwarzania danych zawierano z podmiotami (wykonawcami) realizującymi na rzecz Szpitala zadania związane m.in. ze: świadczeniem usług informatycznych oraz serwisu oprogramowania, badaniami z zakresu diagnostyki obrazowej, usługami laboratoryjnymi, współpracy i konsultacji medycznych.

Analiza pięciu umów (porozumień)[56] dotyczących powierzenia przez Szpital przetwarzania danych osobowych pięciu wykonawcom, ww. usług wykazała m.in. że:

– zawierały one wymagane postanowienia określone w art. 28 ust. 3 RODO i stanowiły integralną część umowy na świadczenie usług zawartej z danym podmiotem zewnętrznym,

[56] Tj. umowy (porozumienia): 1. Z dnia 19.11.2018 r. dotycząca realizacji zadań w zakresie opisywania badań tomografii komputerowej i opisywania badań radiologicznych w oparciu o teleradiologię, 2. Z dnia 25.05.2018 r. dotycząca realizacji zadań w zakresie wykonywania badań radioizotopowych i Rezonansu magnetycznego pacjenci, 3. Z dnia 25.05.2018 r. dotycząca realizacji zadań w zakresie wykonywania badań genetycznych, 4. Z dnia 25.05.2018 r. dotycząca realizacji zadań w zakresie wykonywania badań densytometrycznych, 5. Z dnia 25.05.2018 r. dotycząca realizacji zadań w zakresie wykonywania badań diagnostycznych i konsultacyjnych.

– w każdej z pięciu umów powierzenia wskazany zakres danych osobowych, jaki został powierzony przez Szpital podmiotowi zewnętrznemu, wynikał z rodzaju usług, jakie zgodnie z umową na ich świadczenie miał na rzecz Szpitala realizować wykonawca.

(akta kontroli str. 241-242)

Według stanu na 11 marca 2019 r. usługi na rzecz Szpitala świadczyło na podstawie kontraktów 26 lekarzy (lekarze kontraktowi), przy czym każdy z nich posiadał odrębne imienne pisemne upoważnienie do przetwarzania danych osobowych – z ww. lekarzami nie zawierano umów (porozumień) dotyczących powierzenia przetwarzania danych osobowych.

(akta kontroli str. 243-246)

Prezes Zarządu wyjaśniła, że *Z uwagi na charakter, zakres i cel świadczeń realizowanych przez lekarzy kontraktowych na rzecz Szpitala ich status jest – w mojej ocenie – tożsamy z lekarzami wykonującymi świadczenia na podstawie umowy o pracę, zwłaszcza w zakresie zapewnienia ochrony danych osobowych pacjentów. Dlatego przyjęliśmy jednolite rozwiązanie dotyczące wydawania pisemnych, imiennych upoważnień dla wszystkich lekarzy, bez względu na formę ich zatrudnienia (umowy o pracę albo kontrakty).*

(akta kontroli str. 245-246)

2.7. W Polityce Bezpieczeństwa określono m.in. procedury postępowania w przypadku naruszenia danych osobowych (rozdział VI). W szczególności określono katalog zdarzeń wskazujących na naruszenie danych osobowych, sposób postępowania oraz osoby zobowiązane do określonych działań w przypadku stwierdzenia naruszenia danych osobowych, a także konieczność dokumentowania przez IOD w formie raportów przypadków naruszeń. Zaistniałe naruszenia – wg zapisów Polityki – mogą stać się przedmiotem szczegółowej analizy prowadzonej przez zespół powołany przez ADO.

Analiza postanowień Polityki wykazała ponadto, że:

– nie wprowadzono obowiązku prowadzenia rejestru przypadków (incydentów) naruszeń ochrony danych osobowych,

– nie wprowadzono obowiązku zgłaszania organowi nadzoru każdego przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia (art. 33 ust. 1 RODO).

(akta kontroli str. 86-110)

IOD wyjaśniła, że (…) *przy najbliżej aktualizacji Polityki Bezpieczeństwa uzupełnimy jej zapisy o wprowadzenie postanowień dotyczących obowiązku prowadzenia rejestru przypadków (incydentów) naruszeń ochrony danych osobowych oraz wprowadzimy obowiązek zgłaszania organowi nadzoru naruszeń, o których mowa w art. 33 ust. 1 RODO. Jednocześnie informuję, że dotychczasowy brak takich zapisów w Polityce nie wywoływał negatywnych skutków, gdyż formą dokumentowania ewentualnych incydentów były raporty, a obowiązek zgłaszania organowi nadzoru i tak wynikał z przepisów RODO. Jednak w celu zapewnienia objęcia regulacjami Polityki Bezpieczeństwa całości zagadnień RODO uważam za zasadne uzupełnienie jej zapisów o te postanowienia.*

(akta kontroli str. 184-185)

W okresie objętym kontrolą w Szpitalu nie odnotowano przypadków (incydentów) naruszenia ochrony danych osobowych.

