NAJWYŻSZA IZBA KONTROLI
Delegatura w Zielonej Górze

LZG. 410.002.03.2019

Ewa Nowak-Lewicka
Samodzielny Publiczny Szpital dla Nerwowo i
Psychicznie Chorych w Międzyrzeczu
ul. Poznańska 109
66-300 Międzyrzecz

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	Samodzielny Publiczny Szpital dla Nerwowo i Psychicznie Chorych w Międzyrzeczu ul. Poznańska 109, 66-300 Międzyrzecz (dalej: *Szpital*).
Kierownik jednostki kontrolowanej	Ewa Nowak-Lewicka – Dyrektor Szpitala od 1 października 2017 r. (akta kontroli: str. 3)
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[1]) do dnia zakończenia czynności kontrolnych[2].
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[3].
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Zielonej Górze
Kontroler	Sebastian Stępień, inspektor k.p., upoważnienie do kontroli nr LZG/29/2019 z dnia 1 lutego 2019 r. (akta kontroli: str. 1-2)

1 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*.

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

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

II. Ocena ogólna[4] 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.

Uzasadnienie oceny ogólnej

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 (dalej: *IOD*) osobę posiadającą odpowiednie przygotowanie i kwalifikacje zawodowe oraz zgłoszono ten fakt Prezesowi Urzędu Ochrony Danych Osobowych (dalej: *PUODO*).

Opracowany terminowo Rejestr czynności przetwarzania zawierał wszystkie wymagane elementy. Przeprowadzono także analizę procesów przetwarzania danych oraz ocenę skutków przetwarzania danych osobowych.

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 30% tych pracowników nie zapoznano z regulacjami dotyczącymi ochrony danych osobowych.

Wprowadzone rozwiązania organizacyjne, zmierzające do zapewnienia ochrony danych osobowych pacjentów, zasadniczo gwarantowały poszanowanie ich prywatności.

W szczególności prawidłowo chroniono i przetwarzano dane osobowe w skontrolowanych trzech Oddziałach szpitalnych, trzech poradniach specjalistycznych, a także – za wyjątkiem usytuowania dwóch okienek rejestracyjnych bezpośrednio obok siebie – w rejestracji ogólnej do poradni specjalistycznych.

Personelowi Szpitala zapewniono odpowiedni dostęp do danych medycznych. Wystąpiły jednak dwa przypadki pozostawienia zbyt szerokich uprawnień[5], a także odbierania ze znacznym opóźnieniem możliwości dostępu do tych systemów byłym pracownikom Szpitala.

Szpital zawierał umowy powierzenia przetwarzania danych w sytuacjach tego wymagających, a w pięciu analizowanych umowach zamieszczono postanowienia wymagane art. 28 RODO. Stwierdzono jednak dwa przypadki, w których pomimo działań Szpitala nie doszło – wskutek odmowy kontrahentów – do zawarcia umów, przy czym Szpital nie udostępniał tym podmiotom danych pacjentów.

Prawidłowo udostępniano uprawnionym podmiotom dokumentację medyczną pacjentów, jednak funkcjonujący w Szpitalu wykaz udostępniania tych danych był niezgodny z obowiązującymi wymogami.

Prawidłowo zastosowano fizyczne zabezpieczenia serwerowni Szpitala oraz pomieszczenia wykorzystywanego do przechowywania danych osobowych przetwarzanych w formie elektronicznej. 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[6] oraz możliwości instalowania dowolnego oprogramowania[7] – pełnej ochrony przetwarzanych na tych komputerach danych osobowych pacjentów.

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

---

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

[5] Dot. dwóch pielęgniarek, które zmieniły Oddziały na których świadczyły pracę, a nie zaktualizowano zakresu przyznanych im uprawnień do danych pacjentów.

[6] Stwierdzono w 19 z 30 badanych przypadków.

[7] Stwierdzono w 9 z 30 badanych przypadków.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[8] kontrolowanej działalności

OBSZAR

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

Opis stanu faktycznego

1.1. Zarządzeniem nr 45/2018 z dnia 4 czerwca 2018 r. Dyrektor Szpitala wyznaczyła IOD. Na to stanowisko powołany został pracownik Szpitala, pełniący dotychczas funkcję Administratora Bezpieczeństwa Informacji (dalej: *ABI*).

Stosownie do przepisu art. 38 ust. 3 RODO oraz ww. zarządzania Dyrektor Szpitala IOD podlegał bezpośrednio Dyrektorowi Szpitala. Zakres odpowiedzialności i uprawnień IOD[9] określony został w zakresie obowiązków pracownika z dnia 4 czerwca 2018 r. i zawierał wszystkie zadania określone w art. 39 RODO.

(akta kontroli: str. 4-7)

Dyrektor Szpitala (Administrator Danych Osobowych, dalej: *ADO*) upoważniła IOD do przetwarzania danych osobowych w systemach informatycznych i w zbiorach w wersji papierowej[10] oraz do nadawania upoważnień do przetwarzania danych osobowych pracownikom Szpitala oraz osobom wykonującym czynności na rzecz Szpitala na podstawie zawartych umów cywilnoprawnych[11].

(akta kontroli: str. 8-10)

W dniu 30 sierpnia 2018 r., zawiadomiono PUODO o wyznaczeniu IOD, a zawiadomienie zawierało elementy wymagane przepisem art. 10 ust. 1 i 3 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[12], tj.: imię, nazwisko, adres zamieszkania, adres poczty elektronicznej i numer telefonu inspektora.

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. 11-17)

Zgodnie z wymogami art. 37 ust. 5 RODO, IOD posiadał kwalifikacje zawodowe potwierdzające kompetencje do zajmowania tego stanowiska, tj. m.in.:

- Certyfikat Administratora Bezpieczeństwa Informacji z dnia 27 lutego 2014 r.,
- Certyfikat Administratora Bezpieczeństwa Informacji z dnia 19 stycznia 2015 r .,
- Certyfikat Administratora Bezpieczeństwa Informacji oraz Inspektora Ochrony Danych w związku z Rozporządzeniem UE z 2016 r. – ekspert stosowania przepisów RODO oraz zarządzania systemem ochrony danych osobowych z dnia 21 czerwca 2016 r.,
- Certyfikat Kompetencji Inspektora Ochrony Danych w związku z Rozporządzeniem UE z 2016 r. o Ochronie Danych Osobowych – ekspert stosowania przepisów RODO oraz zarządzania systemem ochrony danych osobowych z dnia 29 listopada 2017 r.

(akta kontroli: str. 18-21)

Szpital nie został dotychczas[13] uznany (nie otrzymał decyzji administracyjnej od właściwego organu do spraw cyberbezpieczeństwa) za operatora usługi kluczowej, o którym mowa w art. 5 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[14].

(akta kontroli: str. 22)

---

8 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.

