NAJWYŻSZA IZBA KONTROLI
Delegatura w Krakowie

LKR. 410.002.01.2019

Pani
dr n.med. Renata Godyń-Swędzioł
Dyrektor Szpitala Miejskiego Specjalistycznego
im. Gabriela Narutowicza w Krakowie

WYSTĄPIENIE POKONTROLNE

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

NAJWYŻSZA IZBA KONTROLI
Delegatura w Krakowie
ul. Łobzowska 67, 30-038 Kraków
T +48 12 342 34 00, F +48 12 342 34 44
lkr@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Szpital Miejski Specjalistyczny im. Gabriela Narutowicza w Krakowie (*Szpital*),
Kierownik jednostki kontrolowanej	dr n.med. Renata Godyń-Swędzioł, Dyrektor Szpitala, od dnia 18 września 2002 r. (*Dyrektor*)
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 29 marca 2019 r. Badania kontrolne mogły dotyczyć działań sprzed tego okresu, jeśli miały związek z zagadnieniami będącymi przedmiotem kontroli.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[1]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Krakowie
Kontroler	Małgorzata Kram, specjalista kontroli państwowej, upoważnienie do kontroli nr LKR/22/2019 z 11 stycznia 2019 r.

(akta kontroli str.1 do 2)

[1] Dz.U. z 2019 r. poz. 489 dalej: *ustawa o NIK*

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

W okresie objętym kontrolą w Szpitalu opracowano wymaganą dokumentację oraz procedury związane z ochroną przetwarzanych danych osobowych. Przyjęte rozwiązania techniczne i organizacyjne nie zapewniały jednak pełnej ochrony danych osobowych i nie eliminowały ryzyka nieuzasadnionego dostępu do danych przetwarzanych w systemach informatycznych Szpitala.

W Szpitalu w sposób prawidłowy sporządzono dokumentację związaną z ochroną danych osobowych, uwzględniającą przepisy 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 (tzw. ogólne rozporządzenie o ochronie danych)[3], w tym opracowano procedury wewnętrzne oraz dokonywano wymaganych przeglądów i aktualizacji opracowanej dokumentacji. W Szpitalu wyznaczono Inspektora Ochrony Danych (*IOD*) i poprzez przyjęte rozwiązania organizacyjne zagwarantowano mu status niezależności w sprawowaniu tej funkcji. Zgodnie z wymogiem określonym w art. 37 ust. 7 RODO, dane IOD oraz sposób i formę kontaktu z IOD udostępniono na tablicach informacyjnych umieszczonych w sąsiedztwie rejestracji. NIK ocenia negatywnie niezamieszczenie tych informacji na stronie internetowej Szpitala, gdyż naruszono art. 11 uodo[4].

W sposób prawidłowy prowadzono rejestr czynności przetwarzania danych osobowych, przeprowadzano analizy procesów przetwarzania danych osobowych, zawarto wymagane umowy powierzenia przetwarzania danych osobowych oraz udostępniano dokumentację medyczną pacjentów. W trakcie kontroli nie stwierdzono przypadków ujawnienia i przekazywania takich danych podmiotom zewnętrznym w ramach procesu zgłaszania błędu/awarii oprogramowania, a także osobom lub podmiotom nieuprawnionym.

Personelowi szpitala zapewniono możliwość dostępu do danych medycznych nadając niektórym z nich uprawnienia dostępu do systemu MLS Medicall SOFTWARE (*System lub HIS*). NIK negatywnie ocenia przyjętą w Szpitalu praktykę dostępu do stacji roboczych w sposób umożliwiający użycie jednego konta użytkownika przez wielu pracowników co wymagało przekazywania pomiędzy pracownikami danych (haseł) do autoryzacji w systemach operacyjnych, uniemożliwiając tym samym ich jednoznaczne rozróżnienie. Dodatkowo przypisywano użytkownikom zbyt wysokie uprawnienia w systemach operacyjnych.

W ocenie NIK zagrożenie dla bezpieczeństwa danych osobowych pacjentów, które może skutkować nieprawidłowościami w przyszłości (jeżeli Szpital nie podejmie odpowiednich działań) stanowić może przechowywanie archiwalnej dokumentacji medycznej zawierającej te dane, w trzech objętych badaniem oddziałach, w niezamkniętych szafach w pomieszczeniach oddziałowych sekretariatów. Nieprawidłowym było nieszyfrowanie dysków twardych komputerów przenośnych co stanowiło naruszenie § 20 ust. 2 pkt 8 i pkt 9 rozporządzenia KRI[5].

---

[2] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej. W niniejszym wystąpieniu zastosowano ocenę opisową.

[3] Dz. Urz. UE L 119 z 2016 r., str. 1, dalej: RODO.

[4] uodo - ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000, ze zm.).

[5] Rozporządzenie 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 (Dz. U. z 2017 r. poz. 2247).

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[6] kontrolowanej działalności

OBSZAR

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

Opis stanu faktycznego

1.1. W dniu 25 maja 2018 r. Dyrektor Szpitala wyznaczył IOD, wywiązując się tym samym z obowiązku określonego w art. 8 u.o.d.o.[7] w związku z art. 37 RODO. Na to stanowisko powołany został Kierownik Działu Organizacji, pełniący dotychczas funkcję Administratora Bezpieczeństwa Informacji (dalej: ABI). W myśl art. 8 i art. 10 uodo, Szpital terminowo (za pośrednictwem formularza elektronicznego) wywiązał się z obowiązku zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych (*PUODO*) o powołaniu IOD. Przekazane zawiadomienia, zawierały niezbędne elementy określone art. 10 ust. 1 i 3 u.o.d.o., tj. m.in. imię, nazwisko oraz adres poczty elektronicznej i numer telefonu IOD, pełną nazwę oraz adres siedziby i numer identyfikacyjny REGON administratora danych osobowych. Zgodnie z wymogiem określonym w art. 37 ust. 7 RODO, dane IOD oraz sposób i formę kontaktu z IOD udostępniono na tablicach informacyjnych umieszczonych w sąsiedztwie rejestracji. Informacji tych nie zamieszczono na stronie internetowej Szpitala co było niezgodne z art. 11 uodo, który mówi, że podmiot, który wyznaczył inspektora, udostępnia dane inspektora, o których mowa w art. 10 ust. 1, niezwłocznie po jego wyznaczeniu, na swojej stronie internetowej.

W zakresie czynności IOD wskazano wszystkie zadania określone w art. 39 RODO oraz umożliwiono mu wykonywanie obowiązków w sposób niezależny, stosownie do art. 38 ust. 3 tego rozporządzenia. Zgodnie z zakresem czynności, IOD podlegał bezpośrednio Dyrektorowi Szpitala natomiast NIK zwraca uwagę, że jego stanowisko nie zostało wyodrębnione w strukturze organizacyjnej i nie zamieszczono w Regulaminie Szpitala[8]. W zakresie czynności wskazano, że do obowiązków IOD należało m.in.:

- informowanie administratora danych osobowych oraz pracowników przetwarzających dane osobowe o obowiązkach spoczywających na nich na mocy RODO;
- monitorowanie przestrzegania RODO i innych przepisów o ochronie danych osobowych;
- inicjowanie działań zwiększających świadomość pracowników z zakresu ochrony danych osobowych, tym szkoleń;
- nadzór nad prowadzonymi audytami i inspekcjami z zakresu zgodności procesów przetwarzania danych osobowych z RODO;
- udzielanie na żądanie Dyrektora zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonywania - zgodnie z art. 35 RODO.

