NAJWYŻSZA IZBA KONTROLI
Delegatura w Szczecinie

LSZ.410.002.03.2019

Krzysztof Prętnicki
Prezes Zarządu Szpitala w Dębnie im. Świętej
Matki Teresy z Kalkuty
ul. Kościuszki 58,
74-400 Dębno

WYSTĄPIENIE POKONTROLNE

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

NAJWYŻSZA IZBA KONTROLI
Delegatura w Szczecinie
ul. Jacka Odrowąża 1, 71-420 Szczecin
T +48 91 831 39 00, F +48 91 831 39 66
lsz@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Szpital w Dębnie im. Świętej Matki Teresy z Kalkuty Sp. z o.o. ul. Kościuszki 58, 74-400 Dębno[1].
Kierownik jednostki kontrolowanej	Krzysztof Prętnicki Prezes Zarządu[2], od 1 sierpnia 2018 r., wcześniej od 5 sierpnia 2016 r. do 31 lipca 2018 r. Oskar Skiba. (akta kontroli str. 3-6)
Zakres przedmiotowy kontroli	1. Opracowanie wymaganej dokumentacji oraz procedur związanych z ochroną przetwarzanych danych osobowych. 2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych.
Okres objęty kontrolą	Od 25 maja 2018 r. do dnia zakończenia czynności kontrolnych.
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 Szczecinie.
Kontroler	Wiesław Kaszak, specjalista kontroli państwowej, upoważnienie do kontroli nr LSZ/18/2019 z dnia 8 stycznia 2019 r., (akta kontroli str.1-2)

[1] Dalej: Szpital lub ADO.
[2] Dalej: Prezes.
[3] Dz. U. z 2019 r. poz. 489; dalej: ustawa o NIK.

II. Ocena ogólna[4] kontrolowanej działalności

OCENA OGÓLNA

Szpital prawidłowo chronił i przetwarzał dane osobowe pacjentów, wprowadził rozwiązania organizacyjne zmierzające do zapewnienia ochrony danych osobowych pacjentów oraz poszanowania ich prywatności.

Szpital opracował i wdrożył dokumentację oraz procedury dotyczące ochrony danych osobowych, z dniem wejścia w życie przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[5].

Szpital wdrożył kompleksowy system zarządzania bezpieczeństwem informacji, określony w § 20 ust. 1 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[6], jednak nie wszystkie wytyczne tego systemu były realizowane.

Jedynie części personelu Szpitala zapewniono szkolenia związane z wejściem w życie RODO oraz zagadnieniami dotyczącymi bezpieczeństwa danych, naruszając tym samym przepisy § 20 ust. 2 pkt 6 rozporządzenia KRI.

Szpital właściwie zrealizował swoje obowiązki związane z przeprowadzeniem analizy procesów przetwarzania danych, dokonaniem oceny skutków przetwarzania danych osobowych i prowadzeniem rejestru czynności przetwarzania. Personelowi szpitala zapewniono odpowiedni dostęp do danych medycznych.

Ponadto stwierdzono nieprawidłowości, polegające m.in. na:

- nieodbieraniu uprawnień byłym pracownikom Szpitala oraz nadanie uprawnień administratora systemów informatycznych dla sześciu pracowników, pomimo, że nikomu za wyjątkiem Informatyka takich uprawnień nie przypisano, w szczególności negatywnie należy ocenić przypisanie uprawnień administratora systemów informatycznych pracownikowi rejestracji oraz byłemu pracownikowi Szpitala. Stanowiło to naruszenie § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI oraz §1 Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Szpitalu.

- możliwości logowania się do systemu operacyjnego Szpitala przez cześć personelu za pomocą jednego zbiorowego loginu i hasła przypisanego dla oddziału lub całego Szpitala. Stanowiło to naruszenie § 20 ust. 2 pkt 7 lit. a i § 21 ust. 2 pkt 3, w związku z § 20 ust. 1 rozporządzenia KRI oraz przyjętych regulacji wewnętrznych określonych w § 4 Instrukcji Zarzadzania Systemem Informatycznym służącym do przetwarzania danych osobowych Szpitala.

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

[5] Dz. Urz. UE L 119 z 4.05.2016 r., str. 1, ze zm. Rozporządzenie zwane dalej: RODO.

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

OBSZAR

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

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

Opis stanu faktycznego

1.1. Szpital umową z dnia 25 maja 2018 r., zawartą ze Spółką Wrzecionek & Wspólnicy spółka z ograniczoną odpowiedzialnością w Poznaniu[8] powierzył Kancelarii, prawną obsługę w zakresie bezpieczeństwa danych.
Zarząd Szpitala uchwałą z dnia 25 maja 2018 r.[9] powołał Inspektora Ochrony Danych[10], który jednocześnie był adwokatem w Kancelarii.

(dowód: akta kontroli str. 7, 62, 66-69)

Kancelaria była zobowiązana do prawnej weryfikacji procesów przetwarzania danych z uwzględnieniem zasad wskazanych w RODO, w szczególności informowanie Szpitala, podmiotów przetwarzających i pracowników Szpitala, którzy przetwarzają dane osobowe o obowiązkach spoczywających na nich na mocy przepisów RODO oraz innych przepisów o ochronie danych osobowych i doradzanie im w tej sprawie, monitorowanie przestrzegania przepisów o ochronie danych, w tym o RODO, przeprowadzanie oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, nadzór przestrzegania zasad ochrony danych osobowych, sporządzanie analizy ryzyka oraz przygotowanie planu kontroli zgodności przetwarzania danych osobowych z aktualnymi przepisami prawa, analiza dokumentacji opisującej sposób przetwarzania danych osobowych oraz środków technicznych i organizacyjnych zabezpieczających dane osobowe, analiza upoważnień do przetwarzania danych osobowych i prowadzenie ewidencji osób upoważnionych do przetwarzania.

(dowód: akta kontroli str. 7-9)

Szpital terminowo wywiązał się z obowiązku zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych[11] o powołaniu IOD[12].
Szpital nie ustanowił Administratora Bezpieczeństwa Informacji przed wejściem w życie RODO. Zgodnie z art. 158 ust. 4 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[13] administrator, który przed dniem wejścia w życie niniejszej ustawy nie powołał administratora bezpieczeństwa informacji, jest obowiązany do wyznaczenia inspektora ochrony danych na podstawie art. 37 RODO i zawiadomienia Prezesa Urzędu o jego wyznaczeniu, w terminie do dnia 31 lipca 2018 r. IOD został ustanowiony w dniu 25 maja 2018 r., Prezes Urzędu został powiadomiony w dniu 27 lipca 2018 r. Zawiadomienie zawierało wszystkie elementy określone art. 10 ust. 3 u.o.d.o. Dane IOD oraz sposób i formę kontaktu udostępniono na stronie internetowej Szpitala, zgodnie z wymogami art. 11 w zw. z art. 10 ust. 1 ustawy o ochronie danych osobowych..