9 Osoba ta pełni także funkcję Głównego specjalisty ds. kontroli zarządczej.

10 Upoważnienie nr 3/18 z dnia 25 maja 2018 r.

11 Upoważnienie Nr SPSNPCH-DK-0113-8/18 z dnia 4 czerwca 2018 r.

12 Dz. U. z 2018 r. poz. 1000, ze zm.

13 Według stanu na 31 marca 2019 r.

14 Dz. U. z 2018 r. poz. 1560.

1.2. W dniu wejścia w życie przepisów RODO (25 maja 2018 r.) w Szpitalu została przyjęta i zatwierdzona przez Dyrektora Szpitala, Polityka Bezpieczeństwa Danych Osobowych (dalej: *Polityka*), czym zrealizowano dyspozycję art. 24 ust. 1 i 2 RODO. Dokument ten został przekazany wg rozdzielnika wszystkim pracownikom Szpitala celem zapoznania z jego treścią.

(akta kontroli: str. 23-121)

W Polityce określono m.in. sposób postępowania, opis zadań, odpowiedzialność i uprawnienia ADO, IOD, Administratorów Systemów Informatycznych (dalej: *ASI*) oraz innych osób przetwarzających dane osobowe. Według postanowień Polityki za dokumentowanie oceny skutków (analiza ryzyka) dla ochrony danych osobowych odpowiedzialny jest ADO przy współudziale IOD.

W załączniku do Polityki zostały wykazane i zidentyfikowane wymagające zabezpieczenia dane osobowe w celu dokonania analizy ryzyka. W ramach analizy ryzyka ADO ma za zadanie zapewnić, aby dane osobowe były przetwarzane legalnie, adekwatnie w stosunku do celu przetwarzania, przez określony czas, wobec osób, w stosunku do których wykonano tzw. obowiązek informacyjny wraz ze wskazaniem ich praw. W Szpitalu opracowane zostały m.in. klauzule informacyjne oraz klauzule zgody dla pacjentów, pracowników, osób wykonujących umowy cywilnoprawne, darczyńców.

Zgodnie z Polityką, ADO odpowiada za nadawanie i anulowanie upoważnień do przetwarzania danych w zbiorach papierowych i systemach informatycznych, które dokonywane jest przez IOD. W celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych, IOD prowadzi ewidencję osób upoważnionych w formie elektronicznej.

(akta kontroli: str. 123-149)

W dniu 25 maja 2018 r. został przyjęty także Regulamin Ochrony Danych Osobowych (dalej: *Regulamin*), określający m.in. zasady bezpiecznego przetwarzania danych osobowych. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi winna także być przeszkolona i zapoznana z przepisami RODO. Za przeprowadzenie szkolenia odpowiada IOD. W Regulaminie zawarte są m.in.: zasady bezpiecznego użytkowania sprzętu IT, polityka haseł, zasady korzystania z nośników z danymi, zasady korzystania z Internetu i poczty elektronicznej, zasady ochrony antywirusowej. Szpital wywiązał się z opracowania kompletnej dokumentacji wymaganej regulacjami wewnętrznymi.

(akta kontroli: str. 84-91)

W okresie objętym kontrolą Szpital nie przeprowadzał aktualizacji Polityki, z uwagi na brak przesłanek uzasadniających taką zmianę.

IOD wyjaśniła, że termin aktualizacji tego dokumentu planowany jest w lipcu lub sierpniu br. Aktualizacja będzie dotyczyła doprecyzowania i rozszerzenia zapisów w nim zawartych w zależności od zidentyfikowanych potrzeb w tym zakresie.

(akta kontroli: str. 122)

1.3. Rejestr czynności przetwarzania danych osobowych (dalej: *Rejestr*), o którym mowa w art. 30 RODO, został sporządzony w dniu 25 maja 2018 r. (wersja I) i zaktualizowany w dniu 22 lutego 2019 r. (wersja II).

Rejestr stanowił kompleksową ewidencję wszystkich operacji realizowanych przez Szpital na danych osobowych. W odniesieniu do wskazanych 19 czynności przetwarzania zawartych w rejestrze, dokonano identyfikacji oraz analizy zagrożeń w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń.

Zgodnie z wymogami art. 30 ust. 3 RODO, Rejestr prowadzony był w formie pisemnej i elektronicznej oraz zawierał wymagane elementy określone w ust. 1 tego przepisu.

(akta kontroli: str. 150-246)

1.4. W dniu 3 września 2018 r. IOD przy udziale ASI opracował Analizę Ryzyka na 2018 r., w której określono m.in. procesy przetwarzania danych osobowych, jakie zachodzą

w Szpitalu, zdiagnozowano i opisano zagrożenia mogące pojawić się w związku z wystąpieniem incydentów oraz oceniono stopień zabezpieczenia w stosunku do stwierdzonych ryzyk. W szczególności są to ryzyka związane ze zniszczeniem danych lub nośników danych, ich modyfikacją, bądź ujawnieniem w wyniku nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych albo w inny sposób przetwarzanych.

Do oceny ryzyka wykorzystano metodykę opisaną w Polityce, w której przyjęto, że analiza ryzyka przeprowadzana jest dla kategorii osób lub dla danych procesów przetwarzania.

Dokonując analizy procesów związanych z przetwarzaniem danych osobowych przez Szpital określono ich liczbę, rodzaj, zidentyfikowano ryzyka (zagrożenia) związane z tymi procesami oraz określono poziom istotności. Z analizy ryzyka wynika, że nie zdiagnozowano ryzyk o wysokim stopniu zagrożenia i o dużym poziomie istotności.

(akta kontroli str. 247-255)

Na wypadek wystąpienia ryzyka opracowano procedury oraz wprowadzono stosowne zabezpieczenia np. opracowanie Procedury nadawania uprawnień do przetwarzania danych osobowych, Instrukcji zarządzania systemem informatycznym, Polityka haseł, Polityka kluczy, Polityka kontroli dostępu, opracowanie instrukcji określających sposób tworzenia i przechowywania kopii baz danych, zabezpieczający je przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą lub modyfikacją – jeżeli ryzyko wystąpienia takich zdarzeń zostało stwierdzone w ramach analizy.

1.5. W dniu 15 marca 2019 r. w Szpitalu został wykonany raport z oceny skutków przetwarzania dla ochronnych danych (dalej: *DPIA*), o której mowa w art. 35 RODO dla następujących procesów (czynności) przetwarzania danych:

- monitoringu wizyjnego,
- udostępniania dokumentacji medycznej pacjentów,
- realizacji zadań ustawowych i statutowych Szpitala związanych m.in. z profilaktyką zdrowotną, diagnozami medycznymi, leczeniem, zapewnieniem opieki zdrowotnej, zabezpieczeniem społecznym.

W dokumencie tym zawarto zapis, że ocena skutków jest procesem, w wyniku którego otrzymujemy odpowiedź m.in. na pytanie, czy przy przetwarzaniu danych osobowych występuje ryzyko naruszenia praw osób, których dane dotyczą. Przykładowe naruszenia to kradzież tożsamości, dyskryminacja, szkoda finansowa, szkoda wizerunkowa i naruszenie tajemnicy zawodowej. Ocena skutków przeprowadzona została na podstawie czynności przetwarzania zawartych w rejestrze czynności przetwarzania. Jest to proces ciągły i związany z analizą ryzyka czynności związanych z przetwarzaniem danych osobowych, które nie są katalogiem zamkniętym.