(akta kontroli str. 5 do 14, 18 do 23)

Dyrektor Szpitala wyjaśniła, że niezależność IOD zapewniono poprzez bezpośrednią podległość Dyrektorowi Szpitala w zakresie pełnionej przez IOD funkcji, a zadania Inspektora Ochrony Danych nie zostały określone w Regulaminie Organizacyjnym ze względu na fakt, że jest to funkcja, a nie stanowisko. Regulamin Organizacyjny określa wyłącznie zadania komórek organizacyjnych (oddziałów, działów, pracowni, samodzielnych stanowisk pracy).

(akta kontroli str. 12 do 14, 509, 511)

Zgodnie z wymogami art. 37 ust. 5 RODO, osoba realizująca zadania IOD miała należyte przygotowanie i kwalifikacje zawodowe do pełnienia swojej funkcji, tj. m.in.: była wcześniej ABI Szpitala, ukończyła studia podyplomowe „Wykonywanie funkcji

---

[6] 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.

[7] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000, ze zm.).

[8] Regulamin Organizacyjny Szpitala wprowadzony Zarządzeniem nr 146/2018 Dyrektora z dnia 23 października 2018 r.

administratora bezpieczeństwa informacji i inspektora ochrony danych", posiadała certyfikaty ukończenia odpowiednich kursów w latach 2016-2019, tj. m.in. zaświadczenia/certyfikaty o udziale w szkoleniach: „Pełnienie roli Administratora Bezpieczeństwa Informacji Prowadzenie Sprawdzeń, „Administrator Bezpieczeństwa Informacji", „Nowa rola administratorów bezpieczeństwa informacji w sektorze ochrony zdrowia w świetle krajowych i unijnych przepisów o ochronie danych osobowych. Ponadto IOD oświadczył, że brał udział w pracach i seminariach organizowanych przez Stowarzyszenie Ekspertów i Inspektorów Ochrony Danych z siedzibą w Krakowie

(akta kontroli str. 275 do 281)

Do 15 marca 2019 r. Szpital nie został uznany za operatora usługi kluczowej, o którym mowa w art. 5 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.[9]

(akta kontroli str. 275)

1.2. W dniu wejścia w życie przepisów RODO oraz u.o.d.o. (25 maja 2018 r.) Dyrektor Szpitala przyjęła Politykę Bezpieczeństwa Danych Osobowych w Szpitalu Miejskim Specjalistycznych im. Gabriela Narutowicza w Krakowie (dalej: Polityka), zgodnie z art. 24 ust. 1 i 2 RODO. W dokumencie tym wskazano, że Polityka określa zasady ochrony danych osobowych przetwarzanych przez Szpital, wskazując obszar zabezpieczenia, podział zadań oraz wymagane zabezpieczenia. W Polityce określono, że opisane i zastosowane w dokumentacji bezpieczeństwa danych osobowych zalecenia mają zapewnić realizację zasad, o których mowa w art. 5 ust.1 RODO. Jako podstawę opracowania Polityki, w szczególności powołano się na motyw 78. Określono w niej (rozdział) środki organizacyjne i techniczne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych, w tym zadania Administratora, IOD, Administratora Systemów Informatycznych (*ASI*), radcy prawnego, kierownika komórki organizacyjnej (w tym: innej osoby pełniącej funkcje kierownicze, osoby zatrudnionej na samodzielnym stanowisku pracy), osób upoważnionych do przetwarzania danych osobowych, a także zakres przedmiotowy i podmiotowy jej stosowania. Ponadto w Polityce wskazano: organizacyjne wymagania zabezpieczenia, zestawienie minimalnych wymagań dla systemów informatycznych przetwarzających dane osobowe, zasady zarządzania ryzykiem przetwarzania danych osobowych (sposób przeprowadzenia analizy ryzyka), zasady udostępniania danych osobowych, sposoby realizacji praw, zabezpieczenie przed oprogramowaniem szkodliwym, fakt zapoznania się z jej treścią przez osoby upoważnione do przetwarzania danych osobowych. Integralną częścią Polityki były załączniki, wśród których znalazły się m.in.: wzór upoważnienia do przetwarzania danych osobowych; wzór ewidencji osób upoważnionych do przetwarzania danych osobowych; wzór wniosku o nadanie uprawnień do przetwarzania danych osobowych w systemie informatycznym; wzór potwierdzenia odbycia szkolenia w zakresie ochrony danych osobowych; wzór ewidencji osób upoważnionych do przetwarzania danych osobowych; przykłady naruszeń ochrony danych osobowych, wzór dziennika systemu informatycznego. Analiza postanowień przyjętej Polityki oraz jej załączników wykazała, że zawierały one aktualne dane. Z postanowieniami przyjętej Polityki zapoznano pracowników Szpitala na przeprowadzonych przez IOD szkoleniach, a dokumenty zamieszczono w folderze dostępnym dla wszystkich pracowników Szpitala folderze.
Dyrektor zatwierdziła jedną aktualizację Polityki (13 lutego 2019 r.) Polegała ona na wprowadzeniu Procedury nr 14 – Realizacja prawa dostępu do dokumentacji medycznej w trybie art. 15 RODO, i zmodyfikowano treści klauzul informacyjnych.

(akta kontroli str. 90 do 195, 279 do 280, 284 do 289)

Polityka nie przewidywała konieczności opracowania dodatkowych reguł i procedur uszczegóławiających (w zakresie ochrony danych osobowych).

(akta kontroli str. 201 do 202)

[9] ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560).

1.3. Rejestr czynności przetwarzania danych osobowych (dalej: Rejestr), o którym mowa w art. 30 RODO, został sporządzony zgodnie z obowiązującymi przepisami 25 maja 2018 r. wraz z aktualizacją Polityki. Był prowadzony w formie elektronicznej oraz został wydrukowany. Zawierał wszystkie wymagane elementy określone w art. 30 ust. 1 RODO, tj. m.in.: nazwę oraz dane kontaktowe ADO i IOD, cele przetwarzania, opis kategorii osób, których dane dotyczą, kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO, planowane terminy usunięcia poszczególnych kategorii danych oraz informację dotyczącą ewentualnego przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej. W Rejestrze zidentyfikowano 23 kategorie osób i przypisano im odpowiednie czynności, m.in.: zakres, charakter i kontekst przetwarzanych danych; podstawę prawną przetwarzania; sposób realizacji praw osób, których dane były przedmiotem przetwarzania.

(akta kontroli str. 277)

1.4. Po dokonaniu analizy procesów przetwarzania danych osobowych pacjentów w Szpitalu, określoną w art. 32 RODO, wprowadzono 25 maja 2018 r, Politykę. Kolejne dwie analizy zostały przeprowadzone przez IOD 29 listopada 2018 r. i 7 lutego 2019 r. Ich wynikiem były:

1) aktualizacja rejestru czynności przetwarzania w zakresie sposobu i formy prowadzenia ;
2) aktualizacja Polityki poprzez wprowadzenie procedury nr 14 – dostarczanie kopii danych w postaci dokumentacji medycznej w trybie art. 15 ust. 3 RODO.

W ramach analiz wskazano 31 czynności przetwarzania danych osobowych, dla których zidentyfikowano od 1 do 9 ryzyk związanych z ochroną tych danych. Dla każdego z ryzyk oszacowano jego wartość wynoszącą od 2[10] (rejestrowanie korespondencji przychodzącej i wychodzącej) do 20 (prowadzenie dokumentacji medycznej; monitorowanie bezpieczeństwa systemu informatycznego w zakresie ryzyka braku zgłaszania, rejestrowania i obsługi incydentów naruszenia zasady ochrony danych) określoną jako iloczyn prawdopodobieństwa wystąpienia i skutku wystąpienia incydentu.