(dowód: akta kontroli str. 63-65, 334-339)

---

[7] Oceny cząstkowe to oceny działalności w poszczególnych obszarach badań kontrolnych. Ocena cząstkowa może być sformułowana jako ocena pozytywna, ocena negatywna albo ocena w formie opisowej.
[8] Dalej: Kancelaria.
[9] Nr 5/2018.
[10] Dalej: IOD lub Inspektor.
[11] Dalej Prezes Urzędu.
[12] Informacja przekazana do Prezesa Urzędu w dniu 27 lipca 2018 r.,
[13] Dz. U. poz. 1000, ze zm.; dalej: u.o.d.o.

IOD miał wystarczające przygotowanie i kwalifikacje zawodowe do pełnienia tej funkcji, zgodnie z wymogami art. 37 ust. 5 RODO. IOD posiadał tytuł doktora nauk prawnych i w badanym okresie prowadził zajęcia z zakresu RODO m.in. dla innych inspektorów ochrony danych.

(dowód: akta kontroli str. 66-69)

Do dnia zakończenia kontroli (26.02.2019 r.) Szpital nie został uznany przez Ministra Zdrowia (właściwy organ) za operatora usługi kluczowej, o której mowa w art. 5 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[14].

(dowód: akta kontroli str. 340)

Przed wejściem w życie RODO Szpital zlecił Kancelarii przeprowadzenie audytu bezpieczeństwa danych osobowych. Audyt[15] weryfikował spełnianie przez Szpital obowiązków wynikających z RODO. Stwierdzono m.in., że:
- obowiązek informacyjny nie został przez jednostkę spełniony – w formularzach brak było klauzul informacyjnych, nie było ich także w ogólnodostępnych miejscach, w których składane były wnioski. Zalecono opracowanie nowego wzoru klauzul,
- obowiązek dokumentacyjny nie był spełniony. Szpital nie posiadał żadnego dokumentu, który spełniałby wymogi przewidziane dla Polityki Przetwarzania Danych Osobowych. Tym samym nie posiadał ustrukturyzowanych zbiorów danych osobowych, co było realnym zagrożeniem wycieku danych i braku jakiejkolwiek możliwości zapanowania nad danymi osobowymi,
- brak było w Szpitalu Instrukcji Zarzadzania Systemem Informatycznym zawierającej m.in.: procedury nadawania uprawnień do przetwarzania danych osobowych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności; procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu; sposób, miejsce i okres przechowywania: elektronicznych nośników informacji zawierających dane osobowe, kopii zapasowych; sposób zabezpieczenia systemu informatycznego przed działalnością zewnętrznego oprogramowania,
- osoby pracujące przy systemach przetwarzających dane osobowe nie posiadały upoważnień wystawionych przez administratora danych, brak było możliwości weryfikacji, do jakich zbiorów danych określona osoba ma dostęp. Szpital nie posiadał ewidencji osób upoważnionych do przetwarzania danych osobowych,
- brak było rejestru czynności przetwarzania danych osobowych,
- brak było analizy ryzyka oraz oceny skutków ryzyka,
- brak było wewnętrznych procedur naruszeń ochrony danych osobowych oraz nie powołano IOD.

(dowód: akta kontroli str. 70-153)

1.2. Po wejściu w życie RODO w Szpitalu opracowano, zatwierdzono i podano do wiadomości personelowi dokumentację dotyczącą ochrony danych osobowych tzw. Politykę Bezpieczeństwa, która zawierała:
- rejestr czynności przetwarzania danych[16],
- analizę ryzyka i jej oceny,
- zadania IOD, zadania ASI[17],
- sprawozdania roczne z funkcjonowania systemów ochrony danych osobowych,
- wykaz budynków i pomieszczeń w których wykonuje się operacje przetwarzania danych osobowych,
- sposób przepływu danych między poszczególnymi systemami,
- schemat współpracy systemów informatycznych ze zbiorami danych.

[14] Dz. U. poz. 1560, dalej: ustawa o cyberbezpieczeństwie.
[15] z dnia 21 maja 2018 r.
[16] Dalej: RCPD lub Rejestr.
[17] Administrator Systemów Informatycznych.

- wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

Utrzymanie bezpieczeństwa w Szpitalu w świetle Polityki Bezpieczeństwa rozumiane było jako zapewnienie poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie, a miarą bezpieczeństwa była akceptowalna wielkość ryzyka związanego z ochroną danych osobowych. Zastosowane zabezpieczenia miały zapewnić: poufność danych (właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym osobom), integralność danych (właściwość zapewniająca, że dane osobowe nie zostały zamienione lub zniszczone lub zniszczone w sposób nieautoryzowany), rozliczalność danych (właściwość zapewniająca, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie), integralność systemu (nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej), dostępność informacji (zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne), zarządzanie ryzykiem (proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych). Dokumentacja dotycząca ochrony danych osobowych została zatwierdzona przez Prezesa Zarządu Szpitala w dniu 24 maja 2018 r. oraz przedstawiona do zapoznania się i stosowania pracownikom realizującym wymogi opisane w tej dokumentacji.

(dowód: akta kontroli str. 17-36)

W Polityce Bezpieczeństwa przyjęto m.in., że przetwarzanie danych osobowych obejmuje wszystkie osoby w Szpitalu, które przetwarzają w jakikolwiek sposób oraz w jakiejkolwiek formie dane osobowe – zarówno w systemie informatycznym jak i na nośnikach papierowych. Zarządzający oddziałami i blokami zobowiązani zostali do odpowiedzialności za wdrożenie, realizację i nadzór nad realizacją polityki bezpieczeństwa przez podległych pracowników. Polityka bezpieczeństwa regulowała prawo do ograniczenia przetwarzania, obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych, lub o ograniczeniu przetwarzania, uwzględnienie ochrony danych osobowych w fazie projektowania oraz domyślną ochronę danych, a także opis bezpieczeństwa przetwarzania. W Szpitalu opracowano także Rejestr czynności przetwarzania danych, który stanowił formę dokumentowania czynności przetwarzania danych, pełnił rolę mapy przetwarzania danych i był jednym z kluczowych elementów umożliwiających realizację zasady rozliczalności (inwentaryzowanie i monitorowanie sposobu wykorzystywania danych osobowych).

(dowód: akta kontroli str. 35, 46, 56, 60)

W Szpitalu opracowano także procedury wewnętrzne[18] do których był zobowiązany przyjętą Polityka Bezpieczeństwa, w tym:

- instrukcję zarzadzania systemem informatycznym służącym do przetwarzania danych osobowych w Szpitalu,
- procedurę postępowania w sytuacjach naruszenia ochrony danych osobowych,
- procedurę obsługi zgłoszeń dotyczących ochrony danych osobowych.

Szpital prowadził także ewidencję osób upoważnionych do przetwarzania danych osobowych. Dokumentacja ta w chwili kontroli NIK nie wymagała aktualizacji.

(dowód: akta kontroli str. 37-47, 48-57)

[18] Procedury wewnętrzne z 24 maja 2018 r.