(akta kontroli str. 256-265)

1.6. Jednym z zadań IOD, w myśl art. 39 ust. 1 lit. b RODO, jest prowadzenie szkoleń personelu uczestniczącego w operacjach przetwarzania danych.

W Szpitalu został opracowany przez IOD jednolity plan szkolenia RODO 2018/2019. Z treści tego planu wynika, że pracownicy Szpitala są szkoleni w zakresie realizacji zadań w sposób uwzględniający wymogi RODO. Szkolenia osób zaangażowanych w proces przetwarzania informacji ujmowały m.in. następujące zagadnienia: zagrożenia bezpieczeństwa informacji, skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawną, stosowanie środków zapewniających bezpieczeństwo informacji. Nie prowadzono szkoleń w tym zakresie przed wejściem w życie przepisów tego rozporządzenia RODO.

(akta kontroli str. 266)

W okresie objętym kontrolą w szkoleniach (ogółem 16) prowadzonych przez IOD dla pracowników Szpitala uczestniczyło ogółem 316 spośród 441 – stan na dzień 25 lutego 2019 r. (tj. 72%) osób zatrudnionych w Szpitalu na umowę o pracę lub umowę cywilnoprawną uczestniczących w procesie przetwarzania danych osobowych. Zatem ok.

30% takich osób nie zostało objęte szkoleniami, co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości".

Szkoleniami zostali objęci m.in.: Dyrektor Szpitala, Zastępca Dyrektora ds. lecznictwa, lekarze kierujący Oddziałami, kierownicy komórek medycznych, pracownicy sekcji obsługi pacjentów i dokumentacji medycznej, pracownicy sekcji analizy, kontraktowania i rozliczeń, specjaliści wykonujący zawody medyczne, pielęgniarki, terapeuci, pracownicy administracji.

(akta kontroli str. 267-268)

1.7. Szpital nie zobowiązał się formalnie (np. poprzez deklarację stosowania) do przestrzegania regulacji zawartych w *Kodeksie postępowania dla sektora ochrony zdrowia*[15], dla którego wniosek o przyjęcie został 13 listopada 2018 r. przedłożony PUODO lub pozostałych opracowań związanych z ochroną danych osobowych, takich jak *Przewodnik po RODO w służbie zdrowia*[16] i *Wytyczne dotyczące inspektorów ochrony danych*[17].

IOD wyjaśniła, że *wprawdzie Szpital formalnie nie przyjął powyższych regulacji niemniej jednak kierujemy się wskazówkami zawartymi w Przewodniku po RODO dla służby zdrowia oraz zapisami, będącego w przygotowaniu, Medycznego Kodeksu Branżowego. Część postanowień zawartych w tych dokumentach znalazła swoje odbicie w Polityce Ochrony Danych Osobowych oraz Zarządzeniu Nr 55/2018 w sprawie wprowadzenia zasad dotyczących udzielania informacji o pobycie pacjenta w Szpitalu.*

(akta kontroli str. 269-271)

Stwierdzone nieprawidłowości

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

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 blisko 30 % pracowników Szpitala.

IOD wyjaśniła, że: *w okresie po wejściu w życie przepisów Rozporządzenia RODO do dnia 14 marca 2019 r. przeprowadzono 16 szkoleń personelu Szpitala w zakresie ochrony danych osobowych, w których uczestniczyło ponad 70% ogółu pracowników. Brak objęcia szkoleniami pozostałych pracowników wynikał przede wszystkim ze znacznej absencji chorobowej personelu w I kwartale bieżącego roku oraz wynikającymi z tego trudnościami w obsadzie dyżurów w komórkach organizacyjnych Szpitala. Ponadto pracownicy rozliczani są z wypracowanych nadgodzin w trzymiesięcznym okresie rozliczeniowym i do końca kwartału muszą je odebrać.*

(akta kontroli str. 441)

OCENA CZĄSTKOWA

Szpital terminowo wywiązał się z obowiązku opracowania i wdrożenia kompletnej dokumentacji oraz procedur dotyczących ochrony danych osobowych. Wywiązano się również z obowiązku powołania na stanowisko IOD osoby posiadającej odpowiednie przygotowanie i kwalifikacje zawodowe.

Opracowany terminowo Rejestr czynności przetwarzania zawierał wszystkie wymagane elementy. Przeprowadzono także analizę procesów przetwarzania danych oraz ocenę skutków przetwarzania danych osobowych.

Nie w pełni zrealizowano obowiązek przeszkolenia pracowników Szpitala uczestniczących w procesie przetwarzania danych osobowych z zagadnień dotyczących bezpieczeństwa danych oraz obowiązywania przepisów RODO, gdyż blisko 30% tych pracowników nie zostało objętych takimi szkoleniami.

[15] Treść kodeksu została opublikowana na stronie internetowej: www.rodowzdrowiu.pl.
[16] Opublikowany 24 września 2018 r. na stronie internetowej Ministerstwa Cyfryzacji.
[17] Opublikowane 10 maja 2018 r. na stronie internetowej Urzędu Ochrony Danych Osobowych.

OBSZAR

2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych

Opis stanu faktycznego

2.1. Przeprowadzone oględziny Rejestracji Ogólnej do Poradni Specjalistycznych w Szpitalu (w Szpitalu funkcjonuje jedna rejestracja) wykazały, że w celu właściwej ochrony danych osobowych pacjentów funkcjonowały poniżej wymienione rozwiązania:

- rejestrowanie pacjentów odbywało się w dwóch czynnych okienkach,
- identyfikacja pacjentów odbywała się na podstawie okazanych rejestratorce dowodów tożsamości wg kolejności przyjścia do rejestracji. Pacjenci znani rejestratorkom, którzy już wcześniej zgłaszali się do poradni nie musieli okazywać dowodu osobistego,
- dwa komputery znajdujące się w rejestracji były ustawione w sposób uniemożliwiający wgląd w treści na nich wyświetlane osobom rejestrującym się,
- okienka znajdowały się bezpośrednio obok siebie. Brak przesłon między okienkami mógł powodować, że osoba znajdująca się przy okienku słyszała informacje podawane przez osobę rejestrującą się przy drugim stanowisku. Jednakże ich usytuowanie uniemożliwiało wgląd w dokumenty osoby z sąsiedniego okienka. Powyższe ustalenie wraz z wyjaśnieniem szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości",
- na podłodze narysowana była linia, poza którą powinni znajdować się pacjenci czekający na możliwość rejestracji. W toku oględzin nie stwierdzono przypadków przekraczania tej linii przez pacjentów;
- na korytarzu, gdzie pacjenci oczekiwali na wizytę znajdowały się m.in. informacje na temat Polityki Jakości przyjętej w Szpitalu, zasad przetwarzania danych osobowych, praw pacjenta, trybu składania skarg i wniosków, sposobu stosowania monitoringu wizyjnego,
- dokumenty w rejestracji były przechowywana w szafkach zamykanych na klucz. Na koniec pracy klucze zanoszone były do zamykanej szafki na klucze,
- dokumenty osób wcześniej zarejestrowanych na dany dzień przenoszone były rano do gabinetu lekarskiego. Gabinet ten był zamknięty do czasu przyjścia lekarza. W przypadku rejestracji w dniu, w którym możliwa jest wizyta w poradni, dokumenty po zarejestrowaniu pacjenta na bieżąco były zanoszone przez rejestratorkę do gabinetu lekarza,
- osoby rejestrujące nie wypowiadały na głos informacji zawierających dane osobowe, przekazując jedynie dane dotyczące dalszego procesu postępowania po zarejestrowaniu się do danego lekarza,
- pacjenci w chwili rejestracji otrzymywali karteczki, na których sami wypisywali datę i godzinę wizyty oraz kolejny numerek do danego lekarza,
- w pomieszczeniu rejestracji nie znajdował się monitoring wizyjny.