W rezultacie przeprowadzonej analizy, jako stanowiące największe zagrożenie (poziom ryzyka – 15-25 pkt) wskazano następujące czynności przetwarzania:

- monitorowanie bezpieczeństwa sytemu informatycznego (ryzyka: w zakresie braku zgłaszania rejestrowania i obsługi incydentów naruszenia zasad ochrony danych; autoryzacji użytkowników za pomocą cudzych loginów i haseł; korzystanie z nieautoryzowanego oprogramowania);
- prowadzenie dokumentacji medycznej indywidualnej i zbiorczej w związku z procesem udzielania świadczeń zdrowotnych (ryzyka: brak usunięcia danych po okresie przetwarzania; brak stosowania polityki haseł, świadome ujawnianie haseł innym użytkownikom; niewłaściwa utylizacja dokumentacji medycznej po zakończonym okresie przetwarzania);
- udostępnianie dokumentacji medycznej – (ryzyka: ujawnienie informacji o stanie zdrowia nieuprawnionym podmiotom).
- Na podstawie przeprowadzonej analizy opracowano Plan postępowania z ryzykiem (dalej: Plan postępowania), w którym dla wszystkich 31 zidentyfikowanych czynności przetwarzania, niezależnie od zidentyfikowanych zagrożeń wartości ryzyka[11], wskazano działania jakie należy wdrożyć w celu ich ograniczenia (przykładowo: zredagowanie uprawnień, wdrożenie procedur zarządzania dostępem, blokowanie komputera, kontrola ruchu osobowego, stosowanie szafek zamykanych na klucz, nadzór pracownika Szpitala nad pracownikiem firmy sprzątającej, prowadzenie szkoleń); nie zostały wskazane terminy przeprowadzenia tych działań natomiast wskazano osoby za to odpowiedzialne – poprzez wskazanie funkcji (kierownik komórki organizacyjnej). Najczęstszym działaniem zaradczym była konieczność przeprowadzenia szkoleń oraz zapoznanie pracowników z Polityką.

(akta kontroli str. 277 do 278)

[10] dla szacowania ryzyka przyjęto skalę od 1 pkt do 25 pkt
[11] rozpoznano 71 zagrożeń

1.5. W Szpitalu została wykonana ocena skutków dla ochrony danych (dalej: DPIA), o której mowa w art. 35 RODO, mimo że jest fakultatywna i taka pojedyncza (bieżąca) ocena dotyczyć powinna operacji wiążących się z wysokim ryzykiem. Również Grupa Robocza ds. Ochrony Danych zdecydowanie zalecała dokonanie tej analizy dla operacji przetwarzania już trwających przed 25 maja 2018 r. oraz w przypadkach, gdy nie jest jasne, czy wymagana jest DPIA. Wyżej wymieniona analiza nie stanowiła elementu Polityki. Opracowana DPIA zawierała wymagane elementy określone w art. 35 ust. 7 RODO, w tym opis operacji przetwarzania i ocenę niezbędności oraz proporcjonalności.

(akta kontroli str. 280, 410 do 435)

IOD wyjaśnił, że jednym z powodów przeprowadzenia oceny skutków było opublikowanie przez Generalnego Inspektora Ochrony danych Osobowych w dniu 27 marca 2018 r. propozycji wykazu operacji przetwarzania, dla których wymagane jest przeprowadzenie oceny skutków dla ochrony danych. Ponadto kierował się Wytycznymi Grupy Roboczej art. 29 dotyczącymi oceny skutków dla ochrony danych oraz pomagających ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679. W wytycznych przyjętych w dniu 4 kwietnia 2017 r. zmienionych 4 października 2017 r. (GIODO opublikował polską wersję językową wytycznych w dniu 10 maja 2018 r.). Ponadto podał, że jeszcze jako ABI, *kierując się powyższymi publikacjami oraz mając na uwadze ryzyka związane z przetwarzaniem danych osobowych szczególnej kategorii przede wszystkim w zakresie prowadzenia i udostępniania dokumentacji medycznej, w systemie HIS oraz mając na uwadze specyfikę organizacyjną poszczególnych komórek organizacyjnych działalności leczniczej, trwające prace remontowe i fakt, iż przetwarzanie odbywa się systematycznie na dużą skalę - podjął decyzję o konieczności przeprowadzenia DPIA w Szpitalu. Decyzja o przeprowadzeniu DPIA była podjęta na długo przed opublikowaniem w dniu 24 sierpnia 2018 r. Komunikatu Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 sierpnia 2018 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony*.

(akta kontroli str. 506 do 507)

1.6. Jednym z zadań IOD, w myśl art. 39 ust. 1 lit. b RODO, jest prowadzenie szkoleń personelu uczestniczącego w operacjach przetwarzania danych. IOD przeprowadził siedem szkoleń w okresie od 13 kwietnia 2018 r. do 25 maja 2018 r.

Na dzień 25 maja 2018 r. w Szpitalu przeszkolono 91% pracowników (liczba zatrudnionych: 953 osoby), co zostało potwierdzone podpisami na listach obecności. Ponadto w każdy nowo zatrudniany pracownik był kierowany do IOD w celu odbycia szkolenia z zakresu ochrony danych osobowych (było to potwierdzane podpisem na karcie obiegowej oraz na liście przeszkolonych osób). Zakres szkoleń obejmował m.in. definicje dotyczące RODO oraz uodo, legalności przetwarzania danych osobowych, obowiązku informacyjnego, zasad ujawniania oraz powierzenia danych osobowych, zasad bezpiecznego użytkowania sprzętu IT, zgłaszania incydentów itp.

Na prośbę IOD treść Polityki, Regulaminu Monitoringu oraz Zasad udostępniania dokumentacji medycznej, poradniki urzędu ochrony danych osobowych i poradniki RODO, zostały umieszczone w zasobach sieciowych, dostępnych dla pracowników Szpitala posiadających dostęp do komputera. Dla osób, które nie miały dostępu do komputera, na kierowników poszczególnych komórek organizacyjnych nałożono obowiązek zapoznania pracowników z zapisami ww. dokumentów. Potwierdzeniem zapoznania się ze wskazaną dokumentacją był podpis każdego pracownika Szpitala na oświadczeniu o zachowaniu danych w poufności. Na dzień 20 marca 2019 r. do przeszkolenia w zakresie RODO pozostało 29 osób, długotrwale nieobecnych w pracy (urlopy macierzyńskie, wychowawcze, świadczenia rehabilitacyjne itd.).

(akta kontroli str. 275 do 281, 282 do 283)

IOD wyjaśnił, że dla grupy 9% pracowników, nieprzeszkolonych do 25 maja 2018 r., którzy pomimo pisemnego powiadomienia przez IOD o terminach poszczególnych szkoleń nie uczestniczyli w tych szkoleniach, utworzony został na dysku publicznym w zasobie RODO – folder: MATERIAŁY SZKOLENIOWE. W folderze zamieszczono materiały ze szkolenia do samodzielnego zapoznania się.

(akta kontroli str. 507 do 508)

1.7. Szpital nie zobowiązał się formalnie do przestrzegania regulacji zawartych w Kodeksie postępowania dla sektora ochrony zdrowia (wniosek o jego przyjęcie został przedłożony PUODO 13 listopada 2018 r.), lub pozostałych opracowań związanych z ochroną danych osobowych, takich jak „Przewodnik po RODO w służbie zdrowia" i „Wytyczne dotyczące inspektorów ochrony danych".

IOD wyjaśnił, że kodeks postępowania, o którym mowa w art. 40 RODO, nie jest stosowany w Szpitalu ponieważ jest on w fazie projektu. Podał ponadto, że Szpital stosuje wytyczne zawarte www. opracowaniach. Treść opracowań omówiono m.in. z Ordynatorami Oddziałów, Kierownikami i Pielęgniarkami Oddziałowymi a jego treść przekazano zainteresowanym oddzielnym pismem.