1.3. ADO prowadził rejestr czynności przetwarzania danych osobowych, za które odpowiadał. Rejestr zawierał wszystkie informacje wymagane art. 30 ust. 1 RODO. Obok formy papierowej ADO prowadził rejestr także w formie elektronicznej (excel). Rejestr dotyczył sześciu kategorii zbiorów: pracownicy, kandydaci do pracy, pacjenci, kontrahenci, uczestnicy programów badawczych i profilaktycznych, rejestr poczty wychodzącej i przychodzącej.
Rejestr zawierał także takie pozycje jak:
- opis struktury, m.in. dla „pacjentów" dotyczył danych osobowych pacjentów potwierdzających rejestrację, świadczenie usług medycznych, profilaktyki zdrowotnej, diagnozy medycznej, wykonania umowy o świadczenia medyczne;
- nazwa programu, nazwa pól informatycznych, cel przetwarzania, podstawa prawna, opis kategorii osób, których dane dotyczą, kategorii danych osobowych przetwarzanych w ramach zbioru, kategorii odbiorców, którym dane osobowe zostały lub zostaną ujawnione, planowany termin usunięcia danych, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

(dowód: akta kontroli str. 154-157)

1.4. IOD przeprowadził w dniu 25 maja 2018 r. inwentaryzację aktywów z ryzykiem oraz analizę procesów przetwarzania danych osobowych w Szpitalu. IOD ustalił ryzyka i ich poziomy dla ośmiu podmiotów w tym dla: potencjalnych pracowników, pracowników, pacjentów, kontrahentów, korespondencji, uczestników programów profilaktycznych i badawczych, mienia szpitala. Analiza procesów przetwarzania danych osobowych pacjentów Szpitala wskazywała rodzaje ryzyka, przypisując im wartości ryzyka, w tym:
- szacowane prawdopodobieństwo wystąpienia ryzyka w obszarze finansowym,
- szacowana strata finansowa,
- szacowane prawdopodobieństwo wystąpienia ryzyka w obszarze wizerunkowym,
- szacowana strata wizerunkowa.

Określono poziomy ryzyka oraz wynikające z nich zagrożenia, które w przypadku pacjentów objęły:
- uzyskanie przez nieupoważnioną osobę dostępu do systemu IT z danymi pacjentów,- udostępnianie lub sprzedaż danych pacjentów znajdujących się w systemach IT:
- wprowadzenie do systemów błędnych danych dotyczących pacjentów,
- utrata komunikacji miedzy systemami IT,
- utrata części danych w wyniku awarii serwera baz danych,
- nieuprawnione działanie w systemie IT (np. usunięcie usługi) spowodowane nadaniem zbyt szerokiego dostępu pracownikowi do systemu IT,
- zagubienie dokumentacji papierowej przez pracownika. Poziomy szacowanego ryzyka w obszarze finansowym i wizerunkowym zostały ustalone od 2 do 5 w przyjętej skali, w której dla przedziału 0-5 przyjęto poziom ryzyka akceptowalny. Poziom ryzyka w przedziale 6-9 został zakwalifikowany jako akceptowalny wymagający planu działania, a powyżej 10 jako poziom nieakceptowalny wymagający podjęcia działań minimalizujących dane ryzyko.

W Szpitalu suma ryzyka finansowego i suma ryzyka wizerunkowego powyżej 10 została określona dla:
- dostępu do danych pacjentów przez nieupoważnioną osobę,
- udostępnianie lub sprzedaż danych pacjentów,
- utraty części danych w wyniku awarii serwera,
- nieuprawnionego działania w systemie IT,
- zagubienia dokumentacji papierowej.

Prezes wyjaśnił, że *w celu minimalizacji ryzyka przygotował i wdrożył dokumenty dot. RODO tj. regulaminy, procedury, instytucje, przeprowadził szkolenia w zakresie RODO i zaznajomił wszystkich pracowników z zasadami dotyczącymi ochrony*

danych osobowych Szpitala, na bieżąco prowadzi politykę informacyjna wśród pracowników, współpracowników i pacjentów Szpitala.

(dowód: akta kontroli str. 158-167, 343-344)

1.5. Szpital nie przeprowadzał oceny skutków dla operacji przetwarzania danych osobowych. ADO przedłożył opinię prawną wskazującą m.in., że ocena skutków ryzyka (tzw. DPIA) powinna być przeprowadzana, jeżeli dane przetwarzane są w szczególności z użyciem nowych technologii i może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Ocena taka jest wymagana w szczególności w przypadku przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO (tj. przetwarzanie danych medycznych chociażby w formie rejestru dokumentacji medycznej prowadzonej przez Szpital). Według ADO pacjenci nie są w stanie sprzeciwić się określonemu przetwarzaniu danych osobowych, z uwagi na szereg przepisów prawnych (jak ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych[19]), na podstawie których Szpital wymaga podania określonych danych pacjenta, celem rozliczenia poszczególnych usług względem Narodowego Funduszu Zdrowia, za pomocą konkretnego systemu IT. Oznacza to, że podmiot, którego dane dotyczą nie może skutecznie sprzeciwić się np. metodom przetwarzania bądź nie może nie wyrazić zgody na przetwarzanie jej danych. W opinii zarekomendowano monitoring przyjęcia kodeksu branżowego dla placówek medycznych w zakresie stosowania RODO, który wskaże konieczność przeprowadzenia DPIA. Kodeks Postępowania dla Sektora Ochrony Zdrowia z dnia 13 listopada 2018 r.[20] w pkt. 5.3. stanowi, że podmioty, które nie przetwarzają na dużą skalę danych nie muszą przeprowadzać oceny skutków dla ochrony danych, wymaganych na podstawie art. 35 ust. 3 RODO.

(dowód: akta kontroli str. 168-175)

1.6. W Szpitalu przeprowadzono w okresie objętym badaniem dwa szkolenia z zakresu RODO. W szkoleniu z dnia 9 kwietnia 2018 r., przeprowadzonym przez Kancelarię uczestniczyło 33 pracowników, w tym 17 pielęgniarek i położnych, sześciu lekarzy (kierownicy oddziałów), pięciu pracowników administracji i statystyki, trzy sekretarki medyczne oraz dwie osoby z innych działów medycznych. W szkoleniu z dnia 12 września 2018 r., przeprowadzonym przez firmę MEDRISK uczestniczyło 21 pracowników, w tym 13 pielęgniarek i położnych, dwóch lekarzy, pięć sekretarek medycznych, oraz jedna fizjoterapeutka.

Trzy osoby uczestniczyły w zorganizowanym w Szczecinie w dniu 4 kwietnia 2018 r. przez Zachodniopomorski Klaster Medyczny Synergia szkoleniu pt. RODO w Jednostkach Ochrony Zdrowia zgodnie z przepisami obowiązującymi od 25 maja 2018 r. Osoby te otrzymały Certyfikaty uczestnictwa w tym szkoleniu. Jedna osoba uczestniczyła w szkoleniu zorganizowanym przez Centrum Usługowo Doradcze Pomerania w Dębnie w dniu 24 października 2017 r., w zakresie założeń wynikających z ustawy RODO (zagadnienie to szerzej opisano w dalszej części wystąpienia, w sekcji „*Stwierdzone nieprawidłowości*").
Wszyscy pracownicy Szpitala (258 osób) zostali zapoznani z obowiązującymi procedurami dotyczącymi postępowania zgodnie z RODO i podpisali stosowne do swoich uprawnień oświadczenie. Oświadczenia umieszczono w aktach osobowych pracowników.