(akta kontroli str. 272-276)

Przeprowadzone oględziny dyżurek pielęgniarskich, sal chorych oraz gabinetów lekarskich na trzech Oddziałach szpitalnych[18] wykazały m.in., że:

- w żadnym z Oddziałów na łóżkach nie zamieszczono kart pacjentów,
- ruch chorych[19] prowadzony był w dyżurkach pielęgniarskich w miejscu niewidocznym dla osób postronnych - listy z danymi pacjentów (imię i nazwisko), numerami sal, w których przebywają oraz innymi informacjami związanymi z ich

[18] Tj. Całodobowy Oddział Psychiatryczny Ogólny nr 2, Całodobowy Oddział Leczenia Alkoholowych Zespołów Abstynencyjnych nr 13, Całodobowy Oddział Rehabilitacji Psychiatrycznej nr 14.

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

pobytem na Oddziałach umiejscowione są na zakrytej tablicy na ścianie (1 dyżurka) lub w segregatorach w szafkach (2 dyżurki),

- podręczna dokumentacja pielęgniarska przechowywana była w drewnianych szafkach posiadających możliwość zamknięcia na klucz,
- w gabinetach lekarskich dokumentacja medyczna pacjentów była przechowywana w szafkach biurek zamykanych na klucz,
- nie stwierdzono nieprawidłowości w zakresie sposobu użytkowania i zabezpieczenia komputerów w dyżurkach i gabinetach[20],
- ani pielęgniarki, ani lekarze nie opuszczali zajmowanych pomieszczeń pozostawiając je otwarte,
- pacjenci nie nosili opasek na nadgarstku, co było zgodne z przepisem art. 36 ust. 4 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej [21].

(akta kontroli str. 277-281)

Naczelna Pielęgniarka Szpitala wyjaśniła że: (…) *jako Szpital o profilu psychiatrycznym jesteśmy zwolnieni z obowiązku noszenia przez pacjentów identyfikatorów. Pacjent, który zgłasza się do Izby Przyjęć sam lub z opiekunem prawnym weryfikowany jest na podstawie dowodu osobistego, bądź innego dokumentu potwierdzającego tożsamość. W momencie przyjęcia do Szpitala, zakładana jest podstawowa dokumentacja medyczna dla danego pacjenta. Po zbadaniu przez lekarza dyżurnego pacjent w obecności ratownika bądź osoby wezwanej z konkretnego Oddziału, na który jest kierowany, udaje się na właściwy Oddział celem podjęcia leczenia. Na Oddziale pacjent jest wpisywany do ruchu chorych. W momencie zdawania dyżuru, pielęgniarka zdająca idzie z segregatorem na konkretną salę z pielęgniarką przyjmującą dyżur, gdzie przekazuje ustnie informację o przyjęciu nowego pacjenta wskazując tę osobę oraz jego łóżko. Z uwagi na to, iż leczenie pacjentów jest długotrwałe i nie dochodzi do kumulacji w ich przyjmowaniu i wypisywaniu, personel nie ma problemu z zapamiętaniem, kto aktualnie przebywa na Oddziale i jakie łóżko zajmuje*.

(akta kontroli str. 282-283)

We wszystkich trzech objętych oględzinami gabinetach poradni specjalistycznych Szpitala[22] ustalono, że dokumentację pacjentów przechowywano we właściwy sposób, tj. karty pacjentów zawierające ich dokumentację medyczną, znajdowały się w szafkach biurek mających możliwość zamknięcia na klucz. Pacjent przebywający w gabinecie nie miał możliwości zapoznania się z danymi innych osób oczekujących w kolejce lub tych, którzy odbyli już wizytę. Ustalono ponadto, że pacjenci wchodzili do gabinetów poradni bez wezwania lekarza wg kolejnych numerków. Ponadto w trakcie oględzin, nie stwierdzono, aby którykolwiek gabinet został pozostawiony bez opieki oraz nie ujawniono przypadków pozostawienia klucza w drzwiach i opuszczenia przez personel gabinetu poradni.

(akta kontroli str. 284-285)

Ponadto dokonano oględzin monitoringu wizyjnego, pod kątem miejsc, w których zamontowane są kamery, co jest przedmiotem monitoringu, jak długo przechowywane są nagrania z kamer i kto ma do nich dostęp.

(akta kontroli str. 286-288)

Zarządzeniem nr 69/2018 z dnia 24 września 2018 r. Dyrektor Szpitala wprowadził Regulamin Monitoringu Wizyjnego CCTV w Szpitalu. Ww. Zarządzenie przekazano pracownikom Szpitala (wg rozdzielnika) celem stosowania się do jego postanowień.

(akta kontroli str. 289-313)

---

[20] W toku oględzin komputery były wyłączone.

[21] Dz. U. z 2018 r. poz. 2190, ze zm.

[22] Oględzinami objęto trzy poradnie: Poradnię Zdrowia Psychicznego, Poradnię Leczenia Uzależnień oraz Poradnię Neurologiczną.

W Szpitalu zamontowany był monitoring wizyjny w 8 pawilonach. Składa się na niego 111 kamer. Obejmowały one wejścia do budynków, korytarze oraz pomieszczenia wspólne (poczekalnie, świetlice, stołówki). Najwięcej kamer umieszczonych było w budynku Nr 19 - Całodobowy Oddział Psychiatrii Sądowej o Wzmocnionym Zabezpieczeniu dla Młodzieży – 74 kamery, które znajdowały się m.in. na zewnątrz, na korytarzach, w pomieszczeniach wspólnych, w salach lekcyjnych i gabinetach.

ADO ma dostęp[23] do nagrań z wszystkich kamer w zakresie podglądu, odtwarzania i nagrywania. W poszczególnych budynkach dostęp do kamer ma dyżurujący personel Szpitala.