(akta kontroli str. 275 do 281, 506 do 508)

Stwierdzone nieprawidłowości

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

Na stronie internetowej Szpitala nie zamieszczono, danych IOD oraz sposobu i formy kontaktu z IOD, które udostępniono (zgodnie z wymogiem określonym w art. 37 ust. 7 RODO) na tablicach informacyjnych umieszczonych w sąsiedztwie rejestracji. Nie zamieszczenie ww. informacji na stronie internetowej Szpitala było niezgodne z art. 11 uodo, który mówi, że podmiot, który wyznaczył inspektora, udostępnia dane inspektora, o których mowa w art. 10 ust. 1, niezwłocznie po jego wyznaczeniu, na swojej stronie internetowej.

(akta kontroli str. 5 do 14, 18 do 23, 275, 522, 523)

IOD podał, że informacje o IOD w trakcie kontroli zostały zamieszczone na stronie BIP Szpitala.

(akta kontroli str. 275)

Kontrola wykazała, że strona o adresie http://www.narutowicz.krakow.pl/rodo - zawiera komunikat: „podana strona nie istnieje".

(akta kontroli str. 522, 523)

OCENA CZĄSTKOWA

Szpital wywiązał się z obowiązku opracowania dokumentacji oraz procedur dotyczących ochrony danych osobowych, które uwzględniały przepisy RODO. Ich aktualizacja i dostosowanie do tych regulacji nastąpiło w dniu wejścia w życie tego rozporządzenia. Wywiązano się z obowiązku powołania IOD i terminowego zgłoszenia tego faktu do PUODO. Przeprowadzono analizę procesów przetwarzania danych oraz ocenę skutków przetwarzania danych osobowych, mimo że nie była ona obligatoryjna. Pracowników Szpitala zapoznano z regulacjami dotyczącymi ochrony danych osobowych i zagadnieniami dotyczącymi bezpieczeństwa danych oraz obejmowano szkoleniami wszystkie nowozatrudnione osoby. Prowadzony rejestr czynności przetwarzania zawierał wszystkie wymagane elementy. NIK negatywnie ocenia brak zamieszczenia na stronie internetowej Szpitala informacji kontaktowych do IOD, co było niezgodne z art. 11 uodo.

OBSZAR

2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych

Opis stanu faktycznego

2.1. Przeprowadzone oględziny trzech funkcjonujących w Szpitalu rejestracji/recepcji wykazały, że w celu ochrony danych osobowych pacjentów funkcjonowanie rejestracji zorganizowano tak, aby zminimalizować wgląd w dokumenty osoby znajdującej się przy sąsiednim stanowisku. W żadnej z rejestracji/recepcji nie zamontowano przesłon pomiędzy poszczególnymi stanowiskami. Nie stwierdzono by osoba znajdująca się przy sąsiednim okienku słyszała informacje podawane przez osobę rejestrującą się obok, co jednak nie wyklucza takiej możliwości.

We wszystkich rejestracjach umieszczono informację o treści: „Przy okienku rejestracji może przebywać tylko jedna osoba" oraz wyznaczono linię rozgraniczającą strefę oczekiwania. W ten sposób zapewniono odstęp pomiędzy osobami przy okienku,

a kolejnymi osobami w kolejce. Przy okienkach rejestracji zamieszczono informację dla pacjentów o konieczności okazania dowodu osobistego. Identyfikacja pacjentów (rejestrujących się w trakcie prowadzonych oględzin) odbywała się na podstawie okazywanych rejestratorce dokumentów. W trakcie oględzin pracownicy rejestracji nie wypowiadali na głos informacji zawierających dane osobowe, przekazując jedynie dane dotyczące dalszego procesu postępowania po zarejestrowaniu się do danej poradni lub gabinetu.

Zapewniono, aby w obrębie wzroku pacjenta znajdującego się przy oknie rejestracji nie znajdowały się dokumenty zawierających dane osobowe innych pacjentów. Dokumenty osób zarejestrowanych na kolejny dzień były przygotowywane w teczkach[12] do przeniesienia do poradni Szpitala.

Wszystkie komputery znajdujące się w rejestracji/recepcji były ustawione w sposób uniemożliwiający osobom postronnym wgląd w treści na nich wyświetlane. Pacjenci po zakończonej rejestracji kierowani byli do gabinetów poradni i tam oczekiwali w kolejce.

(akta kontroli str. 196 do 200)

We wszystkich trzech objętych oględzinami gabinetach poradni specjalistycznych Szpitala[13], dokumentację pacjentów przechowywano we właściwy sposób, tj. pacjent wchodzący do gabinetu nie miał możliwości zapoznania się z danymi osobowymi innych osób oczekujących w kolejce lub tych, którzy odbyli już wizytę. Ponadto w trakcie oględzin, nie zaobserwowano, aby którykolwiek gabinet został pozostawiony bez opieki oraz nie stwierdzono przypadków pozostawienia klucza w drzwiach. Wywoływanie pacjentów wszystkich poradni odbywało się w sposób gwarantujący im anonimowość.

(akta kontroli str. 390 do 406)

Przeprowadzone oględziny dyżurek pielęgniarskich, sal chorych oraz gabinetów lekarskich na trzech oddziałach szpitalnych[14] wykazały m.in., że:

- na oddziałach znajdowały się łącznie 22 sale chorych, dysponujące 67 łóżkami;
- wszystkich 63 zaobserwowanych w trakcie oględzin pacjentów nosiło na nadgarstku wydrukowane opaski informacyjne zawierające kod kreskowy (ID do 6 cyfr), datę i godz. przyjęcia, nazwę Szpitala;
- na jednym oddziale[15] umieszczono karty przy łóżkach pacjentów, w sposób uniemożliwiający odczytanie danych na nich zapisanych;
- ruch chorych[16] prowadzony był w dyżurkach pielęgniarskich w miejscach niewidocznych dla osób postronnych;
- w dyżurkach pielęgniarskich zorganizowanych jako otwarte punkty recepcyjne, dokumentację medyczną przechowywano w zamkniętych szafkach, a bieżące dokumenty były umieszczone pod blatem w sposób uniemożliwiający ich zobaczenie;
- trzy dyżurki pielęgniarskie poddane oględzinom wyposażono w trzy komputery, z których dwa zabezpieczone były wygaszaczem ekranu; w przypadku jednego oddziału zablokowany hasłem wygaszacz ekranu został włączony w trakcie oględzin. W czasie trwania oględzin żaden z komputerów nie pozostał zostawiony bez obsługi;
- na trzech oddziałach poddanych oględzinom znajdowały się cztery gabinety lekarskie, wyposażone w 12 komputerów, z których uruchomionych było 10. W czasie oględzin pracowali na nich lekarze;
- dokumentacja medyczna pacjentów w gabinetach lekarskich dwóch oddziałów z ww. trzech oddziałów była przechowywana w szafach zamykanych na klucz, w jednym[17] oddziale zaś gromadzono ją na półkach nieposiadających możliwości zamknięcia.

(akta kontroli str. 390 do 406)

---

[12] W sposób niepozwalający osobom postronnym na poznanie danych osobowych.
[13] Oględzinami objęto trzy poradnie: Endokrynologiczną, Otolaryngologiczną i Chirurgii Urazowej.
[14] Oględziny przeprowadzono w dyżurkach pielęgniarskich: Oddziału Kardiologii, Oddziału Otolaryngologii i Oddziału Chirurgii Urazowej.
[15] Oddział Kardiologiczny.
[16] Ruch chorych to lista pacjentów danego oddziału wraz z numerem sali, w których przebywają.
[17] Oddział Urazowo-Ortopedyczny.