(dowód: akta kontroli str. 177, 193-204, 275-287)

[19] Dz.U. z 2018 r. poz. 1510, ze zm.
[20] Wersja: 22 przygotowana w celu przedłożenia do Prezesa Urzędu Ochrony Danych Osobowych (załącznik nr 1 do wniosku).

1.7. Po ukazaniu się przewodnika „RODO w służbie zdrowia” (24 września 2018 r.) Szpital przed punktem rejestracji pacjenta umieścił na podłodze przed stanowiskiem rejestracji taśmę oznaczającą obszar, w którym może przebywać obsługiwana osoba, usunięto z sal chorych tzw. karty gorączkowe, które stały się dostępne w gabinetach pielęgniarskich, pacjenci na etapie przyjmowania do Szpitala otrzymywali opaskę identyfikującą na przedramieniu.

(dowód: akta kontroli str. 176)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następującą nieprawidłowość:
IOD nie wywiązał się w pełni z obowiązku prowadzenia szkoleń personelu uczestniczącego w operacjach przetwarzania danych, wynikającego z art. 39 ust. 1 lit. b RODO. Szkoleniami z zakresu RODO, objętych zostało jedynie 57 (22%) spośród 258 pracowników Szpitala. Ponadto obowiązek zapewnienia szkoleń osobom zaangażowanym w proces przetwarzania informacji, z uwzględnieniem zagrożenia jej bezpieczeństwa, skutków naruszenia zasad bezpieczeństwa, konsekwencji prawnych i środków zapewniających jej bezpieczeństwo wynika z § 20 ust. 2 pkt 6 rozporządzenia KRI.
Prezes wyjaśnił: *Szpital jest specyficzną placówką, której trudno jest jednorazowo przeszkolić wszystkich pracowników. W pierwszej kolejności przeszkoleni zostali ci, którzy na co dzień maja kontakt z danymi pacjentów w tym z danymi wrażliwymi. Pozostałych pracowników przeszkolimy w miesiącu marcu bieżącego roku.*

(dowód: akta kontroli str. 291, 311)

OCENA CZĄSTKOWA

Szpital wywiązał się z obowiązku opracowania i wdrożenia dokumentacji oraz procedur dotyczących ochrony danych osobowych z dniem wejścia w życie RODO. W Szpitalu w badanym okresie obowiązywała Polityka Bezpieczeństwa, która zawierała plan eksploatowania, monitorowania i przeglądania oraz utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji zapewniającego poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Przeprowadzono analizę procesów przetwarzania danych. Szpital posiadał regulacje wewnętrzne takie jak instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, procedury postępowania dla Szpitala w sytuacjach naruszeń ochrony danych osobowych, procedury obsługi zgłoszeń dotyczących ochrony danych osobowych.
Szpital tylko dla części personelu zapewnił szkolenia związane z wejściem w życie przepisów RODO oraz zagadnieniami dotyczącymi bezpieczeństwa danych.

OBSZAR

2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych.

Opis stanu faktycznego

2.1. W celu właściwej ochrony danych osobowych w Szpitalu wprowadzono następujące rozwiązania:

- w trzech badanych oddziałach Szpitala[21] na łóżkach szpitalnych nie było kart pacjentów z ich nazwiskiem i innymi danymi o stanie zdrowia pacjenta.

[21] Oddział Ginekologiczno-Położniczy, Oddział Chorób Wewnętrznych, Oddział Chirurgii Ogólnej.

- pacjenci badanych oddziałów posiadali na nadgarstkach opaski z numerem tzw. księgi głównej oraz z imieniem i nazwiskiem pacjenta na wewnętrznej stronie opaski.
- w dyżurkach pielęgniarskich na trzech objętych oględzinami oddziałach szpitalnych ruch chorych prowadzony był w miejscu niewidocznym dla osób postronnych (dane pacjentów były ukryte). Podręczna dokumentacja (karty gorączkowe) przechowywana była w zamkniętych szafkach. Dokumentacja medyczna znajdowała się w gabinetach lekarskich pod zamknięciem na klucz w szafkach. W salach chorych łóżka oznaczono numerem zawierającym numer sali i numer łóżka. Szpital nie posiadał specjalistycznej drukarki do wydruków opasek.
- Personel pielęgniarski we wszystkich objętych oględzinami oddziałach szpitalnych, opuszczając dyżurkę pielęgniarek, blokował dostęp do systemu komputerowego.
- Sposób udostępniania kopii dokumentacji medycznej został uregulowany w instrukcji udostępniania dokumentacji medycznej pacjentom, osobom przez nich upoważnionym oraz przedstawicielom ustawowym pacjentów, a także organom i innym upoważnionym podmiotom[22].

(dowód: akta kontroli str. 178-184, 313-319)

W Szpitalu funkcjonowała jedna ogólna rejestracja z jednym dwuosobowym okienkiem przy którym rejestrowane były jednocześnie dwie osoby, nie było możliwości wglądu przez innego pacjenta do danych osobowych osoby rejestrowanej. W odległości ok. 1,5 metra od okienka znajdowała się linia zapewniająca odstęp pomiędzy osobą obsługiwaną a pacjentami w kolejce do rejestracji. Na blacie okienka umieszczono klauzulę informacyjną o przetwarzaniu danych osobowych. Pacjenci byli proszeni o dowód osobisty i na tej podstawie rejestrowani w systemie do odpowiednich poradni lekarskich. Karty pacjentów znajdowały się w poradniach.

W obrębie wzroku pacjentów rejestrujących się nie było danych osobowych innych pacjentów. Podczas rejestracji do gabinetu lekarzy poradni specjalistycznych pacjentowi przydzielany był kolejny numer z ustną informacją o orientacyjnej godzinie przyjęcia do specjalisty.
Ekrany komputerów (2 komputery) nie były zwrócone w stronę pacjenta, znajdowały się poniżej blatu okienka, nie były widoczne dla pacjentów.

Pacjenci oczekujący na wizytę w poradniach wywoływani byli według kolejności rejestracji bez podawania imienia i nazwiska i innych danych osobowych pacjenta, podając numer nadany w rejestracji.

Dokumentacja pacjentów w trzech objętych oględzinami gabinetów poradni specjalistycznych przechowywano we właściwy sposób, tak aby nie można było odczytać danych osobowych przez nieuprawnione osoby. W miejscu ogólnie widocznym znajdowała się jedynie karta pacjenta aktualnie przebywającego w gabinecie.

W trakcie oględzin gabinety lekarskie były pod nadzorem personelu medycznego. Nie stwierdzono opuszczenia gabinetu lekarskiego przez personel w trakcie wywoływania i trwania wizyt pacjentów.

(dowód: akta kontroli str. 185-188, 225)

W Szpitalu nie było zamontowanego monitoringu wizyjnego. Na poddanych oględzinom oddziałach, poradniach i rejestracji nie stwierdzono niewłaściwego

[22] Zarządzenie wewnętrzne Nr. SD.II./52/05/2015 z dnia 26 maja 2015 r.

zabezpieczenia danych medycznych oraz osobowych pacjentów. Rozwiązania techniczne i organizacyjne nie stwarzały możliwości ujawnienia danych medycznych pacjentów.