2.2. Według stanu na dzień 25 lutego 2019 r. personel administracyjny Szpitala liczył 27 osób. Analiza uprawnień w systemie ESKULAP[24], jakie zostały nadane wszystkim osobom z tej grupy wykazała, że odpowiadały one zakresom zadań i obowiązków realizowanych przez tych pracowników, i tak:

- 24 osoby nie posiadały dostępu do systemu ESKULAP, co wynikało z ich zakresów obowiązków (nie realizowali oni zadań wymagających dostępu do danych medycznych pacjentów Szpitala),
- dwie osoby[25] posiadły nadane uprawnienia do wszystkich modułów 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,
- jedna osoba posiadła ograniczony dostęp do danych w systemie ESKULAP (tylko do danych statystycznych)[26].

(akta kontroli str. 314-315)

2.3. Analiza przeprowadzona na próbie 30 (ze 160) pielęgniarek[27] zatrudnionych w Szpitalu[28] wykazała m.in., że:

- 17 pielęgniarek posiadało dostęp w systemie ESKULAP do danych medycznych pacjentów, a także pisemne upoważnienia do przetwarzania danych osobowych, przy czym 15 z nich w komórkach organizacyjnych (Oddziały, izba przyjęć), na których faktycznie świadczyły pracę, a dwie posiadały uprawnienia do danych pacjentów z Oddziałów, w których pracowały wcześniej[29] (uprawnienia zostały cofnięte i zaktualizowane dopiero w toku kontroli), co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości";
- 13 pielęgniarek nie posiadało dostępu do systemu ESKULAP.

(akta kontroli str. 316-318)

Ustalono, że żadnej z osób zatrudnionych na umowę o pracę lub wykonujących na podstawie umów cywilnoprawnych[30] zadania sanitariusza, salowej lub sprzątaczki nie nadano uprawnień w systemie ESKULAP do przetwarzania danych osobowych pacjentów oraz nie wydano upoważnień do przetwarzania danych osobowych, co było działaniem prawidłowym.

(akta kontroli str. 123-145)

2.4. W okresie od 25 maja 2018 r. do 11 marca 2019 r. Szpital rozwiązał stosunek pracy/umowę cywilnoprawną z 65 osobami. Spośród nich osiem osób miało przyznany

---

23 Nagrania przechowywano od 2 do 10 dni w zależności od rodzaju rejestratora.

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

25 Administratorzy Systemów Informatycznych (informatycy Szpitala).

26 Główny Specjalista ds. Kontraktowania i Monitorowania Rozliczeń.

27 Szpital nie zatrudniał położnych.

28 Na umowę o pracę oraz umowy cywilnoprawne (zlecenie) - stan na 25 lutego 2019 r.

29 Pierwsza z nich zmieniła Oddział w dniu 19 kwietnia 2015 r., a druga w dniu 31 grudnia 2015 r.

30 Ogółem 51 osób - stan na 25 lutego 2019 r.

dostęp do systemu ESKULAP, w tym jedna zatrudniona na umowę cywilnoprawną i siedem na umowę o pracę.

Analiza terminów cofania uprawnień ww. osobom wykazała, że w trzech przypadkach cofnięcie uprawnień nastąpiło w terminie do 10 dni od rozwiązania stosunku pracy/umowy zlecenia, natomiast w pozostałych pięciu przypadkach od 169 do 268 dni od zwolnienia, co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str. 319-320)

2.5. W okresie objętym kontrolą Szpital miał zawarte umowy dotyczące świadczenia usług serwisu oprogramowania oraz pomocy technicznej tzw. help desk. W dokumentacji wewnętrznej uregulowano kwestie zgłaszania ewentualnych problemów z działaniem wdrażanych rozwiązań dla dostawcy oprogramowania lub urządzeń w Polityce.

W przypadku systemu ESKULAP kontakt z help desk odbywał się za pomocą specjalnego narzędzia (np. moduł oprogramowania), natomiast jeżeli chodzi o system FINUS - e-mailowo.

Szpital posiada informacje dotyczące wywiązania się przez dostawcę oprogramowania ESKULAP z obowiązku przeprowadzenia testów akceptacyjnych.

W okresie od 25 maja 2018 r. do 28 lutego 2019 r. wysłanych zostało 16 zgłoszeń help-desk do firmy, która jest przedstawicielem producenta systemu informatycznego Szpitala tj., ESKULAP. Badaniem objęto wszystkie zgłoszenia. Dotyczyły one m.in. następujących tematów:

- automatyzacja wpisów dot. statusu ubezpieczenia pacjenta w EWUŚ,
- błędów aktualizacji systemu,
- prośba o stworzenie raportu niewysłanych świadczeń do NFZ, raportu zastosowania przymusu bezpośredniego, raportu z listą przyjęć bez zgody, raportów danych statystycznych MZ-15, MZ-19 do Ministerstwa Zdrowia, raportu dla umowy Centrum Zdrowia Psychicznego, raport rozliczonych świadczeń na potrzeby pilotażu CZP,
- instalacja usługi KOWAL (weryfikacja autentyczności leków),
- konfiguracji umowy na pilotaż CZP,
- problem ze współczynnikiem Ambulatoryjnej Opieki Specjalistycznej dla świadczeń pierwszorazowych,
- błędy eksportu w formacie fakturowania,
- aktualizacja modułu Ruch Chorych, błędy podczas aktualizacji tego modułu,
- aktualizacja modułu e-rejestracja.

Ponadto w powyższym okresie wysłano 3 zgłoszenia mailowe związane z oprogramowaniem administracyjnym Szpitala - FINUS. Dotyczyły one następujących tematów:

- brak na wydruku umowy o pracę zapisu dot. warunku wygaśnięcia umowy,
- usuwanie pozycji Bilansu Otwarcia z rozrachunków na kontrahentach,
- danych osoby materialnie odpowiedzialnej na wydrukach Magazyn Wyda.

W żadnym z tych zgłoszeń nie stwierdzono przypadków przekazania danych osobowych lub danych medycznych pacjentów podmiotowi świadczącemu usługi serwisu oprogramowania lub pomocy technicznej.

(akta kontroli str. 321-340)

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.

(akta kontroli str. 341-353)

Ustalono, że umowy dotyczące powierzenia przetwarzania danych zawierano z podmiotami (wykonawcami) realizującymi na rzecz Szpitala zadania związane m.in. z wykonywaniem

badań laboratoryjnych i diagnostycznych, świadczeniem usług informatycznych oraz opieki serwisowej, obsługą prawną, świadczeniem usług hostingowych i brokerskich.

Analiza pięciu umów (porozumień) 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,
- 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,
- umowy te zawierane były na wzorze opracowanym przez Szpital i wysyłanym do Zleceniobiorców w celu podpisania zawartych w nim ustaleń lub na zaproponowanym przez Zleceniobiorcę propozycji umowy.