W sekretariatach trzech oddziałów[18] podręczna dokumentacja medyczna zawierająca dane osobowe pacjentów przechowywana była poza szafkami, które nie posiadały możliwości zamknięcia, natomiast pomieszczenia te były zamykane i zaopatrzone w zamki zatrzaskowe. Podobna sytuacja miała miejsce w jednym (z trzech) poddanych oględzinom gabinetów lekarskich – gdzie dokumentację medyczną przechowywano na półkach nieposiadających możliwości zamknięcia. Zgodnie z art. 23 ust. 2 uopp,[19], dane zawarte w dokumentacji medycznej podlegają ochronie. Ponadto zgodnie z postanowieniami pkt 4 Regulaminu, ochrona przed wglądem osób nieupoważnionych lub kradzieżą dokumentacji papierowej zawierającej dane osobowe polega m.in. na zabezpieczeniu (zamykaniu) dokumentów w szafach, biurkach i pomieszczeniach podczas nieobecności w trakcie godzin pracy.

Dyrektor wyjaśniła, że:

1) Na Oddziale Kardiologicznym nieprawidłowo przechowywana dokumentacja medyczna dotyczyła niewielkiej części bieżącej dokumentacji wytworzonej w dniu kontroli. Całość bieżącej dokumentacji medycznej Oddziału Kardiologii przechowywana jest w segregatorach umieszczonych w szafach zamykanych na klucz, a ponadto dokumentacja z lat 2016-2017 znajduje się w pomieszczeniu archiwum oddziałowego zamykanego na klucz w szafach zamykanych na klucz.
2) W zakresie Oddziału Urazowo-Ortopedycznego przechowywanie dokumentacji medycznej poza zamkniętymi na klucz szafkami wynikała z bardzo dużego przyrostu wytwarzanej dokumentacji medycznej w ostatnich dwóch latach wskutek znacznego zwiększenia kontraktu z Narodowym Funduszem Zdrowia. W sekretariacie medycznym dokumentacja przechowywana jest pod nadzorem sekretarki medycznej w kartonowych pudełkach, które uniemożliwiają wgląd w dane. Obecnie zlecono montaż, zamówionych dodatkowych szaf na dokumentację medyczną, co pozwoli na przeniesienie całości dokumentacji do szaf zamykanych na klucz.
3) W zakresie Oddziału Otolaryngologii informuję, że w sekretariacie medycznym przechowywana dokumentacja medyczna w kartonowych pudłach umieszczonych na szafie była przygotowana do przekazania do archiwum, ale z powodu braków kadrowych (ciągłe zastępstwa w sekretariacie) dokumentacja ta nie została przekazana do archiwum.

W odniesieniu do zabezpieczenia dokumentacji medycznej ww. Oddziałów podkreślenia wymaga fakt, że dostęp do pomieszczeń sekretariatów medycznych (za wyjątkiem Oddz. Kardiologii) i dyżurek lekarskich ww. oddziałów chroniony jest poprzez zastosowanie zabezpieczeń fizycznych tj. drzwi zatrzaskowych, uniemożliwiających wejście do pomieszczeń osób nieuprawnionych. Ponadto Szpital przedstawił organowi tworzącemu listę rankingową zawierającą zadania inwestycyjne planowane do realizacji przez Szpital w 2019 roku i w latach następnych. Lista zawiera zadanie p.n. Przystosowanie pomieszczeń archiwum. Na 2020 rok zaplanowane zostało opracowanie dokumentacji projektowej, a na 2021 rok – roboty budowlano-instalacyjne. Realizacja wyżej wymienionego zadania inwestycyjnego pozwoli na zwiększenie powierzchni archiwum Szpitala, co udrożni proces przekazywania przez oddziały bardzo dużej ilości dokumentacji medycznej wytworzonej w ciągu ostatnich dwóch lat i znacznie zmniejszy ryzyko wynikające z jej przechowywania poza zamkniętymi na klucz szafami".

(akta kontroli str. 509 do 513, 516 do 518)

W ramach przeprowadzonych oględzin stwierdzono, że na żadnym z trzech oddziałów nie funkcjonuje monitoring wizyjny. Zamontowano go tylko w drugim budynku Szpitala, w którym mieścił się SOR.

Regulamin funkcjonowania monitoringu wizyjnego został wprowadzony zarządzeniem Dyrektora Szpitala w dniu 29 sierpnia 2018 r. i został udostępniony pracownikom Szpitala 31 sierpnia 2018 r. poprzez zamieszczenie jego treści w katalogu publicznym.

(akta kontroli str. 22 do 23, 390 do 406)

[18] Oddział Kardiologiczny, Otolaryngologiczny, Urazowo - Ortopedyczny
[19] Dz. U. z 2017 r. poz. 1318, ze zm. Ustawa zwana dalej: *u.o.p.p.*

2.2. Według stanu na 28 lutego 2019 r. personel działów administracyjnych Szpitala liczył 103 osób. Analiza uprawnień w systemie HIS[20], jakie zostały nadane 10 osobom z 46 należących do tej grupy wykazała,) że odpowiadały one zakresom zadań i obowiązków realizowanych przez tych pracowników. Osoby z tej grupy zatrudnione były w m.in. w dziale organizacyjnym, recepcji szpitala, dziale dokumentacji medycznej.

(akta kontroli str. 261 do 263, 264)

2.3. Przeprowadzona analiza zakresu posiadanego dostępu do danych medycznych 30 (z 227) pielęgniarek i położnych zatrudnionych w Szpitalu[21] wykazała, że tylko 8 na 30 skontrolowanych posiadało dostęp i przetwarzało dane medyczne pacjentów w systemie HIS, posiadały one pisemne potwierdzenie nadanych im przez administratora upoważnień do przetwarzania danych osobowych. Pozostałe pielęgniarki takiego dostępu do systemu HIS nie miały. Posiadały one natomiast upoważnienia ADO do przetwarzania danych osobowych. Odpowiadało to wymogom art. 32 ust. 4 RODO, aby administrator podjął działania w celu zapewnienia, by każda osoba fizyczna działająca z jego upoważnienia, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na jego polecenie.

(akta kontroli str. 44 do 49, 261 do 263, 264, 267, 269 do 272, 290 do 389)

Dyrektor wyjaśniła, że funkcjonujący w Szpitalu system HIS wykorzystywany był do przesyłania zleceń elektronicznych. Przykładem tego rozwiązania jest zlecenie na wykonanie badań obrazowych tj. RTG, USG lub TK. Powyższe zlecenia są generowane w systemie i automatycznie przesyłane do odpowiedniej pracowni, jak również wyświetlane na poszczególnych urządzeniach obrazowych (tzw. worklista). Nie zmienia to faktu, że skierowanie ze względu na przepisy prawa i wewnętrzne regulacje Szpitala dotyczące dokumentacji medycznej jest drukowane i autoryzowane przez lekarza. Nie wszyscy pracownicy medyczni np. pielęgniarki mają dostęp do systemu HIS. Dostęp do systemu przyznawany jest na podstawie wniosków kierowników komórek organizacyjnych i wynika z zakresów obowiązków, a także z samej organizacji pracy na poszczególnych oddziałach. Jeżeli chodzi o grupę pielęgniarek to nie realizują one w systemie HIS wszystkich swoich czynności. Większość dokumentów tworzona jest przez tą grupę zawodową w formie papierowej." Stopniowo Szpital planuje wprowadzać rozwiązania, które pozwolą na tworzenie dokumentacji pielęgniarskiej w formie elektronicznej.

(akta kontroli str. 509 do 513, 516 do 518)

Analiza przeprowadzona na próbie 30 (z 414)[22] pielęgniarek i położnych zatrudnionych w Szpitalu wykazała, że dostęp w systemie HIS do danych medycznych pacjentów posiadało 13 z nich. Posiadały one dostęp do danych pacjentów z oddziałów/poradni w których świadczyły pracę. Wszystkie 30 osób posiadało w swoich aktach osobowych potwierdzenia nadania im przez ADO pisemnych upoważnień do przetwarzania danych osobowych.