(dowód: akta kontroli str. 174-188)

Szpital dysponował tzw. matrycą systemów IT, w której przypisano dostęp do systemów IT w Szpitalu poszczególnym komórkom organizacyjnym z wyszczególnieniem sprawowanych funkcji np. oddział wewnętrzny: kierownik oddziału, osoba koordynująca oddziału/zastępca, pielęgniarka dyżurna, pielęgniarka zabiegowa, asystent/lekarz dyżurny, opiekun medyczny, sanitariusz. Dostęp do poszczególnych systemów został określony z dwóch poziomów: Poziom I (PI) – wgląd, kopiowanie, modyfikacja, wprowadzenie oraz Poziom II (PII), tj. Poziom I + usuwanie danych; trzecia kategoria to brak dostępu (bd). Na przykładzie oddziału wewnętrznego stwierdzono, że dostęp z poziomu PI do bazy danych HIS był przypisany wyżej wymienionym według funkcji. Ponadto do modułu apteka szpitalna dostęp przypisano tylko osobie koordynującej oddziału/zastępca. Analogicznie przypisano w innych oddziałach szpitalnych (Dziecięcy, ZOL, Położniczo-Ginekologiczny, Neonatologiczny, Chirurgiczny, Blok Operacyjny, Izba Przyjęć, Opieka Nocno-Świąteczna, Ambulatoryjna Opieka Specjalistyczna, Rehabilitacja).

(dowód: akta kontroli str. 189-192)

2.2. Personel działów administracyjnych (niemedycznych)[23] Szpitala liczył 57 osób, z tego dziewięć osób zatrudnionych w Dziale Organizacji i Nadzoru, tj. w Statystyce medycznej cztery osoby, w Rejestracji medycznej cztery osoby oraz Informatyk jedna osoba.

Osoby te posiadały dostęp do systemu HIS, w myśl art. 24 ust. 2 pkt 2 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjentów[24], zgodnie z którym osoby wykonujące czynności pomocnicze przy udzielaniu świadczeń zdrowotnych, a także czynności związane z utrzymaniem systemu teleinformatycznego są uprawnione do dostępu do danych medycznych, na podstawie upoważnień administratora danych.

Na próbie 30 spośród 48 zatrudnionych w działach niemedycznych, stwierdzono, że 22 osoby posiadały aktywny profil w domenie HIS, jednak w żadnym z tych przypadków nie przypisano im ról, nie mogły wykonywać operacji w systemie HIS i przetwarzać danych osobowych pacjentów Szpitala. Aktywny profil w domenie HIS bez przypisania ról oznaczał tylko, że osoby te są pracownikami Szpitala i korzystają z innych programów niemedycznych. Nie mieli oni możliwości zalogowania się do systemów medycznych.

Cztery osoby nie posiadały aktywnego profilu w domenie HIS.

Sanitariusze (cztery osoby) zajmujący się transportem chorych nie posiadali uprawnień do przetwarzania danych osobowych pacjentów w dostępie do profilu w domenie HIS. W systemie nie były widoczne daty ani godziny nadania uprawnień.

(dowód: akta kontroli str. 193-199)

Prezes zarządu Szpitala wyjaśnił: *Cały system HIS pracuje na bazie danych ORACLE można szczegółowo ustalić co się wydarzyło z danym pracownikiem jakie wprowadzał dane, kiedy i z jakich modułów korzystał. Można też ustalić kiedy i kto nadał pracownikowi uprawnienia, ale dostępne jest z poziomu serwisu oprogramowania. System jest tak zabezpieczony, że wpis usunięty z poziomu modułu medis czy innego nie znika z bazy danych ale jest „cieniem", do którego w razie problemu można dojść i ustalić zdarzenie. Szpital z poziomu administratora*

[23] Działy niemedyczne: Biuro obsługi Zarządu (1 osoba), Dział Finansowo-księgowy (5 osób), Dział Kadr i Płac (4 osoby), Dział Techniczno-Gospodarczy (8 osób), Dział Żywienia (1 osoba), Sekcja utrzymania czystości i transportu wewnętrznego (25 osób).

[24] Dz. U. z 2017 r. poz. 1318, ze zm.; dalej: u.o.p.p.

systemów informatycznych ma dostęp do podstawowej historii, a do „cieni" ma tylko dostęp serwis oprogramowania.

(dowód: akta kontroli str. 333)

2.3. Na próbie 30 spośród 108 pielęgniarek i położnych zatrudnionych w Szpitalu stwierdzono, że wszystkie posiadały aktywny profil w domenie HIS w obszarze w którym były zatrudnione. Osobom tym przypisano role: blok operacyjny, izba przyjęć, pielęgniarka, położna. Dostęp do danych medycznych pacjentów został im przypisany tylko z oddziału, którego byli pracownikami. Było to zgodne z ich zakresem obowiązków i nadanymi przez ADO upoważnieniami do przetwarzania danych osobowych.

(dowód: akta kontroli str. 193-201)

W trakcie oględzin stwierdzono, że siedem osób posiadało w systemie HIS nadane uprawnienia administratora z możliwością nadawania uprawnień innym użytkownikom, w tym informatyk, cztery osoby ze statystyki medycznej, jedna z rejestracji oraz jedna osoba (były pracownik Szpitala) – zatrudniona w Szpitalu do 2013 r.
W umowie z dnia 25 maja 2018 r. Szpital powierzył Informatykowi obowiązki Administratora Systemów Informatycznych. W zakresach czynności pracowników statystyki (cztery osoby) brak było zapisów o upoważnieniu tych osób do nadawania uprawnień innym pracownikom. W zakresie czynności rejestratorki (jedna osoba) nie było zapisów do nadawania uprawnień innym pracownikom. Były pracownik Szpitala także takich uprawnień nie posiadał. (zagadnienie to szerzej opisano w dalszej części wystąpienia, w sekcji „*Stwierdzone nieprawidłowości*")

(dowód: akta kontroli str. 218-219, 225, 255-263)

2.4. Na próbie 31 spośród 46 byłych pracowników Szpitala, z którymi rozwiązano stosunek pracy w okresie od 1 stycznia 2017 r. do 24 stycznia 2019 r. ustalono, że wg stanu na 24.01.2019 r. na godzinę 11:15, siedmiu osobom nie odebrano dostępu do systemu informatycznego HIS. Pozostałe 24 osoby nie posiadały aktywnego profilu w domenie HIS (zagadnienie to szerzej opisano w dalszej części wystąpienia, w sekcji „*Stwierdzone nieprawidłowości*")**.**
W panelu administratora systemu, nie znajdowały się informacje o dacie ostatniego logowania się danego użytkownika oraz dacie odebrania/zablokowania mu uprawnień w tym systemie.