(akta kontroli str. 354-378)

Ustalono, że w dwóch przypadkach Szpital zawarł i realizuje umowy główne jako Administrator, a nie zostały zawarte umowy powierzenia przetwarzania danych osobowych. Jako przyczynę tego stanu rzeczy wskazano odmowę zawarcia takiej umowy przez podmioty przetwarzające. Powyższe ustalenie wraz z wyjaśnieniem szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str. 379-381,442,443)

Według stanu na 25 lutego 2019 r. usługi na rzecz Szpitala świadczyło na podstawie kontraktów 27 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.

IOD wyjaśniła, że z *lekarzami zatrudnionymi na kontrakcie nie są zawierane umowy powierzenia przetwarzania danych osobowych, ponieważ nie są oni zobowiązani do samodzielnego prowadzenia dokumentacji medycznej. Prowadzą oni tę dokumentację w imieniu Szpitala. Osoby takie podpisują oświadczenie poufności oraz uzyskują upoważnienie do przetwarzania danych osobowych nadane przez ADO. Osoby te są szkolone w zakresie ochrony danych osobowych. W zakresie przestrzegania ochrony danych osobowych traktowani są jak pracownicy Szpitala.*

(akta kontroli str. 382)

2.7. W funkcjonującej w Szpitalu Polityce zawarto m.in. Instrukcję postępowania z incydentami. 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 ich dokumentowania i zgłaszania.

Analiza postanowień Polityki wykazała ponadto, że:

- wprowadzono obowiązek 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),
- jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych wprowadzono obowiązek zawiadamiania osoby, której dane dotyczą, o takim naruszeniu (art. 34 ust. 1 RODO).

W dniu 15 marca 2019 r. w Szpitalu odnotowano jeden przypadek (incydent) naruszenia bezpieczeństwa danych osobowych. Naruszenie polegało na dokonaniu przez pracownika Szpitala przywłaszczenia dokumentacji medycznej pacjenta i wyniesienia jej poza obszar

Szpitala do domu, o czym w wymaganym terminie powiadomiono PUODO (tj. w dniu 18 marca 2019 r.).

(akta kontroli str. 383-395)

2.8. W Szpitalu została opracowana Instrukcja przechowywania i wydawania dokumentacji medycznej (dalej: *Instrukcja*). W myśl tych regulacji oraz zgodnie z przepisem art. 26 ust. 1 oraz 3 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta[31] (dalej: *u.o.p.p.*), dokumentację medyczną udostępnia się pacjentowi lub jego przedstawicielowi ustawowemu, bądź osobie upoważnionej przez pacjenta oraz podmiotom określonym w ust. 3 ww. przepisu. Opracowano także wzór wniosku o wypożyczenie historii choroby (wykorzystywany w wydawania dokumentacji wewnątrz Szpitala z archiwum zakładu) oraz wzór wniosku o sporządzenie kserokopii dokumentacji medycznej (wykorzystywany do udostępnienia dokumentacji osobom zewnętrznym).

(akta kontroli str. 396-401)

Prowadzony w Szpitalu wykaz dotyczący udostępniania dokumentacji medycznej (*Rejestr wydanych akt*) nie zwierał wszystkich wymaganych przepisem art. 27 ust. 4 u.o.p.p. elementów (tj. informacji o sposobie udostępnienia dokumentacji medycznej, zakresie udostępnionej dokumentacji medycznej, imienia (imion) i nazwiska oraz podpisu osoby, która udostępniła dokumentację medyczną, a także daty udostępnienia dokumentacji medycznej), co szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str. 402-403)

W okresie od 25 maja 2018 r. do 19 lutego 2019 r. do Szpitala wpłynęło ogółem 65 wniosków o udostępnienie dokumentów medycznych pacjentów, przy czym:

- 58 wniosków instytucji publicznych takich jak: Sądy, Prokuratura oraz ZUS,
- w czterech przypadkach były to prośby pacjentów,
- w jednym przypadku z wnioskiem zwróciła się firma ubezpieczeniowa,
- w jednym przypadku z wnioskiem zwróciła się Kancelaria Adwokacka,
- w jednym przypadku z wnioskiem zwrócił się Urząd Miejski w Wałbrzychu.

(akta kontroli str. 404-407)

Dokumenty zostały udostępnione w 63 przypadkach. W dwóch przypadkach odmówiono udostępnienia dokumentacji, tj. Kancelarii Adwokackiej[32] oraz Urzędowi Miejskiemu[33].

(akta kontroli str. 408-411)

Analiza prawidłowości udostępnienia dokumentacji w odniesieniu do komercyjnej instytucji ubezpieczeniowej wykazała, że:

- kserokopie dokumentacji medycznej przesyłano pocztą za zwrotnym potwierdzenie odbioru,
- firma ubezpieczeniowa, posiadała upoważnienie pacjentki do dostępu do jej dokumentacji medycznej.

(akta kontroli str.412-418)

2.9. W Szpitalu zostały wprowadzone procedury określające działania, jakie powinny zostać podjęte w celu ograniczenia ryzyka utraty danych, zasady postępowania w przypadku wystąpienia awarii, błędów lub nieuprawnionej modyfikacji danych. Regulacje dotyczące ochrony danych przed ich utratą w wyniku awarii, błędów lub nieuprawnionej modyfikacji zostały opisane w Polityce:

---

31 Dz. U. z 2017 r. poz. 1318, ze zm.

32 Powodem odmowy było podanie niewystarczających danych osobowych do identyfikacji pacjenta (podano jedynie imię i nazwisko, a w Szpitalu było kilku pacjentów o takich samych danych).

33 Wnioskodawca nie wykazał przesłanek uzasadniających udostępnienie dokumentacji medycznej.

- załącznik nr 4 – Regulamin Ochrony Danych Osobowych,
- załącznik nr 8 – Plan Ciągłości Działania,
- załącznik nr 10 – Instrukcja zarządzania systemami informatycznymi RODO.

W dokumentach tych określono m.in.:

- zasady bezpiecznego użytkowania sprzętu IT,
- procedurę rozpoczęcia, zawieszenia i zakończenia pracy,
- zasady wynoszenia nośników z danymi poza organizację,
- zasady korzystania z internetu,
- zasady korzystania z poczty elektronicznej,
- zasady użytkowania komputerów przenośnych.

(akta kontroli str. 84-91,98-99,101-109)

Ustanowione w Szpitalu procedury wewnętrzne mają na celu m.in. minimalizację ryzyka utraty danych osobowych pacjentów w wyniku awarii, błędów lub nieuprawnionej modyfikacji. Sposób zabezpieczenia pomieszczeń w których przechowywane są istotne dane osobowe pacjentów i ich wyposażenie wskazuje, że w Szpitalu podejmowane są działania mające na celu zapewnić ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także zabezpieczenia przetwarzanych informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie.