(akta kontroli str. 203 do 210, 250 do 260, 268)

IOD wyjaśnił, że przyjęto zasadę wydawania upoważnień dla osób zatrudnionych m.in. jako sanitariusze z uwagi na czynności wiążące się z dostępem do wybranej dokumentacji medycznej, tj.: skierowanie na badanie, wynik badania, dokumentacja związana z przyjęciem do Szpitala. Dostęp do tych dokumentów (prowadzonych w Szpitalu w formie papierowej) jest niezbędny do wykonania pracy zgodnie z zakresem czynności. W tym m.in. transportu chorych na badania, zaprowadzania pacjenta przyjętego na dany oddział.

(akta kontroli str. 514)

Dyrektor wyjaśniła, że system HIS „jest wykorzystywany w Szpitalu jako narzędzie wspomagające tworzenie dokumentacji medycznej. Na dzień udzielania wyjaśnień nie

[20] MLS SOFTWARE - system typu HIS (Hospital Information System – rodzaj oprogramowania do obsługi ruchu pacjentów wewnątrz podmiotu leczniczego).

[21] Według stanu na 10 stycznia 2019 r.

[22] stan na 28 lutego 2019 r.

tworzy dokumentów elektronicznych w myśl Rozporządzenia Ministra Zdrowia o EDM. Dokumentacja jest drukowana z systemu, a następnie autoryzowana przez odpowiednie osoby np. lekarzy. Dotyczy to również skierowań na badania obrazowe, które pomimo ich elektronicznej formy nie są same w sobie dokumentem medycznym. Na podstawie Rozporządzenia Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania, każde skierowanie jest drukowane i opatrzone zarówno podpisem, jak i pieczątką lekarza oraz opatrzone datą dokonania wpisu. Ponadto musi być przechowywane wraz z wynikiem w dokumentacji Zakładu Diagnostyki Obrazowej. Jego forma elektroniczna jest przesyłana pomiędzy poszczególnymi komórkami Szpitala i w dużej mierze ułatwia korzystanie z systemu. Na przykład tworzy kolejki (listy) skierowanych na badania na poszczególnych urządzeniach obrazowych. Również dokumentacja tworzona przy przyjęciu pacjenta musi zostać wydrukowana i zaopatrzona w odpowiednie podpisy i pieczątki, zarówno ze strony pacjenta jak i lekarza. Zatem mając na uwadze powyższe oraz fakt, że w przypadku wykonywania przez niższy personel medyczny (sanitariusze, salowe, opiekunowie medyczni) zadań zgodnych z zakresem ich czynności, podczas realizacji tych zadań zachodzi przetwarzanie danych osobowych pacjentów (wgląd m.in. do danych osobowych pacjentów na skierowaniu do badania i wyniku badania, dokumentacji przy przyjęciu pacjenta do Szpitala), konieczne było nadanie upoważnień do przetwarzania danych osobowych spełniając tym samym wymóg art. 29 RODO. Szpital wykorzystuje wszystkie moduły systemu HIS [przyp. kontr.]. Skala ich wykorzystanie zależy od poszczególnych oddziałów i jest stale rozszerzana. W obecnej chwili trwają prace na przystosowaniu i wdrożeniu dokumentacji elektronicznych wymaganych przez odpowiednie przepisy i zarządzenia."

(akta kontroli str. 512 do 513, 517 do 518)

2.4. W okresie od 25 maja 2018 r. do 31 grudnia 2018 r. Szpital rozwiązał stosunek pracy z 122 osobami. Przy czym 18 pracowników, spośród analizowanych 30, w trakcie zatrudnienia miało przyznany dostęp do systemów informatycznych, w tym do systemu HIS. Przeprowadzona analiza terminu odebrania im tych uprawnień wykazała, że:

- w 11 przypadkach dostęp do systemu HIS odebrano przed lub w ciągu trzech dni od rozwiązania stosunku pracy (tj. w pierwszym dniu roboczym po ustaniu zatrudnienia),
- w siedmiu przypadkach nie odebrano dostępu mimo rozwiązania stosunku pracy (każda z tych osób nadal świadczyło pracę na rzecz Szpitala na podstawie innych form zatrudnienia, np. udzielania świadczeń w ramach pełnienia dyżurów medycznych, umowy kontraktowej na udzielanie świadczeń zdrowotnych).

Upoważnienie do przetwarzania danych osobowych wygasało automatycznie wraz z rozwiązaniem stosunku pracy, co zostało zapisane w przyjętym formularzu.

(akta kontroli str. 290 do 389, 407)

IOD wyjaśnił, że konta aktywne należały do osób nadal zatrudnionych w Szpitalu w oparciu o inne formy zatrudnienia (m.in. udzielania świadczeń w ramach pełnienia dyżurów medycznych, umowy kontraktowej na udzielanie świadczeń zdrowotnych, kolejnej umowy o pracę). Ponadto podał, że powodem takiego stanu rzeczy był niewłaściwie sformułowany zapis zawarty w treści upoważnienia do przetwarzania danych osobowych (skutkował odebraniem uprawnień pomimo zmiany charakteru zatrudnienia, np. przez lekarzy na zasadzie pełnienia dyżuru).

(akta kontroli str. 506 do 508, 519 do 521)

2.5. Zgodnie z umowami zgłaszanie błędów w działaniu systemów HIS i ERD mogło być dokonywane telefonicznie lub mailowo[23]. Kierownik Działu IT oświadczył, że w myśl postanowień umów serwisowych dla systemu HIS i ERP[24], Szpital obowiązany był do zgłaszania błędów w działaniu systemów telefonicznie i/lub pocztą elektroniczną. W Szpitalu przyjęto zasadę dokonywania zgłoszeń telefonicznych.

[23] „Zamawiający może dokonać zgłoszenia telefonicznie pod następującym numerem telefonu".

[24] Zintegrowany systemem zarządzania przeznaczony do obsługi informatycznej przedsiębiorstw (m.in. kadry i płace).

W Szpitalu nie ewidencjonowano zgłoszeń telefonicznych także w przypadku usterki krytycznej, błędu krytycznego. W czasie kontroli nie stwierdzono przypadku przekazania danych osobowych pacjentów Szpitala. Zgodnie z oświadczeniem Kierownika Działu IT zgłoszenie odbywało się z podaniem nr ID i rodzaju błędu (w miesiącu lutym cztery zgłoszenia mailowe, dodatkowo oprócz 20 telefonicznych, które dotyczyły drobnych poprawek w systemie HIS). Ponad to podał, że podstawowe grupy zdiagnozowanych problemów obejmowały:

1. interwencje związane z działaniem SQL-Serwera (motor bazy danych),
2. interwencje związane z funkcjonalnością składowych systemu HIS,
3. interwencje naprawcze związane z błędami użytkowników.

(akta kontroli str. 475, 463, 501 do 504)

2.6. Szpital zawierał pisemne umowy powierzenia przetwarzania danych osobowych. Określały one przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, a także obowiązki i prawa administratora zgodnie z art. 28 RODO.

Szpital wystąpił jako podmiot powierzający przetwarzanie danych (ADO) w 51 spośród 60 zawartych umów, a w 9 jako podmiot przetwarzający. Umowy powierzenia przetwarzania danych Szpital zawierał m.in. w przypadku: zewnętrznego serwisu oprogramowania oraz urządzeń medycznych (posiadających wewnętrzne nośniki danych), korzystania z komercyjnych serwerów poczty elektronicznej, serwisu systemu monitoringu wizyjnego, udzielania świadczeń zdrowotnych (m.in. w zakresie: usług laboratoryjnych, diagnostyki obrazowej, badań histopatologicznych, badań konsultacyjnych, opieki lekarskiej na oddziałach i poradniach, pełnienia dyżurów medycznych na oddziałach, nocnej i świątecznej opieki zdrowotnej, wysokospecjalistycznego transportu o charakterze reanimacyjnym), w tym posiadania innych umów outsourcingowych dotyczących: przekazywania dawkomierzy pracowników do odczytu poziomu promieniowania, usług kurierskich polegających na dowozie przesyłek zwykłych oraz poleconych za zwrotnym potwierdzeniem odbioru, badania sprawozdania finansowego.