(dowód: akta kontroli str. 202-204, 255-258, 265-274)

2.5. Szpital korzystał z mechanizmów zdalnego zgłaszania usterek jedynemu dostawcy oprogramowania związanego z udzielaniem świadczeń zdrowotnych. Zgłaszanie usterek odbywało się drogą e-mailową. W okresie od 25 maja 2018 r. do 26 lutego 2019 r. Szpital zgłosił 13 usterek posiadanego oprogramowania, przy czym w żadnym z tych przypadków nie przekazywano usługodawcy danych osobowych bądź danych medycznych pacjentów. Szpital zawarł umowę na świadczenie usług stałego serwisu eksploatacyjnego[25] zawierającą m.in. załącznik dotyczący zasad powierzenia danych osobowych, w których Wykonawca (Powiernik) oświadczył, że w ramach działalności prowadzonego przez siebie przedsiębiorstwa wdrożył środki dotyczące zabezpieczenia przetwarzanych danych wymagane przepisami ustawy o ochronie danych osobowych oraz wdrożył wymagania, o których mowa w rozporządzeniu 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

[25] Umowa z 30 listopada 2017 r. z Technologie Realizacji Kontraktów w Katowicach.

osobowych[26]. Powiernik oświadczył, że opracował oraz wdrożył System Zarządzania Bezpieczeństwem Informacji zgodny z normą ISO/IEC 27001 i posiada certyfikat poświadczający jego zgodność z tą normą.
Szpital nie posiadał informacji dotyczących wywiązania się przez dostawcę wdrożonego oprogramowania z obowiązku przeprowadzenia testów akceptacyjnych, określonych w art. 21 ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[27]

(dowód: akta kontroli str. 2015-217, 227-240, 241-242, 340)

2.6. Szpital zawarł w badanym okresie jedną umowę dotyczącą powierzenia przetwarzania danych osobowych. Szpital nie zawierał innych umów na przetwarzanie danych osobowych z innymi podmiotami w tym serwisującymi sprzęt medyczny.
Umową z dnia 25 maja 2018 r. powierzono przetwarzania danych osobowych Spółce z ograniczona odpowiedzialnością Wrzecionek & Wspólnicy z siedziba w Poznaniu[28]. Umowa, zgodnie z art. 28 RODO stanowiła, że Kancelaria:
- dokonuje przetwarzania danych osobowych wyłącznie na udokumentowane polecenie Administratora (ADO)[29],
- zapewnia, by osoby upoważnione do przetwarzania danych, jeśli nie podlegają odpowiedniemu ustawowemu obowiązkowi do zachowania danych w tajemnicy, zobowiązały się do zachowania danych osobowych w tajemnicy,
- podejmuje wszelkie niezbędne środki dla zapewnienia bezpieczeństwa powierzonych do przetwarzania danych osobowych, w tym w szczególności w zakresie wdrożenia odpowiednich środków technicznych, organizacyjnych oraz teleinformatycznych, przy uwzględnieniu celu. Zakresu i charakteru przetwarzanych danych osobowych oraz ryzyka naruszenia praw i wolności osób, których przetwarzane dane osobowe dotyczą,
- wspiera ADO w realizacji obowiązków związanych z ochrona danych osobowych,
- pomaga ADO w wywiązywaniu się z obowiązków określonych w art. 32-36 RODO, w tym m.in. w stosownym przypadku zapewni: pseudonimizację i szyfrowanie danych osobowych; zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania; zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego; regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania,
- zawiadamia ADO o każdym incydencie naruszenia bezpieczeństwa powierzonych danych osobowych, każdym żądaniu udostępnienia danych osobowych, każdym żądaniu otrzymanym bezpośrednio od osoby, której dane dotyczą,
- niezwłocznie udziela odpowiedzi na pytanie Administratora dotyczące kwestii związanych z przetwarzaniem powierzonych przez ADO danych osobowych.
Administrator kontroluje sposób przetwarzania powierzonych danych osobowych po uprzednim poinformowaniu Kancelarii o planowanej kontroli. Administrator lub wyznaczone przez niego osoby były uprawnione do wstępu do pomieszczeń oraz wglądu do dokumentacji związanej z przetwarzaniem danych osobowych. ADO był uprawniony do żądania od Procesora udzielania informacji dotyczących przebiegu przetwarzania danych osobowych, oraz udostępniania rejestrów przetwarzania.

---

[26] Dz. U. z 2004 r. Nr 100, poz. 1024; uchylone z dniem 26.02.2019 r.

[27] Dz. U. z 2017 r. poz. 570, ze zm.

[28] Kancelaria Prawna ul. Paderewskiego 8, 61-770 Poznań. Rejestr Przedsiębiorców KRS prowadzonego przez Sąd Rejonowy Poznań-Nowe Miasto i Wilda w Poznaniu, VIII Wydział Gospodarczy Krajowego Rejestru Sadowego, pod numerem 697429..

[29] Szpital.

Do 26 lutego 2019 r. Szpital nie zawierał umów w których byłby podmiotem przetwarzającym dane pacjentów.

(dowód: akta kontroli str. 11-16, 345)

2.7. Zgodnie z zapisami Rejestru Naruszeń (stanowiącego element Polityki Bezpieczeństwa) w Szpitalu nie wystąpiły przypadki naruszenia zasad ochrony danych osobowych pacjentów.

(dowód: akta kontroli str. 290)

2.8. W Szpitalu obowiązywało w badanym okresie zarządzenie wewnętrzne Zarządu Szpitala[30] w sprawie wprowadzenia w życie Instrukcji udostępniania dokumentacji medycznej pacjentom, osobom przez nich upoważnionym oraz przedstawicielom ustawowym pacjentów, a także organom i innym uprawnionym podmiotom. Zarządzenie odpowiadało postanowieniom art. 24 ust. 2 u.o.p.p. i regulowało zasady udostępniania dokumentacji medycznej w szczególności:
- pacjentowi, którego ta dokumentacja dotyczy za okazaniem dowodu tożsamości,
- przedstawicielowi ustawowemu pacjenta za okazaniem: rodzice do ukończenia przez dziecko 18 lat, za okazaniem swojego dowodu osobistego i metryki urodzenia dziecka; opiekunowie ustanowieni przez sąd, za okazaniem stosownego orzeczenia,
- osobie upoważnionej przez pacjenta w dokumentacji medycznej, za okazaniem dowodu tożsamości,
- osobie, posiadającej pisemne upoważnienie od pacjenta.

W okresie objętym kontrolą Szpital udostępnił dokumentację medyczną łącznie 132 krotnie (do 22 lutego 2019 r.), z tego firmom ubezpieczeniowym sześciokrotnie. Podmioty ubezpieczeniowe występujące z wnioskiem o udostepnienie danych miały pisemne upoważnienie pacjenta. W 15 przypadkach dokumentacja medyczna została udostępniona innej osobie niż pacjent, którego ta dokumentacja dotyczyła. Wszystkie 15 osób posiadało upoważnienie do przekazania dokumentacji medycznej osobie z wniosku, z tego w 13 przypadkach upoważnienie udzielone przez pacjentów, jedno orzeczenie sądowe i jedno dla opiekuna dziecka po okazaniu dokumentu tożsamości. W pozostałych 111 przypadkach dokumentacja została udostępniona pacjentom oraz takim instytucjom jak: prokuratura, sądy oraz uprawnione osoby ze Szpitala (lekarze, pielęgniarki).
Nie stwierdzono naruszeń ochrony danych osobowych w tym zakresie.