W toku kontroli dokonano oględzin serwerowni oraz pomieszczenia wykorzystywanego do przechowywania kopii zapasowych baz danych Szpitala. W wyniku oględzin ustalono m.in., że:

- serwerownia umiejscowiona była w osobnym budynku znajdującym się w centralnej części Szpitala, na drzwiach serwerowni nie stwierdzono oznaczeń informujących o jej przeznaczeniu,
- pomieszczenie serwerowni wyposażone było w: gaśnice, system klimatyzacji, czujki ruchu, dymu i temperatury, układ podtrzymywania napięcia UPS, podłogę techniczną dzięki której urządzenia znajdują się powyżej poziomu posadzki. Znajduje się w nim kamera monitoringu wizyjnego, a działające w serwerowni urządzenia informatyczne zamontowane były w szafach typu RACK,
- pomieszczenie w którym przechowywane są kopie baz danych umiejscowione jest na parterze budynku administracji Szpitala, obok pomieszczenia, w którym pracują informatycy,
- na drzwiach nie stwierdzono oznaczeń informujących o jego przeznaczeniu,
- pomieszczenie wyposażone było w układ podtrzymywania napięcia UPS, nie było objęte systemem monitoringu wizyjnego,
- działające w pomieszczeniu urządzenie informatyczne zamontowane było w szafie typu RACK,
- nie stwierdzono mechanicznych uszkodzeń na kablowaniu lub urządzeniach podłączonych do infrastruktury informatycznej Szpitala, nie było widocznych rur mogących stanowić potencjalne zagrożenie zalaniem.

(akta kontroli str. 419-425)

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

- na 26 komputerach zainstalowany był system operacyjny Windows XP oraz Windows Vista, dla których producent oprogramowania zakończył wsparcie techniczne odpowiednio 8 kwietnia 2014 r. i 11 kwietnia 2017 r. Po tych dniach producent przestał dostarczać aktualizacje zabezpieczeń, poprawki niezwiązane 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,

- we wszystkich 30 komputerach porty USB nie zostały zabezpieczone przed możliwością podłączenia do nich nośników pamięci,
- w 17 przypadkach hasło do systemu operacyjnego Windows było niezgodne z zasadami przyjętymi w Polityce Szpitala (zbyt mała ilość znaków lub niewystarczający rodzaj znaków np. brak cyfry),
- w jednym przypadku system nie wymagał podania hasła do systemu operacyjnego Windows, a jedynie login użytkownika,
- w jednym przypadku pracownik korzystał z nie przypisanego mu loginu i hasła do systemu operacyjnego Windows,
- w dziewięciu przypadkach użytkownicy mieli uprawnienia administratora do systemu komputerowego, tym samym posiadali oni możliwość instalacji dowolnego oprogramowania jako administrator,
- we wszystkich 30 komputerach zainstalowany był program antywirusowy ESET ENDPOINT ANTYVIRUS, aktualny na dzień przeprowadzenia oględzin.

Powyższe ustalenie wraz z wyjaśnieniem szerzej opisano w dalszej części wystąpienia, w sekcji „Stwierdzone nieprawidłowości".

(akta kontroli str. 426-428)

W Szpitalu funkcjonuje system informatyczny do obsługi medycznej ESKULAP („część biała") oraz oprogramowanie administracyjne FINUS („część szara"). Dane z bazy ESKUAP tworzone są 2 razy dziennie o godz. 6:00 i godz. 16:00, natomiast z bazy FINUS raz dziennie o godz. 23:00. Jest to proces zautomatyzowany. Kopie bezpieczeństwa baz danych przechowywane są na serwerach w serwerowni (odrębnie dla bazy ESKULAP i dla bazy FINUS). Dodatkowo kopie obu baz przechowywane są na serwerze plików w serwerowni zapasowej, która znajduje się na terenie budynku Administracji Szpitala.

Pracownicy Szpitala wykorzystują 8 komputerów przenośnych, nie są one jednak używane poza terenem Szpitala, w związku z tym nie stosuje się ochrony kryptograficznej nośników pamięci, ani pseudonimizacji danych osobowych na tym sprzęcie.

Z wyjaśnień udzielonych przez ASI wynika, że (…) *planowane jest podjęcie sprawdzeń poprawności wykonania kopii bezpieczeństwa baz danych z częstotliwością raz na kwartał. Ponadto, w jednym z projektów unijnych przewidziane są rozwiązania pozwalające na podniesienie poziomu bezpieczeństwa w zakresie pamięci przenośnych (blokowanie portów USB, białe i czarne listy USB, szyfrowanie) stosowanie ochrony kryptograficznej nośników pamięci lub pseudonimizacji danych osobowych.*

(akta kontroli str. 429-430)

Stwierdzone nieprawidłowości

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

1. W przypadku rejestracji, usytuowanie dwóch okienek 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.

   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.

Z wyjaśnień Dyrektora Szpitala wynika, że *obecnie nie ma możliwości technicznych, aby oddzielić od siebie okienka rejestracji. Brana jest natomiast pod uwagę możliwość wyłączenia jednego z okienek z obsługi i wówczas pacjenci będą obsługiwani tylko przy jednym okienku.*

(akta kontroli str. 432)

2. W dwóch przypadkach stwierdzono, że pielęgniarki posiadały uprawnienia do danych pacjentów z Oddziałów, w których pracowały wcześniej i na których nie wykonują obecnie obowiązków (uprawnienia te zostały im cofnięte i zaktualizowane dopiero w toku kontroli NIK). Ponadto w przypadku pięciu byłych pracowników cofnięcie uprawnień do danych pacjentów w systemie informatycznym nastąpiło dopiero od 169 do 268 dni od daty rozwiązania stosunku pracy.

   Stanowiło to naruszenie § 20 ust. 2 pkt 5 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[34] (dalej: *rozporządzenie KRI*), zgodnie z którym należy podejmować działania polegające na bezzwłocznej zmianie uprawnień, w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji.

ASI wyjaśnił, że (…) *brak zmiany uprawnień wynikało z przeoczenia. Z kolei tak późne zablokowanie dostępu byłych pracowników do będących w posiadaniu Szpitala systemu ESKULAP związane było z tym, że wcześniej zablokowano tym osobom możliwość logowania się do poszczególnych jednostek tego systemu, co i tak uniemożliwiało pracę w tym systemie, natomiast przez nieuwagę nie zablokowano im konta w tym systemie.*

(akta kontroli str. 433-434)

3. W dwóch przypadkach[35] Szpital zawarł i realizuje umowy główne jako Administrator, a nie zostały zawarte umowy powierzenia przetwarzania danych osobowych (odmowa zawarcia takiej umowy przez podmioty przetwarzające), co stanowiło naruszenie przepisu art. 28 RODO.

Dyrektor Szpitala wyjaśniła, że (…) *w przypadku pierwszej firmy, pomimo zawarcia umowy, której przedmiotem były badania diagnostyczne w zakresie Tomografu Komputerowego i Rezonansu Magnetycznego Szpital nigdy nie korzystał z jej usług. Po wejściu w życie przepisów RODO Szpital zwrócił się do niej z prośbą o zawarcie umowy powierzenia. Spółka odmówiła zawarcia umowy na formularzu przygotowanym przez Szpital uzasadniając, iż jako duża korporacja przygotuje własny wzór umowy, który zostanie przesłany do wszystkich kontrahentów. W związku z powyższym do chwili podpisania umowy powierzenia Szpital nie zleca badań Spółce. W przypadku drugiego podmiotu Szpital planuje podjęcie dalszych kroków w celu zawarcia umowy powierzenia.*

(akta kontroli str.435-436)

4. Wbrew wymogom określonym w przepisie art. 27 ust. 4 pkt 2, 3, 5 i 6 u.o.p.p. prowadzony w Szpitalu wykaz dotyczący udostępniania dokumentacji medycznej (*Rejestr wydanych akt*) nie zawierał informacji o sposobie udostępnienia dokumentacji medycznej, zakresie udostępnionej dokumentacji medycznej, imienia (imion) i nazwiska oraz podpisu osoby, która udostępniła dokumentację medyczną, a także daty udostępnienia dokumentacji medycznej.

---

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

[35] Dotyczy: 1) umowy nr 4/2009 z dnia 31 grudnia 2008 r. dotyczącej udzielania świadczeń zdrowotnych z zakresu wykonywania badań diagnostycznych w Pracowni Tomografii Komputerowej, 2) umowy nr 1/2018 z dnia 26 kwietnia 2018 r. w zakresie udzielania świadczeń zdrowotnych z zakresu wysokospecjalistycznych badań diagnostycznych w zakresie Tomografii Komputerowej (TK) i Rezonansu Magnetycznego (RM).

Starszy statystyk medyczny w Sekcji Obsługi Pacjentów i Dokumentacji Medycznej oświadczyła, że *od lipca br. planowana jest zmiana Rejestru tak, aby spełniał ustawowe wymogi, co do elementów jakie powinien zawierać.*

(akta kontroli str. 404)

5. Sposób użytkowania i zabezpieczenia wykorzystywanych w Szpitalu komputerów stacjonarnych (badaniami objęto 30 komputerów) nie gwarantował pełnej ochrony danych osobowych pacjentów, gdyż:

a) w przypadku 17 komputerów hasło do systemu operacyjnego Windows było niezgodne z zasadami przyjętymi w Polityce Szpitala (zbyt mała ilość znaków lub niewystarczający rodzaj znaków np. brak cyfry), w jednym przypadku system nie wymagał podania hasła, a jedynie login użytkownika (pracownik ten nie miał uprawnień admina), a w kolejnym przypadku pracownik korzystał z nieprzypisanego mu loginu i hasła;

b) w dziewięciu przypadkach użytkownicy mieli uprawnienia administratora do systemu komputerowego, tym samym posiadali oni możliwość instalacji dowolnego oprogramowania jako administrator,

W myśl przepisu § 20 ust. 2 pkt 7 i 9 rozporządzenia KRI, kierownictwo podmiotu publicznego jest obowiązane do podejmowania działań zapewniających ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także zabezpieczenia przetwarzanych informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie. Dodatkowo, zgodnie z przepisem § 20 ust. 2 pkt 12 ww. rozporządzenia, zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych polega w szczególności na dbałości o aktualizację oprogramowania, minimalizowaniu ryzyka utraty informacji w wyniku awarii oraz ochronie przed błędami, utratą, nieuprawnioną modyfikacją. W myśl art. 5 ust. 1 lit. f RODO, dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

ASI wyjaśnił, że:

ad a) (…) *jeszcze w toku kontroli podjęte zostały działania, które pozwoliły na usunięcie powyższych nieprawidłowości. Aktualnie wszystkie hasła spełniają wymogi Polityki co do ilości i rodzaju znaków. W przypadku jednego z pracowników zmieniono ustawienia jego konta w ten sposób, że obecnie do zalogowania wymagany jest zarówno login jak i hasło, w przypadku kolejnej osoby został jej założony login, do którego przypisała hasło.*

ad b) (…) *wynikało to z niedoskonałości oprogramowania, które do pełnej funkcjonalności wymaga uprawnień administratora na danym komputerze.*

(akta kontroli str. 437-440)

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 prawidłowo chroniono i przetwarzano dane osobowe w skontrolowanych trzech Oddziałach szpitalnych, trzech poradniach specjalistycznych, a także – za wyjątkiem usytuowanie dwóch okienek rejestracyjnych bezpośrednio obok siebie – w rejestracji ogólnej do poradni specjalistycznych.

Personelowi Szpitala zapewniono odpowiedni dostęp do danych medycznych. Wystąpiły jednak dwa przypadki pozostawienia zbyt szerokich uprawnień[36], a także odbierania ze znacznym opóźnieniem możliwości dostępu do tych systemów byłym pracownikom Szpitala.

[36] Dot. dwóch pielęgniarek, które zmieniły Oddziały, na których świadczyły pracę.

Szpital zawierał umowy powierzenia przetwarzania danych w sytuacjach tego wymagających, a w pięciu analizowanych umowach zamieszczono postanowienia wymagane art. 28 RODO. Stwierdzono jednak dwa przypadki, w których pomimo działań Szpitala nie doszło – wskutek odmowy kontrahentów – do zawarcia umów, przy czym Szpital nie udostępniał tym podmiotom danych pacjentów.

Prawidłowo udostępniano uprawnionym podmiotom dokumentację medyczną pacjentów, jednak funkcjonujący w Szpitalu wykaz udostępniania tych danych był niezgodny z obowiązującymi wymogami.

Prawidłowo zastosowano fizyczne zabezpieczenia serwerowni Szpitala oraz pomieszczenia wykorzystywanego do przechowywania danych osobowych przetwarzanych w formie elektronicznej. 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[37] oraz możliwości instalowania dowolnego oprogramowania[38] – pełnej ochrony przetwarzanych na tych komputerach danych osobowych pacjentów.

IV. Uwagi i 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:

Wnioski

1. Objęcie szkoleniami z zakresu ochrony danych osobowych wszystkich pracowników Szpitala uczestniczących w przetwarzaniu tych danych.
2. Dostosowanie funkcjonującego w Szpitalu wykazu udostępniania dokumentacji medycznej (*Rejestru wydanych akt*) do wymogów u.o.p.p.
3. Wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających ochronę danych osobowych 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. Podjęcie skutecznych działań w celu zawarcia z dwoma kontrahentami Szpitala[39] umów powierzenia przetwarzania danych osobowych przez Szpital w sytuacji, kiedy występuje on w charakterze Administratora tych danych.
6. Przestrzeganie obowiązujących w Szpitalu wymogów dotyczących jakości stosowanych haseł.

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

[37] Stwierdzono w 19 z 30 badanych przypadków.
[38] Stwierdzono w 9 z 30 badanych przypadków.
[39] Dotyczy umów wykazanych w nieprawidłowości Nr 3 w obszarze 2 niniejszego wystąpienia.

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, 17 kwietnia 2019 r.

	Najwyższa Izba Kontroli
Kontroler	Delegatura w Zielonej Górze
Sebastian Stępień	p.o. Dyrektora
St. Inspektor k.p.	Włodzimierz Stobrawa
.....	.....
podpis	*podpis*