(akta kontroli str. 457 do 459)

Analiza pięciu umów dotyczących powierzenia przez Szpital przetwarzania danych osobowych czterem firmom świadczącym usługi serwisowe oraz jednemu lekarzowi, wykazała m.in. że:

- zawierały one wszystkie wymagane postanowienia określone w art. 28 ust. 3 RODO i stanowiły integralną część umowy na świadczenie usług zawartej z danym podmiotem zewnętrznym,
- wskazany zakres danych osobowych, jaki został powierzony przez Szpital podmiotowi zewnętrznemu, wynikał z rodzaju usług jakie zgodnie z umową na ich świadczenie miał na rzecz Szpitala realizować wykonawca.

(akta kontroli str. 460 do 500, 505)

2.7. W okresie objętym kontrolą w prowadzonym rejestrze nie dokonano zapisów, jakoby wystąpiły przypadki naruszenia ochrony danych osobowych ani nie wpłynęły do Szpitala skargi związane z naruszeniem ochrony danych osobowych.

(akta kontroli str. 505)

2.8. W Szpitalu funkcjonowały procedury dotyczące udostępniania dokumentacji medycznej opracowane 25 maja 2018 r. W myśl tych regulacji dokumentację medyczną udostępnia się pacjentowi lub jego przedstawicielowi ustawowemu, bądź osobie upoważnionej przez pacjenta oraz podmiotom określonym w ust. 3 ww. przepisu. Ponadto w procedurze nr 14 wskazano, że udostępnienie tej dokumentacji na zewnątrz Szpitala następuje w przypadku osobistego zgłoszenia się pacjenta lub przedstawienia upoważnienia w jego imieniu. Regulacje wewnętrzne Szpitala nakładały obowiązek prowadzenia ewidencji każdego przypadku udostępnienia dokumentacji medycznej instytucji lub innej osobie niż pacjent.

(akta kontroli str. 204 do 213)

Według stanu na 31 stycznia 2019 r., w prowadzonym przez Szpital wykazie odnotowano 2.334 przypadki udostępnienia dokumentacji medycznej osobom i podmiotom zewnętrznym[25]. W tym pięciokrotnie odmówiono udostępnienia dokumentacji (czterokrotnie z powodu braku upoważnienia, jeden raz z powodu braku podstaw prawnych[26]). Wśród nich w okresie od 25 maja 2018 r. do 31 stycznia 2019 r. odnotowano 728 przypadków udostępnienia tej dokumentacji osobom fizycznym innym niż pacjent, którego udostępniana dokumentacja medyczna dotyczyła. Przeprowadzona analiza prawidłowości udostępnienia dokumentacji w odniesieniu 56 przypadków[27] wykazała, że:

- w 29 przypadkach na 30 dokumentacja medyczna została udostępniona osobom, które posiadały upoważnienie pacjenta do dostępu do tej dokumentacji na podstawie wniosków o jej udostępnienie określonych w przyjętych regulacjach wewnętrznych Szpitala; w jednym przypadku wydano płytę CD poza Działem Statystyki i Dokumentacji Medycznej, co było niezgodne z zasadami przyjętymi w Szpitalu, w dokumentacji odnotowano upoważnienie osoby wnioskującej i jej upoważnienie, a fakt wydania dokumentacji poza ww. Działem został stwierdzony i odnotowany przez pracownika Szpitala,
- w 25 przypadkach, instytucje ubezpieczeniowe, którym udostępniono dokumentację medyczną posiadały upoważnienie pacjenta do dostępu do tej dokumentacji,
- w jednym przypadku nie udostępniono dokumentacji medycznej pacjenta firmie ubezpieczeniowej, która nie przedstawiła upoważnienia w tym zakresie.

(akta kontroli str. 203 do 249, 265 do 266)

IOD wyjaśnił, że przez przeoczenie nie podjęto działań weryfikujących powód wydania płytki CD poza Działem Statystyki i Dokumentacji Medycznej. Ponadto podał, że w trakcie kontroli NIK podjęto przygotowanie procedury regulującej postępowanie pracowników w przypadku wystąpienia takich zdarzeń.

(akta kontroli str. 266)

2.9. Regulacje dotyczące ochrony danych przed ich utratą w wyniku awarii, błędów lub nieuprawnionej modyfikacji zostały opisane w Polityce. W dokumencie określono m.in. zasady: bezpiecznego użytkowania sprzętu IT, dysków i programów; zarządzania uprawnieniami, w tym procedurę rozpoczęcia, zawieszenia i zakończenia pracy; uwierzytelniania w systemach i zarządzania dostępem do nich; zabezpieczenia dokumentacji papierowej z danymi osobowymi; korzystania z Internetu; korzystania z poczty elektronicznej i ochrony antywirusowej; tworzenia, przechowywania i testowania kopii bezpieczeństwa. Ponadto określono sposób postępowania w przypadku naruszenia ochrony danych osobowych oraz obowiązek zachowania poufności i ochrony danych osobowych. W okresie objętym kontrolą nie stwierdzono i nie odnotowano przypadku naruszenia ochrony danych osobowych oraz obowiązek zachowania poufności i ochrony danych osobowych. Nie stwierdzono przechowywania w komputerach dokumentów zawierających dane osobowe bądź medyczne. Komputery posiadały niezablokowane porty USB, aktualne programy antywirusowe z zaktualizowaną bazą sygnatur wirusów natomiast konta użytkowników posiadały niewłaściwe (nadmierne) uprawnienia w dostępie do systemu operacyjnego.

Każdy z komputerów wymagał logowania przy użyciu nazwy użytkownika (jednego dla każdego komputera) i hasła do systemu operacyjnego (tego samego dla kilku osób). Zainstalowany na komputerach w dyżurkach lekarskich system HIS wymagał dodatkowego zalogowania się (poza zalogowaniem się do systemu operacyjnego) już indywidualnym identyfikatorem użytkownika i hasłem niezależnym od hasła używanego do logowania się do systemu operacyjnego (silne hasło, którego zmiana była wymuszana co 30 dni). Po 30 minutach bezczynności system automatycznie wylogowywał użytkownika

(akta kontroli str. 390 do 406, 408 do 409, 501 do 504)

[25] udostępnienie w okresie od 25 maja 2018 r. do 31 stycznia 2019 r.
[26] Grodzki Urząd Pracy.
[27] 30 udostępnień osobom fizycznym innym niż pacjent i 26 wniosków o udostępnienie firmom ubezpieczeniowym.

Przeprowadzone oględziny serwerowni Szpitala wykazały, m.in. że:

- zabezpieczono dostęp do tego pomieszczenia stosując drzwi metalowe, ale nie przeciwwłamaniowe, pomieszczenie nie posiadało okien;
- zamontowano system alarmowy oraz przeciwpożarowy;
- w pomieszczeniu umieszczono gaśnicę oraz układ klimatyzacji;
- wszystkie serwery zamontowano w specjalnie do tego przystosowanych szafach RACK.

Ponadto w Szpitalu na wypadek czasowego zaniku zasilania zastosowano układy podtrzymujące napięcie UPS i generator.

(akta kontroli str. 24 do 43)

Kopie zapasowe baz danych Szpitala, w myśl przepisów § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI oraz postanowień instrukcji, były przechowywane w zamykanym pomieszczeniu znajdującym się w innej niż serwerownia części budynku.