(dowód: akta kontroli str. 313-325, 326-332)

2.9. Szpital był wyposażony w dziewięć komputerów z zainstalowanym systemem operacyjnym Windows XP, jeden z Windows Vista. Komputery z tymi systemami zlokalizowane były po jednym: Blok operacyjny, Chirurgia, Noworodki, oraz dwa na Ginekologii, dwa w Statystyce służące do archiwalnego systemu obsługi Szpitala i do rejestracji rozmów telefonicznych, dwa w księgowości do archiwalnego systemu ST w MS-DOS i do pracy tymczasowej (Windows Vista), jeden w serwerowni jako archiwalny stary system Płatnik ZUS. Systemy te nie posiadały wsparcia producenta. Zainstalowanie ich na komputerach w Szpitalu stwarzało przez te urządzenia ryzyko dla bezpieczeństwa infrastruktury informatycznej Szpitala, które może skutkować nieprawidłowościami w przyszłości, jeśli Szpital nie podejmie odpowiednich działań, np. wycofanie tych systemów z użytku.

Prezes wyjaśnił, że *Szpital ciągle modernizuje infrastrukturę informatyczną, jednostki z XP i Vista pracujące zostaną wymienione na nowe. Są trzy komputery archiwalne na których musi zostać system XP ponieważ stare programy, które pracowały pod MS-DOS nie uruchomimy na nowych komputerach. Komputery te*

[30] Nr SD.II./52/05/2015 z dnia 26 maja 2015 r.

włączane są sporadycznie w celu dostępu do archiwalnych danych, komputer Vista został już wyłączony z eksploatacji.

(dowód: akta kontroli str. 243, 245, 288, 291)

Na podstawie losowo wybranych 30 komputerów w Szpitalu[31], spośród 59 komputerów służących do przetwarzania danych osobowych ustalono, że:
- w każdym z 30 badanych przypadków zalogowanie się do systemu HIS wymagało podania własnego loginu przypisanego użytkownikowi i podanie jego hasła,
- metodą uwierzytelniania przy logowaniu się do systemu operacyjnego w 10 przypadkach było podanie nazwy użytkownika (loginu) oraz indywidualnego hasła, w 10 przypadkach poprzez podanie loginu i hasła przypisanego działowi lub oddziałowi Szpitala, w 10 przypadkach poprzez podanie loginu i hasła jednego zbiorowego dla Szpitala (zagadnienie to szerzej opisano w dalszej części wystąpienia, w sekcji „*Stwierdzone nieprawidłowości*"),
- we wszystkich 30 badanych przypadkach loginy przy logowaniu się do systemu HIS były zgodne z instrukcją zarządzania systemem informatycznym. W trakcie oględzin nie stwierdzono przypadku wprowadzania przez użytkownika innych nie swoich danych autoryzacyjnych, przydzielonych innej osobie,
- długość haseł indywidualnych dostępu do systemu HIS odpowiadał wymaganiom określonym w dokumentacji wewnętrznej Szpitala tj. w Instrukcji zarządzania systemem Informatycznym służącym do przetwarzania danych osobowych w Szpitalu.
- na wszystkich wybranych komputerach zostały zainstalowane programy antywirusowe (ESET Endpoint Antivirus) i były one aktualne (miały aktualna bazę sygnatur antywirusowych),
- spośród 30 poddanych oględzinom komputerów w 16 był zainstalowany system operacyjny Windows 7 PRO, na dwóch Windows 7 Ultimate, na 10 system Windows 10 PRO, na jednym Windows Serwer 2016, na jednym Windows 8.1. PRO,
- na żadnym z 30 komputerów uprawnienia nadane użytkownikowi nie pozwalały na instalację oprogramowania.
- na dyskach komputerów poddanych oględzinom nie stwierdzono plików zawierających dane medyczne lub osobowe oraz nie stwierdzono niezabezpieczonych USB.

(dowód: akta kontroli str.243-247, 291-310)

W kwestii tworzenia i testowania kopii zapasowych, Administrator Systemów Informatycznych wyjaśnił, że:

- wykonywany jest zrzut całej bazy danych, później pakowany w celu zmniejszenia rozmiaru kopii, a następnie przekopiowany w miejsce docelowe, kopie wykonywane są automatyczne codziennie w nocy, system jest rotacyjny a najstarsza kopia ma 10 dni. Kopiowane są też programy KAMSOFT wraz z bieżącą konfiguracją i ustawieniami,
- kopia obejmuje główną bazę danych HIS, wszystkie systemy medyczne i administracyjne, (MEDIS, SOMED, ZZL, PPS),
- kopie przechowywane są na twardych dyskach jedna jest w serwerowni, druga w budynku administracji na dysku sieciowym NAS, zamknięta w szafie teleinformatycznej, co około pół roku przeprowadzone jest rozpakowanie archiwum i sprawdzenie zgodności zrzutu bazy danych przed importem na serwer.

Szpital posiadał pięć komputerów typu laptop, które nie były szyfrowane. ASI wyjaśnił, że dwa używane były jako mobilne, a dostęp do danych odbywa się w szyfrowanym tunelu VPN i pracowały na terminalach lokalnych (na laptopach był

[31] po 10 użytkowanych przez lekarzy, pielęgniarki lub położne oraz przez pracowników administracji Szpitala.

tylko system operacyjny).Trzy laptopy były częścią sieci i pracowały jak zwykłe komputery, zainstalowane zostały z powodu braku miejsca na instalację zestawu stacjonarnego. Znajdowały się w zamkniętych gabinetach gdzie nie miały dostępu osoby trzecie (pokoje lekarskie, gabinet oddziałowej). Do dnia kontroli Szpital nie wykorzystywał pseudonimizacji. ASI wyjaśnił, że dotychczas nie było potrzeby pseudonimizacji danych.

(dowód: akta kontroli str. 289, 312)

Szpital posiadał jedno pomieszczenie serwerowni. Pomieszczenie było odpowiednio zabezpieczone, wyposażone w drzwi przeciwpożarowe (antywłamaniowe) zamykane na klucz, nie było systemu alarmowego lub przeciwwłamaniowego, nie stosowano systemu kontroli dostępu, nie było systemu monitoringu kamer. Serwerownię wyposażono w wolnostojącą gaśnicę oraz w klimatyzację. Serwery i urządzenia znajdowały się w specjalnie do tego przeznaczonych szafach. Urządzeniom zapewniono układy podtrzymywania napięcia (tzw. UPS) na wypadek zaniku zasilania. Nie stwierdzono w serwerowni niewykorzystanych urządzeń takich jak komputery przeznaczone do utylizacji lub innych materiałów np. łatwopalnych akt i mebli.

(dowód: akta kontroli str. 143)

Ustalone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowości:

1. Siedem osób miało w systemie HIS uprawnienia administratora z możliwością nadawania uprawnień innym użytkownikom. Jedyną osobą uprawnioną do nadawania uprawnień innym pracownikom zgodnie z umową był tylko Administrator Sieci Informatycznych (Informatyk). Pozostałe sześć osób takich uprawnień na piśmie nie posiadało.

(dowód: akta kontroli str. 218-219, 225, 255-263)

Zgodnie z przepisami art. 5 pkt 1 lit. c RODO dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane ("minimalizacja danych"). W myśl § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI zarządzanie bezpieczeństwem informacji realizuje się m.in. poprzez podejmowanie 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; bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.

Prezes wyjaśnił: *Uprawnienia administracyjne obecnie posiadają cztery osoby – statystyka i administrator. Pani nr 5 ze statystyki obecnie jest na urlopie wychowawczym i uprawnienia zostały jej wyłączone. Pani nr 6 rejestratorka miała nadane uprawnienia administratora, przez problemy z systemem nie mogła pracować zostały one włączone na test i nie wyłączone po nim, obecnie są wyłączone. Pani nr 7, która pracowała do 2013 r. zmieniła nazwisko wyszła za mąż, zostało to przeoczone, nowe nazwisko wyłączone było po zakończeniu pracy stare pozostało.*

Paniom nadano uprawnienia administratora systemów informatycznych ponieważ pracują w jednym dziale Organizacji i Nadzoru i wzajemnie się zastępują. Przeoczeniem ze strony pracodawcy było nie sformalizowanie tych uprawnień w formie pisemnej. Informujemy, że zostanie to niezwłocznie uzupełnione.

(dowód: akta kontroli str. 288, 311, 341)

2. Siedmiu osobom spośród 31, którzy odeszli z pracy w latach 2017-2019 (do 24 stycznia 2019 r.) nie odebrano dostępu do systemu informatycznego HIS.

(dowód: akta kontroli str. 219, 224)

Art. 5 pkt 1 lit. c RODO wskazuje zasadę adekwatności i minimalizacji danych, tj. wymóg ustalenia kto i w jakim zakresie jest uprawniony do przetwarzania danych. Natomiast, w myśl motywu 39 RODO, dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu.

Zgodnie z 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 z wykonywaniem zawodu medycznego.
Stosownie do przepisu § 20 ust. 2 pkt 5 rozporządzenia KRI, kierownictwo podmiotu publicznego jest obowiązane do podejmowania działań zapewniających bezzwłoczną zmianę uprawnień, w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji (np. odbierania uprawnień w systemach po zakończeniu zatrudnienia).

Prezes Zarządu wyjaśnił, że siedmiu osobom spośród 31, które odeszły z pracy ze Szpitala w latach 2017-2019 nie odebrano dostępu do systemu informatycznego HIS ponieważ w dalszym ciągu jesteśmy na etapie doskonalenia procedur związanych z wymogami RODO. Eliminujemy wszystkie usterki i niedociągnięcia, które się pojawiły w minionym okresie. Osoby, które odeszły z pracy nie posiadały przynależności do oddziałów i w konsekwencji nie miały dostępu do danych wrażliwych pacjentów.

(dowód: akta kontroli str. 288, 311)

3. Spośród 30 badanych komputerów w 10 przypadkach metodą uwierzytelniania przy logowaniu się do systemu operacyjnego było podanie loginu i hasła przypisanego działowi lub oddziałowi Szpitala, w 10 przypadkach poprzez podanie loginu i hasła jednego zbiorowego dla Szpitala. Nie było znane, która z osób fizycznych używających tego samego (jednego) loginu, przetwarzała w systemie operacyjnym dane podlegające prawnej ochronie.

(dowód: akta kontroli str. 243-247, 291-310)

Działanie to było niezgodne 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 użytkowniokom, nie jest możliwa prawidłowa rozliczalność sytemów.

Takie działania stanowiły także naruszenie przyjętych w Szpitalu regulacji wewnętrznych wyrażonych w § 4 Instrukcji Zarzadzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Szpitalu.

Natomiast, w myśl motywu 39 RODO, dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu.

Prezes wyjaśnił: *System informatyczny w części używa haseł grupowych są to głównie komputery pielęgniarek używane jako terminal dostępowy do systemu MEDIS (tu hasła są indywidualne). Wynikało to z niezgodności systemów operacyjnych w trakcie instalacji domeny. Komputery miały system w wersji HOME i nie współpracowały z domeną lokalną. Obecnie przygotowujemy się do modernizacji*

zasobów serwerowych i aktualizacji systemów operacyjnych serwerów, co pozwoli nam na rozwiązanie tego problemu. Duża rozbieżność czasowa między systemami serwerowymi nie pozwoli też na sprawną delegację domeny lokalnej i obecnie włożona praca była by nie efektywna. System W10 nie w pełni współpracuje z Windows 2003 serwer.

(dowód: akta kontroli str. 345)

OCENA CZĄSTKOWA

Szpital wprowadził rozwiązania organizacyjne zmierzające do zapewnienia ochrony danych osobowych pacjentów oraz poszanowania ich prywatności. Personelowi szpitala zapewniono odpowiedni dostęp do danych medycznych, jednak wystąpiły przypadki nadania uprawnień administratora systemów informatycznych pracownikom nieuprawnionym oraz nie odebrania części byłym pracownikom dostępu do systemów informatycznych. Było to niezgodne z zasadami określonymi przepisami art. 5 pkt 1 lit. c RODO oraz § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI. Takie działania stanowiły także naruszenie przyjętych w Szpitalu regulacji wewnętrznych wyrażonych w § 1 i 2 Instrukcji Zarzadzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Szpitalu. Dostęp do systemu operacyjnego dla części komputerów był nieodpowiednio zabezpieczony, gdyż znaczna cześć użytkowników systemu operacyjnego nie posiadała indywidualnego loginu i hasła i logowała się do systemu za pomocą loginu i hasła przypisanego dla oddziału bądź całego Szpitala. Stanowiło to naruszenie § 20 ust. 2 pkt 7 lit. a i § 21 ust. 2 pkt 3, w związku z § 20 ust. 1 rozporządzenia KRI oraz przyjętych regulacji wewnętrznych określonych w § 4 Instrukcji Zarzadzania Systemem Informatycznym służącym do przetwarzania danych osobowych Szpitala. Personel medyczny Szpitala adekwatnie do swoich uprawnień przetwarzał dane medyczne pacjentów zgodnie z art. 24 u.o.p.p.

Wnioski

IV. Wnioski

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

1. Bezzwłoczne odbieranie uprawnień w systemach informatycznych byłym pracownikom Szpitala.

2. Delegowanie uprawnień administratora sieci informatycznych jedynie osobom do tego upoważnionym.

3. Zapewnienie szkoleń, o których mowa w § 20 ust. 2 pkt 6 rozporządzenia KRI, wszystkim pracownikom zaangażowanym w proces przetwarzania informacji.

4. Wyeliminowanie możliwości logowania się do systemu operacyjnego Szpitala za pomocą zbiorowego loginu i hasła przypisanego oddziałom szpitalnym lub dla całego Szpitala.

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 Szczecinie. 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 dnia 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.

Szczecin, 25 marca 2019 r.

Najwyższa Izba Kontroli
Delegatura w Szczecinie

Wiesław Kaszak
Specjalista k.p

Dyrektor