(akta kontroli str. 297)

2.8. W okresie objętym kontrolą, w Szpitalu funkcjonowały procedury dotyczące udostępniania danych osobowych, opracowane 10 sierpnia 2015 r. (Instrukcja Systemu Zarządzania Jakością - *Wytyczne prowadzenia i przechowywania dokumentacji medycznej pacjenta*). W myśl tych regulacji oraz zgodnie z przepisem art. 26 ust. 1 oraz ust. 3 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta[57] (dalej: *u.o.p.p.*), dokumentację medyczną udostępnia się pacjentowi lub jego przedstawicielowi

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

ustawowemu, bądź osobie upoważnionej przez pacjenta oraz podmiotom określonym w ust. 3 ww. przepisu. Ponadto w procedurach wewnętrznych określono m.in. wzór wniosku o udostępnienie dokumentacji medycznej, wzór upoważnienia do wydania kopii dokumentacji medycznej oraz karta wydania/udostępnienia oryginału dokumentacji medycznej.

W okresie objętym kontrolą w Szpitalu informacje o udostępnieniu dokumentacji medycznej każdorazowo ujmowano w wykazie, o którym mowa w art. 27 ust. 4 u.o.p.p. (prowadzono odrębne wykazy udostępniania dokumentacji dla instytucji oraz dla osób prywatnych). W Szpitalu nie prowadzono ewidencji spraw, w przypadku których odmówiono udostępnienia dokumentacji. Powyższą ewidencję założono w toku kontroli NIK[58].

(akta kontroli str. 247-264)

W okresie od 25 maja 2018 r. do 21 lutego 2019 r., w prowadzonym przez Szpital wykazie odnotowano ogółem 26 przypadków udostępnienia dokumentacji medycznej, w tym osobom fizycznym (osiem przypadków) oraz podmiotom zewnętrznym (18 przypadków[59]).

Wśród nich odnotowano dwa przypadki dotyczące udostępnienia tej dokumentacji osobie upoważnionej innej niż pacjent, którego udostępniana dokumentacja medyczna dotyczyła oraz trzy przypadki udostępnienia jej komercyjnym instytucjom ubezpieczeniowym.

Przeprowadzona analiza prawidłowości udostępnienia dokumentacji w odniesieniu do wszystkich (pięciu) ww. przypadków wykazała, że:

- w jednym przypadku osoba upoważniona osobiście odebrała dokumentację medyczną, natomiast w pozostałych czterech przypadkach dokumentację przesyłano pocztą za zwrotnym potwierdzeniem odbioru;
- w każdym przypadku udostępniono kopię dokumentacji medycznej;
- we wszystkich przypadkach (pięciu) dokumentacja medyczna została udostępniona osobom/instytucjom, które posiadały pisemne upoważnienie pacjenta do dostępu do tej dokumentacji na podstawie wniosków o jej udostępnienie;
- osoby udostępniające dane w imieniu Szpitala każdorazowo posiadały wymagane upoważnienie.

(akta kontroli str. 268-273)

2.9. Regulacje dotyczące ochrony danych przed ich utratą w wyniku awarii, błędów lub nieuprawnionej modyfikacji zostały opisane w Polityce Bezpieczeństwa (rozdział IV) oraz w *Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych*[60] (dalej: *Instrukcja*), a także w *Zasadach korzystania z komputerów przenośnych, na których są przetwarzane dane osobowe*[61] (dalej: *Zasady*). W dokumentach tych określono m.in.: [1] zasady zabezpieczenia przed nieautoryzowanym dostępem do baz danych, w tym przez Internet; [2] zasady bezpiecznego użytkowania komputerów przenośnych, w tym ich transportu, przechowywania danych, blokowania dostępu; [3] metody i środki uwierzytelniania w systemie informatycznym; [4] procedury nadawania i zmiany uprawnień do przetwarzania danych osobowych oraz rejestrowania tych uprawnień w systemie informatycznym; [5] procedury rozpoczęcia, zawieszenia i zakończenia pracy przez użytkowników systemów informatycznych; [6] procedury tworzenia kopii zapasowych systemów informatycznych oraz przechowywania nośników zawierających dane oraz kopii zapasowych; [7] środki ochrony systemu informatycznego oraz monitorowanie dostępu do danych; [8] procedury wykonywania przeglądów i konserwacji systemu informatycznego.

(akta kontroli str. 86-110)

---

58 W dniu 1 marca 2019 r.

59 Z tego 15 dotyczyło przekazania dokumentacji instytucjom publicznym (np. ZUS, KRUS, Sądy, Prokuratura).

60 Stanowiącej załącznik nr 2 do Polityki Bezpieczeństwa.

61 Stanowiących załącznik nr 1 do Polityki Bezpieczeństwa.

Oględziny jedynej serwerowni Szpitala[62] wykazały, m.in. że właściwie: [1] zabezpieczono dostęp do tego pomieszczenia, stosując drzwi na zamek otwierany kluczem oraz dodatkowo zabezpieczony zamkiem elektromagnetycznym oraz kratę i folię antywłamaniową na oknie (jedynym); [2] w pomieszczeniu umieszczono gaśnicę typu D (wolnostojącą) oraz układ klimatyzacji; [3] wszystkie urządzenia znajdowały się na tzw. podłodze antystatycznej oraz ok. 10 cm powyżej poziomu posadzki; [4] na wypadek czasowego zaniku zasilania zastosowano układy podtrzymujące napięcie UPS (3 szt.); [5] wszystkie urządzenia informatyczne zamontowano w specjalnie do tego przystosowanych szafach typu RACK.

Ponadto ustalono, że w serwerowni nie było widocznych rur mogących stanowić potencjalne zagrożenie zalaniem, a także nie pozostawiono w niej elementów, materiałów, urządzeń niezwiązanych z funkcjonowaniem serwerowni, które mogłyby wywołać ryzyko pożaru lub sprzyjać jego rozprzestrzenieniu.

(akta kontroli str. 275-282)

Kopie zapasowe baz danych Szpitala, w myśl przepisów § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI oraz postanowień Instrukcji, były przechowywane w pomieszczeniu znajdującym się w innym niż serwerownia budynku Szpitala[63].

Oględziny tego pomieszczenia wykazały, że przyjęte w nim rozwiązania i stwierdzony stan faktyczny nie zapewniały pełnego bezpieczeństwa przechowywanych w nim kopii baz danych z uwagi na: [1] drzwi do pomieszczenia zamykane były na jeden zamek patentowy (brak innych zabezpieczeń), a okno (jedno) nie posiadało żadnych zabezpieczeń; [2] w pomieszczenia brak było gaśnicy, systemu klimatyzacji; [3] działające w pomieszczeniu urządzenia informatyczne (serwer) umieszczone były na drewnianym stole (brak szafek typu RACK); [4] w pomieszczeniu umiejscowiono rury CO (pod sufitem), które w razie awarii mogłyby zalać urządzenia elektroniczne; [5] w pomieszczeniu znajdowały się elementy, materiały, urządzenia niezwiązane z jego funkcją, które mogłoby wywoływać ryzyko pożaru bądź sprzyjać jego rozprzestrzenieniu (np. pudła tekturowe, zbędny sprzęt – m.in. aparat USG, dwie uszkodzone kserokopiarki), co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str. 275-283)

Ponadto w Szpitalu dotychczas nie wdrożono przewidzianych w Analizie środków eliminujących lub ograniczających ryzyko pożaru[64] (opis wraz z wyjaśnieniami zamieszono w pkt 1.4. niniejszego wystąpienia), a serwerownia i objęte oględzinami pomieszczenie na przechowywanie kopii zapasowych baz danych nie posiadały systemu alarmowego, przeciwwłamaniowego ani przeciwpożarowego.

Prezes Zarządu wyjaśniła, że: *W miarę możliwości finansowych Szpitala postaramy się sukcesywnie podejmować działania zamierzające do poprawy bezpieczeństwa infrastruktury technicznej, w tym serwerowni. W szczególności w zakresie bezpieczeństwa pożarowego. Jednocześnie informuję, że radykalna poprawa funkcjonowania infrastruktury sieci informatycznej powinna nastąpić wskutek wdrożenia projektu Lubuskie e-Zdrowie, którego Szpital jest planowanym beneficjentem.*

(akta kontroli str. 245-246)

Oględziny 30 komputerów stacjonarnych Szpitala, w tym 20 wykorzystywanych na oddziałach Szpitala przez lekarzy (10), pielęgniarki (10) oraz 10 użytkowanych w dziale Administracji Szpitala, wykazały m.in., że:

– na 19 komputerach zainstalowany był system operacyjny Windows XP, dla którego producent oprogramowania zakończył wsparcie techniczne 8 kwietnia 2014 r., a po tym dniu producent przestał dostarczać aktualizacje zabezpieczeń, poprawki niezwiązane

---

62 Serwerownia umiejscowiona w Budynku głównym Szpitala - segment II, pomieszczenie 03, w której znajdowały się serwery z bazami danych medycznych, w tym dane osobowe pacjentów Szpitala oraz pracowników.

63 Pomieszczenie umiejscowione w Budynku Oddziału rehabilitacji kardiologicznej, tzw. „budynek w lesie", pomieszczenie 01/12, w której przechowywane są kopie zapasowe baz danych, w tym danych osobowych pacjentów.

64 Tj.: 1. Alarm ppoż.; 2. System gaszenia gazem; 3. Redundantne serwery w innej lokalizacji.

z zabezpieczeniami, bezpłatne lub płatne opcje asystowanej pomocy technicznej i aktualizacje zawartości technicznej online, co znacznie wpływało na bezpieczeństwo tych systemów operacyjnych. W związku z tym w Szpitalu istnieje potencjalna możliwość, iż urządzenia te stwarzają ryzyko dla bezpieczeństwa infrastruktury informatycznej jednostki, które może skutkować nieprawidłowościami w przyszłości;

- na wszystkich użytkownicy posiadali ograniczone uprawnienia w systemie operacyjnym, które nie pozwalały na wprowadzanie zmian w konfiguracji tych urządzeń oraz instalację oprogramowania;
- wszystkie były zarządzane domenowo i na każdym z nich był zainstalowany był program antywirusowy, posiadający aktualną wersję bazy sygnatur wirusów;
- w żadnym nie zostały zablokowane porty USB, umożliwiając podłączenie do nich nośników pamięci i kopiowanie danych;
- 27 komputerów było wykorzystywanych do przetwarzania danych w systemie InfoMedica, z tego 23 do danych medycznych, a cztery do przetwarzania danych osobowych pracowników Szpitala;
- na dziewięciu komputerach użytkowanych wspólnie przez personel medyczny, użytkownicy logowali się do systemu operacyjnego z użyciem wspólnego loginu i hasła, co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości";
- w sześciu przypadkach hasło do systemu operacyjnego Windows, a w 21 przypadkach hasło do systemu InfoMedica było niezgodne z zasadami przyjętymi w Polityce Szpitala (zbyt mała liczba znaków lub brak spełnienia wymogów złożoności hasła), co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości";
- wbrew wymogom przyjętym w Polityce Szpitala hasła do systemu operacyjnego Windows oraz hasła do systemu InfoMedica nie podlegały okresowej zmianie, a trzykrotne błędne wpisanie hasła do sytemu operacyjnego Windows nie skutkowało zablokowaniem dostępu, co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str. 287-292)

Kopie zapasowe baz danych – stosownie do wymogów określonych w Polityce – tworzone były automatycznie na serwerze bazodanowym co 24 h. Wytworzona w ten sposób kopia pobierana była przez skrypt na serwerze zapasowym znajdującym się w innej lokalizacji. Kopie dodatkowo spakowane RAR przechowywane były na tym serwerze przez ok. rok. Ponadto raz w miesiącu jedna paczka RAR kopiowana była na zewnętrzny szyfrowany dysk USB i zamykana na szafie.

(akta kontroli str. 293)

W Szpitalu poza opaskami noszonymi przez pacjentów nie stosowano innych form pseudoanonimizacji danych. Pracownicy Szpitala wykorzystywali 14 komputerów przenośnych, przy czym tylko jeden zawierał dane osobowe[65] i był używany poza terenem Szpitala (dyski tego komputera były szyfrowane[66]).

(akta kontroli str. 294, 298)

Stwierdzone nieprawidłowości

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

1. W przypadku jednej rejestracji (Rejestracja Centralna) usytuowanie trzech stanowisk rejestracyjnych bezpośrednio obok siebie z uwagi na bardzo małą odległość między nimi oraz brak przesłon (barier) między stanowiskami może powodować, że osoba znajdująca się przy stanowisku słyszy informacje podawane przez osobę rejestrującą się przy drugim stanowisku. Ponadto poza zamieszczeniem przy stanowiskach informacji o treści „Prosimy o przebywanie przy stanowisko recepcyjnym tylko jednego

65 Komputer użytkowany przez Dyrektor ds. ekonomicznych – zawierał dane osobowe pracowników Szpitala i dostęp do danych systemu InfoMedica (moduł administracyjny).

66 Programem BitLocker.

pacjenta" nie wprowadzono innych rozwiązań (np. poziomych linii) zapewniających odstęp pomiędzy osobami przy okienku, a kolejnymi osobami w kolejce, a odległość usytuowanych przed stanowiskami miejsc siedzących dla osób oczekujących na rejestrację nie uniemożliwiała podsłuchanie informacji podawanych przez osoby rejestrujące się.

Tak zorganizowany sposób rejestracji pacjentów, stanowił naruszenie art. 24 ust. 1 RODO, w którym jako jeden z obowiązków ADO wskazano wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających ochronę danych osobowych. Ponadto, w myśl Przewodnika po służbie zdrowia, należy dążyć do minimalizacji ryzyka ujawnienia informacji osobom postronnym w procesie rejestracji, wyznaczając obszar, w którym może przebywać wyłącznie obsługiwany pacjent.

(akta kontroli str. 178-185)

IOD wyjaśniła, że: *Pracownicy Szpitala zostali przeszkoleni o konieczności zachowania poufności podczas procesu rejestracji pacjentów. Rejestracja odbywa się po okazaniu dowodu osobistego pacjenta oraz skierowania od właściwego lekarza. W najbliższym czasie postaramy się szczegółowo przeanalizować – w miarę posiadanych możliwości finansowych – warianty rozwiązań techniczno-organizacyjnych zapewniających zwiększenia ochrony danych osobowych pacjentów w Rejestracji Centralnej.*

(akta kontroli str. 184-185)

2. Na jednym z trzech objętych oględzinami oddziałów szpitalnych[67] zamieszczono na łóżkach pacjentów karty z ich imieniem i nazwiskiem w sposób umożliwiający odczytanie tych danych przez osoby przebywające w tych salach (w tym również osoby postronne, np. gości odwiedzających chorych).

   W myśl przepisu art. 13 u.o.p.p., pacjent ma prawo do zachowania w tajemnicy przez osoby wykonujące zawód medyczny informacji z nim związanych, uzyskanych w związku wykonywaniem tego zawodu. Ponadto zgodnie z przepisem art. 24 ust. 1 RODO Szpital jest zobowiązany do wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z przepisami RODO.

   (akta kontroli str. 184-185, 190-196)

   IOD wyjaśniła, że: *Stwierdzona praktyka zamieszczania na łóżkach szpitalnych na Oddziale gruźlicy i chorób płuc informacji o imieniu i nazwisku pacjenta jest niedopuszczalna i została już wyeliminowana. Według informacji uzyskanych od Ordynatora oddziału oraz pielęgniarek miała ona na celu ułatwić identyfikację pacjenta, co eliminowałby ewentualne ryzyka związane z niewłaściwym rozpoznaniem pacjenta, zwłaszcza w sytuacji dużej rotacji personelu na tym oddziale. Aktualnie wprowadzone rozwiązanie polegające na umieszczeniu tych danych w specjalnych koszulkach (bez możliwości ich bezpośredniego odczytania przez osoby postronne) zapewnia zgodność z obowiązującymi przepisami przy jednoczesnym zapewnieniu personelowi łatwej identyfikacji pacjenta w celu wyeliminowania zgłaszanych ryzyk.*

   (akta kontroli str. 184-185)

   W toku kontroli NIK wyeliminowano powyższą nieprawidłowość poprzez zamieszczanie imienia i nazwiska pacjenta w specjalnych koszulkach – dane niewidoczne dla osób postronnych.

   (akta kontroli str. 196)

3. Analiza zakresu posiadanego dostępu do danych medycznych 30 (z 84) pielęgniarek[68] zatrudnionych w Szpitalu[69] wykazała, że 16 spośród nich (tj. 53,3%), oprócz dostępu do danych medycznych (w systemie InfoMedica) pacjentów w komórkach organizacyjnych, w których świadczyły pracę, posiadały również dostęp do danych pacjentów (obszarów – modułów w systemie InfoMedica) z innych oddziałów, na których nie świadczyły pracy.

---

[67] Tj. Oddział gruźlicy i chorób płuc.

[68] Szpital nie zatrudniał położnych.

[69] Na umowę o pracę oraz umowy cywilnoprawne (zlecenie) - stan na 13 marca 2019 r.

I tak przykładowo pielęgniarka świadcząca pracę na Oddziale rehabilitacji pulmonologicznej posiadała również dostęp (uprawnienie w systemie InfoMedica) do danych pacjentów z Oddziału chorób płuc, Oddziału onkologii pulmonologicznej i chemioterapii, a także z Zakładu opiekuńczo-leczniczego.

(akta kontroli str. 206-215)

Stosownie do przepisu § 20 ust. 2 pkt 4 KRI zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie 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. Ponadto w przepisie art. 5 ust. 1 lit. c RODO wskazano zasadę adekwatności i minimalizacji danych, tj. wymóg ustalenia, kto i w jakim zakresie, powinien być uprawniony do przetwarzania danych.

Administrator systemów informatycznych w Szpitalu wyjaśnił, że: (…) *Pozostawianie tych uprawnień było naszym niedopatrzeniem wynikającym z braku bieżącej analizy adekwatności dostępu do danych tylko do tych modułów w programie InfoMedica, które są niezbędne do wykonywania obowiązków służbowych. Jednocześnie informuję, że dostęp do zbędnych danych został tym pielęgniarkom już cofnięty i w przyszłości na bieżąco będzie monitorowane nadawanie i cofanie uprawnień w systemach informatycznych.*

(akta kontroli str. 214-215)

W toku kontroli NIK zablokowano dostęp ww. pracowników do danych pacjentów (obszarów – modułów w systemie InfoMedica) z oddziałów, w których nie wykonywały pracy.

(akta kontroli str. 211, 214-215)

4. Konta użytkownika w systemie InfoMedica, ośmiu byłych pracowników/osób wykonujących zdania na podstawie umowy zlecenia Szpitala, zostały zablokowane dopiero w toku kontroli NIK (w dniu 1 marca 2019 r.), tj. po upływie od 60 do 274 dni od daty rozwiązania stosunku pracy/umowy cywilnoprawnej; przy czym w jednym przypadku administrator systemów informatycznych Szpitala dokonał zmiany hasła dostępu (po upływie 124 dni po zakończeniu zatrudnienia, dostęp zblokowano po upływie 274 po zakończeniu zatrudnienia).

Stanowiło to naruszenie § 20 ust. 2 pkt 5 rozporządzenia KRI, zgodnie z którym należy podejmować działania polegające na bezzwłocznej zmianie uprawnień, w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji.

(akta kontroli str. 217-221)

Administrator systemów informatycznych w Szpitalu wyjaśnił, że: *Tak późne zablokowanie dostępu byłych pracowników do będących w posiadaniu Szpitala systemów informatycznych wynikało z mojego przeoczenia. Jako administrator systemów informatycznych oraz jedyny informatyk w Szpitalu wykonuję wiele zadań i nie zawsze jestem w stanie na bieżąco cofać uprawnienia byłym pracownikom. Pragnę również zauważyć, że zdarzają się przypadki powtórnego zatrudnienia, zwłaszcza na stanowiskach medycznych, w związku z powyższym zbyt szybkie cofnięcie dostępu wymagałoby procedury ponownego nadawania uprawnień. Jednocześnie deklaruję, że w przyszłości każdorazowo po otrzymaniu z kadr informacji o rozwiązaniu stosunku pracy lub umowy zlecenia bezzwłocznie będę cofał uprawnienia dostępu do systemów informatycznych Szpitala.*

(akta kontroli str. 220-221)

5. Oględziny pomieszczenia do przechowywania kopii zapasowych baz danych Szpitala[70] wykazały, że przyjęte w nim rozwiązania i stwierdzony stan faktyczny nie zapewniały pełnego bezpieczeństwa przechowywanych w nim kopii baz danych (zwłaszcza w zakresie przeciwdziałania ryzyku wystąpienia i rozprzestrzenienia się pożaru) z uwagi

[70] Pomieszczenie umiejscowione w Budynku Oddziału rehabilitacji kardiologicznej, tzw. „budynek w lesie", pomieszczenie 01/12, w której przechowywane są kopie zapasowe baz danych, w tym danych osobowych pacjentów.

na składowanie w nim przedmiotów łatwopalnych oraz urządzeń niezwiązanych z jego funkcją (np. pudła tekturowe, zbędny sprzęt – m.in. aparat USG, dwie uszkodzone kserokopiarki), przy jednoczesnym braku w pomieszczeniu gaśnicy oraz systemów przeciwpożarowych.

(akta kontroli str. 275-283)

Administrator systemów informatycznych w Szpitalu wyjaśnił, że *Zbędne elementy umieszczone w serwerowni zastępczej zostały już z niej usunięte, a pomieszczenie zostało wyposażone w gaśnicę przeznaczoną do gaszenia urządzeń elektrycznych do 1000 V. Jednocześnie deklaruję, że w przyszłości nie będę składował tam żadnych niezwiązanych z przeznaczeniem tego pomieszczenia elementów lub materiałów, które mogłyby sprzyjać rozprzestrzenianiu się pożaru.*

(akta kontroli str. 283)

Po zakończeniu oględzin ww. przedmioty zostały usunięte z pomieszczenia, które ponadto zostało wyposażone w gaśnicę typu D.

(akta kontroli str. 284-286)

6. Na dziewięciu spośród 30 objętych oględzinami komputerów użytkowanych wspólnie przez personel medyczny Szpitala, użytkownicy logowali się do systemu operacyjnego z użyciem wspólnego loginu i hasła.

Działanie to było niezgodne z postanowieniami Polityki[71] oraz z § 20 ust. 2 pkt. 7 lit. a i § 21 ust. 2 pkt 3, w związku z § 20 ust. 1 rozporządzenia KRI, gdyż bez przyznania indywidualnych loginów użytkownikom, nie jest możliwa prawidłowa rozliczalność systemów. Taki sposób autoryzacji nie pozwala na ustalenie, która z osób fizycznych używających tego samego (jednego) loginu, przetwarzała w systemach (w tym przypadku w systemie operacyjnym) dane podlegające prawnej ochronie.

(akta kontroli str. 214-215, 287-292)

Administrator systemów informatycznych w Szpitalu wyjaśnił, że *Powyższe rozwiązanie wynika wyłącznie ze względów organizacyjno-technicznych. Taki sposób logowania się personelu do systemu operacyjnego, do komputerów użytkowanych przez wielu użytkowników, usprawnia pracę pielęgniarek. Należy mieć również na uwadze, że dostęp do danych osobowych (medycznych) pacjentów możliwy jest jedynie po zalogowaniu się przy pomocy zindywidualizowanego loginu i hasła do systemu InfoMedica, gdyż nie przechowujemy danych medycznych na dyskach twardych komputerów. Jednocześnie deklaruję, że przeanalizujemy powyższe zagadnienie w celu wyeliminowania ewentualnych ryzyk związanych z współdzieleniem komputerów.*

(akta kontroli str. 214-215)

7. Wbrew postanowieniom Polityki[72] w sześciu przypadkach (na 30 zbadanych) hasło do systemu operacyjnego Windows, a w 21 przypadkach hasło do systemu InfoMedica było niezgodne z przyjętymi zasadami (zbyt mała liczba znaków lub hasło nie spełniało wymogów złożoności); hasła nie podlegały okresowej zmianie (w Polityce wymóg zmiany hasła do systemu InfoMedica co 30 dni, faktycznie wymuszanie zmiany hasła ustawiono na 180 dni, ważność hasła do systemu operacyjnego ustawiona bezterminowo – system nie wymuszał zmiany hasała), a trzykrotne błędne wpisanie hasła do sytemu operacyjnego Windows nie skutkowało zablokowaniem dostępu do systemu.

(akta kontroli str. 214-215, 287-292)

Administrator systemów informatycznych w Szpitalu wyjaśnił, że *W najbliższym czasie postaram się wyeliminować te błędy m.in. poprzez wprowadzenia mechanizmów wymuszających wymogi jakościowe oraz zmianę hasła w terminach wynikających z postanowień Polityki Bezpieczeństwa, a także blokowanie dostępu do sytemu Windows po próbie trzykrotnego wpisania*

---

71 Określonym w rozdziale IV *Procedura rozpoczęcia, zawieszenia i zakończenia pracy przez użytkowników systemu informatycznego*.

72 Określonymi w rozdziale III *Metody i środki uwierzytelniana w systemie* informatycznym oraz IV *Procedura rozpoczęcia, zawieszenia i zakończenia pracy przez użytkowników systemu informatycznego*.

błędnego hasła. Dotychczasowa sytuacja podyktowana była w pewnej mierze względami praktycznymi, gdyż zbyt częsta zmiana haseł stwarza pracownikom dodatkowe obowiązki i może utrudniać bieżące wykonywanie podstawowych zadań, jakimi są świadczenie usług zdrowotnych.

(akta kontroli str. 214-215)

W toku kontroli NIK, ustawiono ważność hasła do systemu InfoMedica na 30 dni oraz długość hasła na minimum osiem znaków, a także wprowadzono blokadę do sytemu Windows po trzykrotnym błędnym wprowadzeniu hasła.

(akta kontroli str. 295-296)

OCENA CZĄSTKOWA

W Szpitalu wdrożono rozwiązania organizacyjne i techniczne zmierzające do zapewnienia prawidłowej ochrony i przetwarzania danych osobowych. Nie były one jednak w pełni przestrzegane.

W szczególności na ogół prawidłowo chroniono i przetwarzano dane osobowe w skontrolowanych oddziałach szpitalnych[73], poradniach specjalistycznych[74], a także w procesie rejestracji pacjentów[75]. Stwierdzone w tym obszarze nieprawidłowości dotyczyły zamieszczania na łóżkach szpitalnych na jednym z oddziałów[76] danych osobowych (imienia i nazwiska) pacjentów, a także niezapewnienia – z uwagi na usytuowanie trzech stanowisk rejestracyjnych[77] w sposób umożliwiający wzajemne podsłuchanie informacji podawanych przez osoby rejestrujące się – pełnej ochrony tych danych.

Szpital zawierał umowy powierzenia przetwarzania danych w sytuacjach tego wymagających, a w pięciu analizowanych umowach zamieszczono postanowienia wymagane art. 28 RODO. Prawidłowo udostępniano również uprawnionym podmiotom dokumentację medyczną pacjentów oraz rzetelnie prowadzono wykaz dotyczący udostępnienia tych danych.

Wskutek braku bieżącej analizy wymaganych uprawnień personelu Szpitala w dostępie do danych medycznych pacjentów (badaniem objęto 30 pielęgniarek), stwierdzono aż 16 przypadków nadania zbyt szerokich uprawnień w systemie informatycznym[78]. Ponadto ze znacznym opóźnieniem (od 60 do 274 dni od daty rozwiązania stosunku pracy) odbierano możliwości dostępu do tych systemów byłym pracownikom Szpitala.

Prawidłowo zastosowano fizyczne zabezpieczenia serwerowni Szpitala, natomiast w przypadku pomieszczenia do przechowywania kopii zapasowych baz danych Szpitala przyjęte w nim rozwiązania i stwierdzony stan faktyczny nie zapewniały pełnego bezpieczeństwa przechowywanych danych, w tym zwłaszcza w zakresie ryzyk związanych z pożarem.

We wszystkich 30 badanych komputerach zainstalowany był program antywirusowy, aktualny na dzień przeprowadzenia oględzin. Należy jednak zauważyć, że sposób użytkowania i zabezpieczenia wykorzystywanych w Szpitalu komputerów stacjonarnych nie gwarantował – wskutek m.in. nieprzestrzegania wymogów dotyczących obowiązujących haseł oraz praktyce logowania się do systemu operacyjnego z użyciem wspólnego loginu i hasła – pełnej ochrony przetwarzanych na tych komputerach danych osobowych pacjentów.

Podkreślenia wymaga, że jeszcze w toku kontroli podjęto lub zadeklarowano działania zmierzające do uśnięcia stwierdzonych nieprawidłowości.

---

73 Oględzinami objęto trzy oddziały szpitalne (sale chorych, dyżurki pielęgniarskie, gabinety lekarskie) tj.: 1. Oddział rehabilitacji kardiologicznej, 2. Oddział onkologii pulmonologicznej i chemioterapii, 3. Oddział gruźlicy i chorób płuc, budynek główny.

74 Oględzinami objęto trzy poradnie: 1. Poradnia geriatryczna, 2. Poradnia gruźlicy i chorób płuc, 3. Poradnia onkologiczna.

75 Oględzinami objęto dwie funkcjonujące w Szpitalu rejestracje, tj. Rejestrację Centralną oraz Rejestrację do poradni kardiologicznej i geriatrycznej.

76 Tj. Oddział gruźlicy i chorób płuc.

77 Dotyczy Rejestracji Centralnej.

78 Ww. pielęgniarki oprócz dostępu do danych medycznych (w systemie InfoMedica) pacjentów w komórkach organizacyjnych, w których świadczyły pracę, posiadały również dostęp do danych pacjentów (obszarów – modułów w systemie InfoMedica) z innych oddziałów.

IV. Uwagi i wnioski

Wnioski

W związku ze stwierdzonymi nieprawidłowościami, a także działaniami podjętymi w toku kontroli w celu ich wyeliminowania, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK, przedstawia następujące wnioski:

1. Objęcie szkoleniami z zakresu ochrony danych osobowych wszystkich pracowników Szpitala uczestniczących w procesie przetwarzania danych osobowych.
2. Aktualizację obowiązującej w Szpitalu Polityki Bezpieczeństwa.
3. Wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających ochronę danych osobowych pacjentów oddziałów szpitalnych oraz minimalizację ryzyka ujawnienia informacji osobom postronnym w procesie rejestracji.
4. Nadawanie pracownikom uprawnień w systemach informatycznych oraz w systemach operacyjnych komputerów Szpitala w stopniu adekwatnym do realizowanych przez nich zadań, a także bezzwłoczne odbieranie uprawnień w systemach informatycznych byłym pracownikom Szpitala.
5. Przestrzeganie obowiązujących w Szpitalu wymogów dotyczących okresów ważności i jakości stosowanych haseł.
6. Nadanie wszystkim użytkownikom komputerów indywidualnych danych do autoryzacji w systemach operacyjnych oraz wprowadzenie rozwiązań uniemożliwiających pracę kilku osób na jednym koncie użytkownika.

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

Obowiązek poinformowania NIK o sposobie wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 30 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.

Zielona Góra, 19 kwietnia 2019 r.

Najwyższa Izba Kontroli
Delegatura w Zielonej Górze

Kontroler
Mariusz Kniat
Doradca prawny

p.o. Dyrektora
Włodzimierz Stobrawa

…….. podpis

…….. podpis