(akta kontroli str. 275 do 281)

Kierownik Działu IT wyjaśnił, że kopie systemu HIS wykonywane były automatycznie dwukrotnie na dobę (kopie przyrostowe baz danych) a testy odtworzeniowe backupu „wykonywane były na bieżąco przez producenta systemu w ramach umowy o asyście techniczne". Kopie systemu ERP [przyp. kontr.] wykonywane były automatycznie od wtorku do soboty". Ponadto podał, że przyrosty środowiska systemu i bazy danych kopiowane były na płyty DVD na koniec każdego miesiąca.

(akta kontroli str. 409)

Przeprowadzone oględziny 30 komputerów stacjonarnych Szpitala, w tym 20 wykorzystywanych na oddziałach Szpitala przez lekarzy, pielęgniarki i położne przy wykonywaniu ich obowiązków służbowych oraz 10 użytkowanych w dziale Administracji Szpitala wykazały m.in., że:

- na wszystkich zainstalowany był program antywirusowy posiadający aktualną wersję bazy sygnatur wirusów,
- porty USB umożliwiały podłączenie do nich nośników pamięci i kopiowanie danych,
- na wszystkich użytkownicy posiadali niewłaściwe uprawnienia w systemie operacyjnym, które pozwalały na wprowadzanie zmian w konfiguracji tych urządzeń oraz instalację oprogramowania,
- 20 komputerów, na których pracowali lekarze lub pielęgniarki[28] i 10 użytkowanych przez pracowników administracyjnych zarządzanych było przy użyciu domeny,
- 20 komputerów wykorzystywanych było do przetwarzania danych medycznych w systemie HIS (komputery lekarzy na oddziałach), kolejne 10 do przetwarzania danych osobowych pracowników Szpitala (system ERD),
- dostęp do systemu operacyjnego wymagał podania loginu i hasła, przy czym na każdym komputerze z tych samych danych uwierzytelniających korzystało kilku użytkowników, a hasła nie posiadały odpowiedniej złożoności i nie podlegały okresowej zmianie; dostęp do systemu HIS wymagał dodatkowego zalogowania się silnym hasłem na konto użytkownika, system automatycznie wylogowywał użytkownika po 30 minutach braku aktywności.
- wśród dodatkowo skontrolowanych 30 komputerów pracowników niemedycznych Szpitala 12 funkcjonowało poza domeną; także te komputery wyposażone w system operacyjny posiadały aktualny system antywirusowy (z aktualną bazą sygnatur wirusów), i używano jednego , wspólnego użytkownika do logowania dla wszystkich pracowników danej komórki organizacyjnej.

(akta kontroli str. 250 do 260, 436 do 456, 515)

[28] Pielęgniarki oddziałowe lub ich zastępczynie

W Szpitalu posiadano 11 komputerów przenośnych, na których nie stosowano ochrony kryptograficznej nośników pamięci (dysków twardych).

(akta kontroli str. 267)

Stwierdzone nieprawidłowości

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

1. W Szpitalu przyjęto nieprawidłową zasadę dostępu do systemu operacyjnego przez użytkowników (pracowników Szpitala):

- na podstawie z tych samych danych uwierzytelniających (tego samego loginu i hasła);
- niestosowanie haseł o odpowiedniej złożoności i okresowej zmianie;
- pozostawienie niewłaściwych uprawnień pracownikom do systemów operacyjnych komputerów.

Było to niezgodne z § 20 ust. 2 pkt 4 rozporządzenia KRI (odpowiednie uprawnienia), § 20 ust. 2 pkt. 7 lit. c) KRI (wspólne loginy i hasła). Ponadto takie działanie nie zapewnia rozliczalności w systemach teleinformatycznych (§ 21 ust. 1 KRI).

Dyrektor wyjaśniła, że przyjęto system jednego użytkownika z nadanymi uprawnieniami do systemu operacyjnego dla komputerów „ze względu na istniejące ograniczenie techniczne i organizacyjne. Szpital przez wiele lat borykał się z problemami finansowymi i nie dysponował odpowiednią ilością sprzętu komputerowego. Chodzi zarówno o ilość jednostek komputerowych dla poszczególnych oddziałów, jak i serwery Szpitala, które nie były przystosowane do stworzenia odpowiedniego środowiska informatycznego. Ze względu na bardzo małą ilość komputerów, do których dostęp musiało posiadać wiele osób (jeden komputer dla kilku lekarzy) ze względów organizacyjnych i technicznych przyjęto zasadę wspólnego konta do systemu operacyjnego.(…) W ostatnim roku dzięki środkom pochodzącym z dotacji Gminy Miejskiej Kraków, Szpital wymienił przestarzały sprzęt i jest w trakcie reorganizacji systemów informatycznych, które pozwolą na wprowadzenie jednolitego systemu indywidualnych kont użytkowników, umieszczonych w domenie [przyp. kontr.]. Zakupiono również rozwiązania, które pozwolą na centralne zarządzanie zasobami softwarowymi i sprzętowymi użytkowników”.

(akta kontroli str. 512 do 513)

2. W posiadanych w Szpitalu 11 komputerach przenośnych nie stosowano rozwiązania polegającego na szyfrowaniu danych zgromadzonych na tych komputerach, co stanowiło naruszenie § 20 ust. 2 pkt 8 i 9 rozporządzenia KRI.

Kierownik Działu Informatyki wyjaśnił, że nie wprowadzono na nich dodatkowej ochrony kryptograficznej ponieważ w Szpitalu przyjęto „bezwzględną zasadę nie wynoszenia laptopów poza teren Szpitala”.

(akta kontroli str. 409)

OCENA CZĄSTKOWA

W ocenie NIK wdrożone w Szpitalu rozwiązania techniczne i organizacyjne nie zapewniają w pełni prawidłowego przetwarzania i ochrony danych osobowych.

Wprawdzie w okresie objętym kontrolą Szpital w sposób prawidłowy zawarł umowy powierzenia przetwarzania danych, które zawierały wymagane przez RODO postanowienia. W sposób właściwy udostępniano dokumentację medyczną pacjentów oraz podejmowano pewne działania w celu minimalizacji ryzyka utraty danych osobowych w wyniku awarii, błędów lub nieuprawnionej modyfikacji. Wdrożone przez Szpital rozwiązana tylko częściowo zapewniają prawidłowe przetwarzanie i ochronę danych osobowych. NIK negatywnie ocenia przyjęte rozwiązania techniczne i organizacyjne, które mogły spowodować dostęp do danych osobowych pacjentów osób nieuprawnionych, w szczególności nieprawidłowym jest, zdaniem NIK, pozostawienie użytkownikom systemów operacyjnych nie właściwych uprawnień do systemów operacyjnych oraz nieszyfrowanie posiadanych 11 urządzeń przenośnych.

Nienadawanie indywidualnych danych do autoryzacji w systemach operacyjnych wszystkim użytkownikom komputerów oraz założenie pracy kilku osób na jednym koncie użytkownika nie zapewniało[29] środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji, tj. było niezgodne m.in. z § 20 ust. 2 pkt 7 lit. c rozporządzenia KRI.

IV. Wnioski

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

Wnioski

1) zamieszczenie stosownych informacji o IOD na stronie internetowej Szpitala;
2) wdrożenie scentralizowanego systemu zarządzania użytkownikami poprzez nadanie indywidualnych danych do autoryzacji w systemach operacyjnych wszystkim użytkownikom komputerów oraz wprowadzenie rozwiązań uniemożliwiających pracę kilku osób na jednym koncie użytkownika ze stosownymi uprawnieniami dostępu do systemu operacyjnego;
3) zastosowanie szyfrowania danych zgromadzonych na przenośnych komputerach.

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 Krakowie. 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 21 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.

Kraków, kwietnia 2019 r.

Kontroler:
Małgorzata Kram
specjalista kontroli państwowej

[29] – jeden z elementów zarządzania bezpieczeństwem informacji, zmierzającym do zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami