NAJWYŻSZA IZBA KONTROLI

Delegatura w Olsztynie

LOL.411.5.3.2023

Mirosław Gorbaczewski
Dyrektor
Szpitala Miejskiego św. Jana Pawła II
w Elblągu,
ul. Jana Amosa Komeńskiego 35,
82-300 Elbląg

WYSTĄPIENIE POKONTROLNE

I/23/003 - Ochrona danych pacjentów przed cyberatakami w podmiotach leczniczych na terenie województwa warmińsko-mazurskiego.

NAJWYŻSZA IZBA KONTROLI
Delegatura w Olsztynie
ul. Artyleryjska 3e, 10-165 Olsztyn
T +48 89 678 82 00, F +48 89 678 82 30
lol@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana

Szpital Miejski św. Jana Pawła II w Elblągu, ul. Jana Amosa Komeńskiego 35, 82-300 Elbląg, dalej: Szpital.

Kierownik jednostki kontrolowanej

Mirosław Gorbaczewski, Dyrektor Szpitala od 20 marca 2019 r., dalej: Dyrektor.

Zakres przedmiotowy kontroli

1. Działania związane z przygotowaniem technicznym i organizacyjnym dotyczącym przetwarzania i ochrony danych pacjentów przed cyberatakami.
2. Funkcjonowanie przyjętych rozwiązań i ich wpływ na ochronę danych pacjentów przed cyberatakami.

Okres objęty kontrolą

Lata 2020-2023 (I półrocze) z uwzględnieniem okresów wcześniejszych i późniejszych, jeżeli miało to wpływ na realizowane zadania.

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 Olsztynie

Kontrolerzy

1. Izabela Kowalska, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LOL/166/2023 z 5 grudnia 2023 r.
2. Beata Saba, specjalista kontroli państwowej, upoważnienie do kontroli nr LOL/146/2023 z 17 listopada 2023 r.
3. Zbigniew Wołodko, doradca techniczny, legitymacja służbowa nr 22213.
4. Bartosz Kościukiewicz, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LOL/173/2023 z 21 grudnia 2023 r.
5. Sebastian Helbrecht, specjalista kontroli państwowej, upoważnienie do kontroli nr LOL/164/2023 z 4 grudnia 2023 r.
6. Artur Żukowski, starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LOL/165/2023 z 5 grudnia 2023 r.

(akta kontroli str. 1-11)

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

W Szpitalu wprowadzono wymagane procedury związane z zapewnieniem bezpieczeństwa informacji, jednak w niektórych przypadkach zawarte w nich postanowienia dotyczące m.in. nadawania uprawnień do przetwarzania danych osobowych, odbierania uprawień do systemów informatycznych, a także stosowania wymaganych zabezpieczeń systemów informatycznych nie były przestrzegane.

Zgodnie z wymogiem określonym w § 20 ust. 1 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności minimalnych

[1] Dz. U. z 2022 r. poz. 623, dalej: ustawa o NIK.
[2] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.

wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[3], wprowadzono kompleksowy system zarządzania bezpieczeństwem informacji określony w Polityce Bezpieczeństwa Informacji[4]. Stosownie do postanowień 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] opracowano i wdrożono w Szpitalu dokumentację oraz procedury dotyczące ochrony danych osobowych. Zapewniono także szkolenia personelowi Szpitala związane z zagadnieniami dotyczącymi bezpieczeństwa danych. Powierzone w ww. Polityce Inspektorowi Ochrony Danych (dalej: IOD) zadania w zakresie nadawania i aktualizacji upoważnień do przetwarzania danych osobowych w systemach informatycznych lub zbiorach w wersji papierowej wykraczały jednak poza katalog zadań określonych w art. 39 RODO. Ponadto, na etapie wdrażania tej Polityki, nie realizowano w sposób rzetelny obowiązku składania przez pracowników Szpitala „oświadczeń użytkownika o zachowaniu poufności informacji", określonego w punkcie 5 rozdziału 15 Polityki. Dotyczyło to 15 pracowników administracji (94% objętych badaniem) i 27 pracowników medycznych (90%).

Personelowi Szpitala zapewniono odpowiedni dostęp do danych medycznych, zgodnie z zajmowanymi stanowiskami. Nie w pełni realizowano obowiązki wynikające z wprowadzonych procedur związanych z ochroną danych osobowych, w tym danych medycznych m.in. w zakresie odbierania uprawnień dostępu do systemów informatycznych oraz korzystania przez pracowników Szpitala z tych systemów. Wystąpiły bowiem przypadki odbierania uprawnień dostępu do systemów informatycznych byłym pracownikom od 4 do aż 691 dni po zakończeniu zatrudnienia. Takie postępowanie nie było rzetelne oraz zgodne z art. 29 oraz art. 32 ust. 4 RODO. W wyniku tego naruszenia dwóch byłych pracowników logowało się do systemu Optimed NXT – szpitalnego systemu medycznego HIS (dalej: system Optimed NXT) po zakończeniu ich pracy w Szpitalu.

Nie w pełni przestrzegano również postanowień przyjętych w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania Danych Osobowych[6]. W trakcie oględzin ustalono bowiem, że:

- dostęp do pulpitu użytkownika (systemu operacyjnego Windows) na stanowiskach medycznych nie wymagał podania danych uwierzytelniających, (co nie było zgodne z wymogiem określonym w rozdziale 5 pkt 3 lit. c Instrukcji),
- porty USB na wszystkich poddanych oględzinom komputerach nie były zablokowane (rozdział 5 pkt 2 lit. e Instrukcji),
- czas bezczynności do automatycznego wylogowania był ustawiony na 15 minut zamiast 5 (rozdział 6 pkt 9 Instrukcji).

Nie przestrzegano także wewnętrznych uregulowań w zakresie nadawania upoważnień do przetwarzania danych osobowych. Według stanu na dzień 14 grudnia 2023 r. 435 pracowników Szpitala posiadało dostęp do takich danych bez nadanych pisemnych upoważnień, co było niezgodne z wymogami określonymi w punkcie 4 rozdziału 10 Polityki Bezpieczeństwa Informacji. Ponadto, wydane w latach 2020-2023 (do 6 listopada 2023 r.) trzy upoważnienia były niezgodne ze wzorem określonym w załączniku nr 5 Instrukcji, zaś w przypadku trzech, tj. 10%

[4] Dz. U. z 2017 r. poz. 2247, dalej: rozporządzenie KRI.
[4] Dalej: Polityka lub PBI.
[5] Dz. Urz. UE L 119 z 4 maja 2016 r., str. 1, ze zm., dalej: RODO lub rozporządzenie RODO.
[6] Dalej: Instrukcja lub IZSI.

(z 30 objętych badaniem) wydane zostały po nadaniu uprawnień w systemie Optimed NXT, co stanowiło naruszenie regulacji wewnętrznych, określonych w rozdziale 10 Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

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

OBSZAR

1. Działania związane z przygotowaniem technicznym i organizacyjnym dotyczącym przetwarzania i ochrony danych o pacjentach przed cyberatakami

Opis stanu faktycznego

1.1. Szpital[8], wg stanu na dzień 23 listopada 2023 r., nie został uznany przez właściwego Ministra za Operatora usług kluczowych (dalej: OUK) na podstawie art. 5 ust.1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[9].

Na stronie internetowej Szpitala zamieszczono informacje dla pacjentów dotyczące zasad i sposobów ochrony danych osobowych określonych zgodnie z art. 13 RODO.

(akta kontroli str. 12-16)

1.2. W Szpitalu opracowano PBI wraz z dokumentem powiązanym, tj. Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych wymaganą w § 20 ust. 2 rozporządzenia KRI. Dokumenty te zostały zatwierdzone przez Dyrektora 25 stycznia 2019 r. i obowiązują od dnia zatwierdzenia. Zastąpiły one Politykę Bezpieczeństwa Informacji wraz z Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych wprowadzoną 30 listopada 2014 r.

Ww. dokumentacja była zgodna z normą PN-EN ISO/IEC 27001, tj. m.in. obejmowała ona ustalenia dotyczące:

- charakterystyki infrastruktury;
- szacowania ryzyka dla obiektów infrastruktury;
- oceny aktualnego stanu ochrony infrastruktury;
- opisu zabezpieczeń infrastruktury.

Wdrożenie w Szpitalu ww. Polityki w 2019 r. przeprowadzono w cyklu szkoleń grupowych, które zostały udokumentowane na listach obecności osób biorących udział w takich szkoleniach. Jednocześnie we wszystkich komórkach organizacyjnych Szpitala prowadzone były listy osób zobowiązanych do przestrzegania procedur określonych w Polityce i IZSI. Listy takie zawierały imię i nazwisko pracownika, jego podpis oraz datę.

W latach 2020-2023 (do 30 października) wdrożenie ww. procedur wśród pracowników nowozatrudnionych polegało na przeszkoleniu łącznie

[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] Samodzielny publiczny podmiot leczniczy, którego podmiotem tworzącym była Gmina Miasto Elbląg. W skład wchodzą: Szpital Miejski, Medyczne Laboratorium Diagnostyczne, Przychodnie Szpitala Miejskiego, Zakład Opiekuńczo-Leczniczy, Zakład Lecznictwa Psychiatrycznego Stacjonarnego z Centrum Zdrowia Psychicznego – część Ambulatorium oraz Zakład Lecznictwa Psychiatrycznego Ambulatoryjnego z Centrum Zdrowia Psychicznego - część Ambulatorium.

[9] Dz. U. z 2023 r. poz. 913, ze zm.

448 pracowników, w tym: 109 w 2020 r., 125 w 2021 r., 114 w 2022 r. oraz 98 w 2023 r. (do 30 października).

(akta kontroli str. 17-124, 331-363)

Badaniem objęto 46 teczek akt osobowych pracowników, w tym: 16 teczek akt osobowych pracowników administracji[10] oraz 30 pracowników medycznych[11].

Analiza ww. teczek 36 pracowników zatrudnionych przed wdrożeniem PBI i 10 po jej wdrożeniu wykazała, że w aktach osobowych:

- jednego pracownika administracji (z 16 objętych badaniem) i trzech pracowników medycznych (z 30 objętych badaniem), zatrudnionych po wprowadzeniu PBI, przechowywane były „oświadczenia użytkownika o zachowaniu poufności informacji" wymagane na podstawie punktu 5 rozdziału 15 PBI oraz określone w § 3 pkt 2 lit. e tiret trzeci rozporządzenia Ministra Rodziny, Pracy i Polityki Społecznej z dnia 10 grudnia 2018 r. w sprawie dokumentacji pracowniczej,
- 15 pracowników administracji (zatrudnionych przed wprowadzeniem PBI) oraz 27 pracowników medycznych[12] (20 zatrudnionych przed wprowadzeniem PBI i siedmiu po jej wprowadzeniu) nie było ww. oświadczeń (opisano w sekcji Stwierdzone nieprawidłowości).

(akta kontroli str. 125-156)

1.3. W rozdziale 3 Polityki wskazano zakres odpowiedzialności pracowników Szpitala za bezpieczeństwo informacji, w szczególności odpowiedzialność i uprawnienia osób pełniących istotną rolę w zapewnieniu bezpieczeństwa informacji. I tak:

- Dyrektor Szpitala (Administrator Danych Osobowych) — odpowiadał za zatwierdzenie instrukcji,
- Inspektor Ochrony Danych — nadzorował stosowanie zapisów instrukcji i okresowo sprawdzał jej aktualność,
- Administrator Systemów Informatycznych[13] (Kierownik Działu informatyki) — nadzorował i sprawdzał stosowanie zapisów instrukcji w codziennej praktyce,
- Ordynatorzy/Koordynatorzy/Kierownicy komórek organizacyjnych odpowiadali za wdrożenie zapisów instrukcji, nadzorowanie przebiegu jej stosowania i przestrzeganie jej postanowień w obrębie swojej komórki organizacyjnej,
- Pracownicy — ochronę danych osobowych realizowano przez wszystkich pracowników Szpitala oraz inne osoby posiadające dostęp do danych osobowych na podstawie innych zasad (stażyści, wolontariusze itp.), przy wykorzystaniu zabezpieczeń fizycznych, procedur organizacyjnych, oprogramowań systemowych, aplikacji itp.

W rozdziale 10 ww. Polityki nadawanie i podpisywanie „upoważnień do przetwarzania danych osobowych w systemach informatycznych lub zbiorach w wersji papierowej", których wzór został określony w załączniku nr 5 IZSI, zostało przypisane IOD. Przypisanie takich uprawnień wykraczało poza zakres obowiązków Inspektora Ochrony Danych określonych w przepisie art. 39 ust. 1 RODO, co opisano w sekcji Stwierdzone nieprawidłowości.

(akta kontroli str. 17-63)

[10] Z czego 15 pracowników zatrudnionych przed wdrożeniem PBI i jeden po wdrożeniu.
[11] Z czego 20 pracowników zatrudnionych przed wdrożeniem PBI i 10 po wdrożeniu.
[12] Objętych badaniem.
[13] Dalej: ASI.

1.4. W Szpitalu określono zasady zarządzania incydentami[14] związanymi z bezpieczeństwem informacji, zarówno w Polityce, jak i w Instrukcji. I tak, w rozdziale 11 Polityki zawarto Instrukcję Alarmową, której celem była minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości. Regulacja wskazywała osoby[15], które należy powiadomić w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych oraz zawierała otwarty katalog zdarzeń/sytuacji powodujących zagrożenia bezpieczeństwa danych osobowych[16]. Ponadto w rozdziale 20 IZSI zawarto skróconą instrukcję postepowania w przypadku naruszenia danych osobowych. Regulacja wskazywała osobę[17], którą należy powiadomić w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych oraz zawierała otwarty katalog zdarzeń[18], które należy bezwzględnie traktować jako wymagające zgłoszenia.

(akta kontroli str. 17-108)

1.5. W § 25 pkt 11 rozdziału VII Regulaminu organizacyjnego Szpitala z 8 stycznia 2018 r. w pionie Dyrektora wskazano stanowisko Inspektora Ochrony Danych (dalej: Inspektor lub IOD). W punkcie 34 załącznika nr 4 do ww. Regulaminu doprecyzowano zakres jego obowiązków służbowych. Zakres zadań przypisanych IOD zawierał czynności określone w art. 39 RODO, tj. m.in.:

- informowanie ADO oraz pracowników, którzy przetwarzają dane osobowe o obowiązkach spoczywających na nich na mocy przepisów o ochronie danych i doradzanie im w tych sprawach,
- składanie kierownictwu rocznego raportu dotyczącego prowadzonych działań,
- opracowanie wewnętrznych zasad i procedur zapewniających w tym zakresie wydajny i szybki przepływ informacji dotyczących ochrony danych,
- prowadzenie szkoleń pracowników w zakresie ochrony danych,
- udzielanie zaleceń dotyczących oceny skutków dla ochrony danych oraz monitorowanie ich wykonania.

(akta kontroli str. 157-212)

IOD do 22 maja 2018 r. pełnił obowiązki Administratora Bezpieczeństwa Informacji, posiadając wykształcenie techniczne, 42-letnie doświadczenie w zakresie informatyki oraz odbyte kursy i szkolenia dotyczące ochrony danych osobowych[19].

---

[14] Zdefiniowane w Polityce Bezpieczeństwa Informacji jako naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność.

[15] Inspektor Ochrony Danych i Administratora Danych Osobowych (dalej: ADO).

[16] Do typowych sytuacji należały sytuacje związane z nieprzestrzeganiem zasad ochrony danych osobowych przez pracowników, w szczególności: niestosowanie zasady czystego biurka, ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek, a także nieprzestrzeganie zakazu zachowania tajemnicy danych osobowych przez pracowników Szpitala i ujawnienie tych danych.

[17] IOD.

[18] Tj.: a) ślady na drzwiach oknach i szafach wskazują na próbę włamania.
b) dokumentacja jest niszczona bez użycia niszczarki.
c) fizyczna obecność budynku lub pomieszczeniach osób zachowujących się podejrzanie.
d) otwarte drzwi do pomieszczeń szaf, gdzie przechowywane są dane osobowe.
e) ustawienie monitorów pozwala na wygląd osób postronnych na dane osobowe.
f) wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez upoważnienia IOD.
g) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej.
h) telefoniczne próby wyłudzenia danych osobowych.
i) kradzież komputerów lub CD twardych dysków pendrive z danymi osobowymi.
j) maile zachęcające do ujawnienia identyfikatora i lub hasła.
k) pojawienie się wirusa komputerowego lub niestandardowa. Zachowanie komputerów.
l) hasła do systemów przyklejany są w pobliżu komputera.

[19] Szkolenie przeprowadzone: 20 lutego 2017 r. – ochrona danych osobowych dla ABI, 26 września 2017 r. – obowiązujące krajowe przepisy prawne, dotyczące systemu ochrony danych osobowych w powiązaniu z nowymi

Dane IOD oraz sposób i formę kontaktu, udostępniono na stronie internetowej Szpitala — spełniając tym samym wymóg określony w art. 37 ust. 7 RODO.

(akta kontroli str. 213-218)

1.6. W latach 2020-2023 (do 30 października) zapewniono personelowi Szpitala szkolenia dotyczące m.in. bezpieczeństwa danych. I tak, przeszkolono łącznie 309 osób, z czego w: 2020 r. 64 pracowników, 2021 r. – 88, 2022 r. – 112 oraz 2023 r. (do 30 października) – 45 pracowników.

Szkolenia te obejmowały m.in. ogólną charakterystykę aktów prawnych w zakresie ochrony danych osobowych, praktyczne aspekty stosowania przepisów związanych z ochroną danych osobowych (polityka czystego biurka, logowanie do systemu, polityka kluczy), cyberbezpieczeństwo – charakterystyka zagrożeń wynikających z użytkowania poczty elektronicznej, cyberhigiena w codziennych zadaniach i obowiązkach.

Dyrektor wyjaśnił, że dodatkowo pracownicy mieli stały dostęp do wszystkich wewnętrznych regulacji Szpitala, znajdujących się w folderze „Zarządzenia", zlokalizowanym na każdym pracowniczym stanowisku komputerowym. Dokumenty udostępnione w wewnętrznej sieci – Intranet, były na bieżąco aktualizowane. System ten stanowił bazę aktów prawnych, mających zastosowanie w pracy Szpitala.

(akta kontroli str. 219-244, 331-363)

1.7. W okresie objętym kontrolą Szpital uzyskał dofinansowanie na dwie inwestycje poprawiające bezpieczeństwo infrastruktury teleinformatycznej. Łączna wartość tych projektów wg umów wynosiła 3159,6 tys. zł, z czego kwota dofinansowania to 2737,9 tys. zł. Wydatki Szpitala na zrealizowane projekty wyniosły 3149,4 tys. zł, zaś uzyskana kwota dofinansowania to 2728,4 tys. zł.

I tak, w latach 2020-2021 Szpital zrealizował projekt w ramach działania 3.2. „E-zdrowie" Regionalnego Programu Operacyjnego Województwa Warmińsko-Mazurskiego na lata 2014-2020 „Cyfrowy Region", współfinansowanego ze środków Europejskiego Funduszu Rozwoju Regionalnego[20]. Wydatki Szpitala na zrealizowanie tego projektu wyniosły 2755,6 tys. zł, z czego uzyskana kwota dofinansowania to 2334,5 tys. zł. Na pokrycie wkładu własnego zawarto umowę[21] z Gminą Miasto Elbląg na kwotę 502,6 tys. zł. Wydatki w ramach umowy wyniosły 303,9 tys. zł.

Projekt polegał na wdrożeniu e-usług w Szpitalu i został zrealizowany w sześciu etapach, tj. m.in. w zakresie: rozbudowy serwerowni o niezbędną infrastrukturę na potrzeby wdrożenia e-usług oraz wdrożenia tych e-usług, w tym: e-rejestracji pacjentów, e-wyników, e-recepty, e-zlecenia i e-skierowania. W wyniku przeprowadzonych prac unowocześniono zaplecze techniczne, tj. sprzęt informatyczny oraz poprawiono bezpieczeństwo działania systemów informatycznych wraz z zapewnieniem bezpieczeństwa informacji medycznych. W ramach projektu pn.

wymaganiami rozporządzenia PE, 23 października 2018 r. – Bezpieczeństwo danych i infrastruktury IT w placówkach medycznych, 24 października 2019 r. – Absurdy RODO oraz kurs ochrony danych osobowych i obsługa pacjenta w świetle RODO odbyty 18 listopada 2019 r.

[20] Umowa Nr RPWM.03.02.00-28-0027/18-00 z 28 marca 2019 r. zawarta z Województwem Warmińsko-Mazurskim.

[21] Nr DZiSS/32/2019 z 1 października 2019 r.

Wdrożenie e-usług, Szpital zakupił sprzęt komputerowy[22], wartości niematerialne i prawne, usługi wdrożeniowe[23] oraz poniósł koszty związane z pozyskaniem dotacji[24].

Drugą inwestycję Szpital przeprowadził w 2022 r. na podstawie umowy zawartej z Narodowym Funduszem Zdrowia[25] (dalej: NFZ) o finansowanie ze środków pochodzących z Funduszu Przeciwdziałania covid-19 podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniobiorców. Wartość projektu określono w ww. umowie na kwotę 400 tys. zł, zaś wydatkowano 393,9 tys. zł. Całość inwestycji została sfinansowana przez NFZ. W ramach tego projektu Szpital zakupił sprzęt komputerowy[26], wartości niematerialne i prawne[27] oraz usługi wdrożeniowe i audytowe[28].

(akta kontroli str. 245-327)

Stwierdzone nieprawidłowości

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

1. W przypadku 15 pracowników administracji[29], tj. 94% (z 16 objętych badaniem) oraz 27 pracowników medycznych, tj. 90% (z 30 objętych badaniem), wg stanu na dzień 17 stycznia 2024 r., nie wyegzekwowano obowiązku złożenia przez nich oświadczeń użytkownika o zachowaniu poufności informacji, o których mowa w punkcie 5 rozdziału 15 Polityki. Określono w nim, że: „po szkoleniu lub zapoznaniu się z polityką ochrony danych osobowych, użytkownik zobowiązany jest do podpisania Oświadczenia użytkownika o zachowaniu poufności informacji (wzór wg załącznika nr „I" PBI)".

Jak wyjaśnił Dyrektor, że przyczyną powyższej nieprawidłowości było przeoczenie IOD.

(akta kontroli str. 125-156, 364-367)

2. W rozdziale 10 Polityki Bezpieczeństwa Informacji, wprowadzonej 25 stycznia 2019 r., nadawanie i podpisywanie „upoważnień do przetwarzania danych osobowych w systemach informatycznych lub zbiorach w wersji papierowej", których wzór został określony w załączniku nr 5 IZSI, zostało przypisane IOD. Wskazane wyżej zadania wykraczają natomiast poza zakres zadań określonych w art. 39 ust. 1 rozporządzenia RODO, a ich realizacja faktycznie powodowałaby naruszenie zasad sprawowania funkcji IOD. Jednym z zadań IOD jest bowiem monitorowanie przestrzegania rozporządzenia RODO, innych przepisów prawa oraz Polityki. Podejmowanie decyzji

[22] Macierz PowerVault MD3400, 12G SAS, Fortigate -201E Hardware plus 1 Year 8*5 FortiCare and FortiGuard UTM Budle wraz z usługą wdrożeniową, zestaw komputerowy, repozytorium EDM:SERWER HPE PROLIANT DL360 (2 szt.) z macierzą z dwoma serwerami, dysk sieciowy NAS Synology RS820+ z dyskami WD102KRYZ, switch Hpe FlexNetwork, zasilacze, fortigate 201E, komputer-serwer aplikacyjny power Edge, budowa instalacji sieci Lan i zasilania komputerów.

[23] Projekt sieci teleinformatycznej, licencja dostępowa dla 50 klientów, licencja do oprogramowania do back-up, licencja - oprogramowanie dziedzinowe, bazodanowe do realizacji e-usług oraz elektronicznej dokumentacji medycznej.

[24] Studium wykonalności, nadzór nad projektem, promocja projektu.

[25] Nr 6/2022 z 13 czerwca 2022 r.

[26] Serwer typu I DL380G10PLUS/XEON SILVER, serwer typu I DL380G10PLUS/XEON SILVER, serwer typ II (do backupu) HPE DL380G10PLUS/XEON SILVER, serwerowy system operacyjny - oprogramowanie (licencja) Microsoft Windows SERVER 2022 Standard 16, serwerowy system operacyjny - oprogramowanie (licencja) Microsoft Windows SERVER 2022 Standard 16, serwerowy system operacyjny - oprogramowanie (licencja) Microsoft Windows SERVER 2022 Standard 16, licencja na oprogramowanie (system) do backupu VEEAN BACKUP Essebtials Universal Perpetual License 5, licencja na oprogramowanie (system) do backupu VEEAN BACKUP Essebtials Universal Perpetual License 5, macierz dyskowa HPE MSA 2060/12x900GB SAS HDD/4x16 GB SW SFP+Transceiver/3YR, licencja bezterminowa open optimed.nxt backup dokumentacji, licencja bezterminowa open optimed.nxt.

[27] Konfiguracja środowiska serwerowego.

[28] Audyt zdarzeń i audyt bezpieczeństwa.

[29] Posiadających dostęp do danych osobowych, w tym medycznych.

w zakresie nadawania lub odbierania upoważnień powodowałoby zatem konflikt interesów, o którym mowa w art. 38 ust. 6 rozporządzenia RODO. IOD oceniałby bowiem zgodność własnych działań z przepisami rozporządzenia.

Jak wyjaśnił Dyrektor, zaistniała sytuacja wynikała z innej interpretacji przepisów.

(akta kontroli str. 17-63, 370-373)

OCENA CZĄSTKOWA

W Szpitalu stworzone zostały odpowiednie rozwiązania organizacyjne i techniczne dotyczące bezpieczeństwa informacji, w tym danych pacjentów. We właściwy sposób wywiązano się z opracowania dokumentacji PBI, tj. z obowiązku, o którym mowa § 20 ust. 2 rozporządzenia KRI. Należy jednak zauważyć, że zadania powierzone ww. Polityce Inspektorowi Ochrony Danych odnoszące się do nadawania i aktualizacji upoważnień do przetwarzania danych osobowych w systemach informatycznych lub zbiorach w wersji papierowej wykraczały poza katalog zadań określonych w art. 39 rozporządzenia RODO, a ich realizacja faktycznie powodowałaby konflikt interesów, o którym mowa wart. 38 ust. 6 tego aktu. Personelowi Szpitala zapewniono szkolenia związane z zagadnieniami dotyczącymi bezpieczeństwa informacji, w tym ochrony danych. W przypadku 15 pracowników administracji i 27 pracowników medycznych nie wyegzekwowano obowiązku złożenia przez nich oświadczeń użytkownika o zachowaniu poufności informacji.

OBSZAR

2. Funkcjonowanie przyjętych rozwiązań i ich wpływ na ochronę danych o pacjentach przed cyberatakami

Opis stanu faktycznego

2.1. W okresie objętym kontrolą w Szpitalu funkcjonowało pięć systemów informatycznych, w tym: system Optimed NXT, Simple.ERP – system finansowo-księgowy, Kamsoft KS-ZZL – system kadrowo-płacowy, ProfLab – system laboratoryjny LIS, Alteris – system radiologiczny RIS/PACS.

(akta kontroli str. 376)

2.2. W Szpitalu od 2016 r. prowadzono ewidencję osób upoważnionych do przetwarzania danych osobowych wymaganą w punkcie 5 rozdziału 10 Polityki. Wzór takiej ewidencji określony został w załączniku nr 6 IZSI. Wg stanu na dzień 6 listopada 2023 r. w Szpitalu wydano 837 upoważnień pracownikom medycznym[30] i 96 pracownikom administracji[31], z czego w okresie 2016-2019 r. (do 25 stycznia 2019 r.) łącznie 540 upoważnień oraz od 26 stycznia 2019 r. do 6 listopada 2023 r. łącznie 393 upoważnienia.

(akta kontroli str. 377-411)

Wg stanu na dzień 23 listopada 2023 r. personel działów administracyjnych[32] Szpitala liczył 71 pracowników. I tak, 14[33] spośród tych pracowników posiadało dostęp do systemu Optimed NXT[34], w tym dwóm pracownikom nadano dodatkowo dostęp do systemów LIS i RIS. W Szpitalu zarządzanie siecią nie odbywało się za pomocą usługi Active Directory. Uprawnienia do systemów zawierających dane medyczne

[30] Z czego w: 2016 r. - 359, 2017 r. - 53, 2018 r. - 57, 2019 r. – 60 (14 do 25 stycznia), 2020 r. - 62, 2021 r. - 85, 2022 r. - 74 oraz do 6 listopada 2023 r. – 87.

[31] Z czego w: 2016 r. - 51, 2017 r. - 1, 2018 r. - 4, 2019 r. – 6 (1 do 25 stycznia), 2020 r. – 10, 2021 r. - 5, 2022 r. - 10 oraz do 6 listopada 2023 r. – 9.

[32] Dział techniczny-administracja, Dział ewidencji i rozliczeń usług medycznych, Dział finansowo-księgowy, Dział Informatyczny, Dział kadr, Dział zamówień publicznych, Dział marketingu, promocji i programów pomocowych, Dział szkoleń, Sekcja płac, Sekcja BHP oraz samodzielne stanowiska pracy.

[33] Dane uzyskane na podstawie ewidencji upoważnień.

[34] Hospital Information System - rodzaj oprogramowania do obsługi ruchu pacjentów wewnątrz podmiotu leczniczego.

nadawane były tym osobom na podstawie, wymaganych w punkcie 4 rozdziału 10 Polityki, „upoważnień do przetwarzania danych osobowych w systemach informatycznych lub zbiorach w wersji papierowej" (dalej: upoważnienia), których wzór został określony w załączniku nr 5 IZSI.

(akta kontroli str. 412-414)

Analiza 14 upoważnień pracowników administracji, którym nadano dostęp do danych medycznych (wszystkich, których ujęto w ewidencji) wykazała, że:

- 13 upoważnień[35] było wydanych 2 grudnia 2016 r. i jedno[36] - 1 czerwca 2018 r.
- we wszystkich upoważnieniach (14) w sposób ogólny określono zakres uprawnienia do przetwarzania danych osobowych wykorzystywany w ramach obowiązków realizowanych na zajmowanym stanowisku. Po wprowadzeniu z dniem 25 stycznia 2019 r. nowej PBI wymagane było doprecyzowanie tych danych, m.in. z podaniem nazwy systemu informatycznego, do którego nadano upoważnienie. Do aktualizacji upoważnień zobowiązany został IOD na podstawie punktu 3 rozdziału 10 IZSI. Do dnia 14 grudnia 2023 r. nie zaktualizowano ww. upoważnień na podstawie wzoru ujętego w załączniku nr 5 IZSI, co opisano w sekcji Stwierdzone nieprawidłowości,
- wszystkie upoważnienia zostały podpisane przez ADO.

Analiza teczek akt osobowych tych pracowników wykazała, że nie przechowywano w nich ww. uprawnień.

(akta kontroli str. 125, 415-440)

W toku kontroli oględzinom poddano pięć stanowisk komputerowych obsługiwanych przez pracowników administracji. W ich wyniku ustalono, że:

- na stanowiskach tych był zapewniony dostęp do systemu operacyjnego Windows oraz systemu Optimed NXT, a dostęp do pulpitu użytkownika (systemu operacyjnego Windows) wymagał podania danych uwierzytelniających,
- liczba znaków we wpisanych przez pracowników hasłach była zgodna z zapisami IZSI i wynosiła od 8 do 13 znaków,
- na wszystkich stanowiskach komputerowych, oprócz konta użytkownika, utworzone było konto administratora zabezpieczone hasłem,
- na komputerach był dostęp do portów USB, co opisano w sekcji Stwierdzone nieprawidłowości,
- wszystkie stanowiska posiadały dostęp do internetu oraz program antywirusowy z aktualną bazą sygnatur antywirusowych,
- nadane w systemie uprawnienia pracownikom objętym badaniem były zgodne z zakresem obowiązków określonym na danym stanowisku.

(akta kontroli str. 441-442)

2.3. Analiza teczek akt osobowych oraz ewidencji upoważnień, wybranych losowo, 30 (z 382) pielęgniarek zatrudnionych w Szpitalu na dzień 23 listopada 2023 r. wykazała, że 11 pracownikom upoważnienia wydano w latach 2020-2023, zaś 19 w latach 2016-2019. I tak:

- w przypadku dziewięciu osób zatrudnionych po wprowadzeniu PBI po 25 stycznia 2019 r. - wydane tym pracownikom upoważnienia[37] nie były zgodne ze wzorem

[35] 1/2016/A, 7/2016/A, 13/2016/A, 14/2016/A, 17/2016/A, 21/2016/A, 23/2016/A, 25/2016/A, 26/2016/A, 35/2016/A, 36/2016/A, 37/2016/A, 38/2016/A.
[36] 2/2018/A.
[37] 398/2021/M, 386/2021/M, 377/2021/M, 421/2022/M, 477/2022/M, 511/2023/M, 367/2020/M, 349/2020/M, 356/2020/M.

określonym w załączniku nr 5 do IZSI, co opisano w sekcji Stwierdzone nieprawidłowości,

- w przypadku dwóch pracowników zatrudnionych przed wprowadzeniem PBI - nadane tym osobom upoważnienia[38] zostały zmienione i wydane po dacie wprowadzenia PBI. Jednak nie były one zgodne z obowiązującym wzorem określonym w IZSI, co opisano w sekcji Stwierdzone nieprawidłowości,
- w przypadku 16 pracowników medycznych - do 15 grudnia 2023 r., nie wydano im pisemnych upoważnień, tj. wbrew wymogom określonym w punkcie 4 rozdziału 10 Polityki Bezpieczeństwa Informacji, zaś przedłożone w trakcie kontroli upoważnienia[39] z lat 2016-2018 (do 10 maja) zostały sporządzone na potrzeby kontroli NIK, co opisano w sekcji Stwierdzone nieprawidłowości,
- w przypadku jednego pracownika w nadanym upoważnieniu[40], w sposób ogólny określono uprawnienia do przetwarzania danych osobowych, tj. w zakresie pełnionych obowiązków na zajmowanym stanowisku, a po wprowadzeniu z dniem 25 stycznia 2019 r. nowej PBI wymagane było doprecyzowanie tych zapisów, m.in. z podaniem nazwy systemu informatycznego, do którego nadano upoważnienie. Do dnia 14 grudnia 2023 r. nie zaktualizowano ww. upoważnienia na podstawie wzoru ujętego w załączniku nr 5 IZSI, co opisano w sekcji Stwierdzone nieprawidłowości,
- w 26 przypadkach uprawnienia do systemu Optimed NXT nadano po uzyskaniu upoważnienia, co było zgodne z procedurą określoną w rozdziale nr 10 IZSI,
- w trzech przypadkach upoważnienia[41] były wydane po dacie nadania uprawnień do systemu Optimed NXT. Było to niezgodne z procedurą określoną w rozdziale 10 Instrukcji (opisano w sekcji Stwierdzone nieprawidłowości),
- wszystkie objęte badaniem upoważnienia zostały podpisane przez ADO.

Analiza nadanych w systemie uprawnień 30 pracownikom medycznym objętym badaniem wykazała, że (wg stanu na dzień 12 stycznia 2024 r.) dostęp do danych medycznych pacjentów w systemie Optimed NXT był zgodny z zakresem obowiązków określonych w umowie/kontrakcie.

(akta kontroli str. 142, 443-519)

Na podstawie analizy ewidencji upoważnień ustalono, że w Szpitalu nie nadawano upoważnień nieuprawnionym grupom pracowników, tj. m.in. sanitariusze, salowe.

W Szpitalu w latach 2020-2023 (I połowa) było zatrudnionych 10 lekarzy z zagranicy[42], z czego dziewięciu posiadało uprawnienia w systemie medycznym Optimed NXT.

(akta kontroli str. 520-524)

Na podstawie analizy 837 upoważnień z lat 2016 – 2023 (do 6 listopada 2023 r.) ujętych w ewidencji tych dokumentów ustalono, że 435 upoważnień (52%), w których zawarto informację, iż zostały one nadane pracownikom Szpitala w latach 2016-2018 (do 10 maja 2018 r.) faktycznie zostały sporządzone dopiero w toku kontroli NIK, co opisano w sekcji Stwierdzone nieprawidłowości.

(akta kontroli str. 377-411, 525-962)

[38] 459/2022/M, 445/2022/M.
[39] 13/2016/M, 131/2016/M, 214/2016/M, 98/2016/M, 227/2016/M, 219/20216/M, 206/2016/M, 237/2016/M, 106/2016/M, 16/2016/M, 232/2016/M, 133/2016/M, 3/2016/M, 212/2016/M, 265/2017/M, 285/2018/M.
[40] 305/2018/M.
[41] 459/2022/M, 445/2022/M, 349/2020/M.
[42] Nie byli w trakcie postępowania nostryfikacyjnego.

2.4. Od 1 stycznia 2022 r. do 30 czerwca 2023 r. 86 osób zakończyło zatrudnienie w Szpitalu. Spośród tych osób, 80 w trakcie zatrudnienia miało przyznany dostęp do systemu informatycznego Optimed NXT. W przypadku dwóch osób dostęp ten został odebrany do dnia zakończenia zatrudnienia, w pozostałych 78 przypadkach od 4 do 691 dni po jego ustaniu (opisano w sekcji Stwierdzone nieprawidłowości).

Badanie wykazało ponadto, że trzy osoby, które posiadały uprawnienia do systemu Optimed NXT, ostatni raz logowały się do niego 825, 667 i 595 dni przed zakończeniem pracy w Szpitalu. Zgodnie z wyjaśnieniami Dyrektora, każdy nowo zatrudniony pracownik medyczny otrzymywał dostęp do systemu informatycznego Optimed NXT.

(akta kontroli str. 964-966)

2.5. Przeprowadzone przez NIK (w dniu 4 stycznia 2024 r.) oględziny 16 stanowisk komputerowych (11 komputerów, pięć terminali) obsługiwanych przez lekarzy i pielęgniarki na izbie przyjęć, oddziale chirurgii ogólnej i onkologicznej z pododdziałem chirurgii ręki oraz oddziale chorób wewnętrznych Szpitala, wykazały m.in., że:

- Na wszystkich stanowiskach był zapewniony dostęp do systemu operacyjnego Windows oraz systemu Optimed NXT.
- Dostęp do pulpitu użytkownika (systemu operacyjnego Windows) na tych stanowiskach nie wymagał podania danych uwierzytelniających, co było sprzeczne z zapisami rozdziału 5 pkt 3 lit. c Instrukcji zarządzania systemem informatycznym służącym do przetwarzania Danych Osobowych[43] (opisano w sekcji Stwierdzone nieprawidłowości).
- Na stanowiskach komputerowych (11 szt.), oprócz konta użytkownika, utworzone było konto administratora zabezpieczone hasłem.
- We wszystkich przypadkach dostęp do systemu Optimed NXT wymagał uwierzytelnienia loginem i hasłem.
- Wprowadzone loginy (zweryfikowane na siedmiu stanowiskach) odpowiadały przypisanym loginom. Liczba znaków wpisanych haseł wynosiła od ośmiu do 11.
- W przypadku ww. siedmiu stanowisk w folderach: pobrane, dokumenty i obrazy nie było plików z danymi osobowymi, zaś w przypadku czterech stanowisk w folderze pobrane znajdowało się od 9 do 265 plików pobranych z Internetu.
- Po zalogowaniu się do systemu Optimed NXT we wszystkich przypadkach zakres uprawnień nadanych w systemie był zgodny z zakresem uprawnień określonych na zajmowanym stanowisku.
- Użytkownicy wszystkich stanowisk korzystali w systemie operacyjnym Windows ze wspólnego konta typu lokalnego.
- Porty USB w terminalach były zablokowane w systemie operacyjnym, zaś na wszystkich komputerach był dostęp do portów USB, co było niezgodne z zapisami rozdziału 5 pkt 2 lit. e Instrukcji (opisano w sekcji Stwierdzone nieprawidłowości).
- Wszystkie stanowiska posiadały dostęp do Internetu oraz program antywirusowy ESET z aktualną bazą sygnatur antywirusowych z 3 i 4 stycznia 2024 r.

W toku oględzin pobrano z systemu ustawienia dotyczące wspólnych parametrów kont użytkowników systemu, tj.:

[43] Z 25 stycznia 2019 r., dalej: Instrukcja.

- czas bezczynności do automatycznego wylogowania został ustawiony na 15 minut, co było sprzeczne z zapisami rozdziału 6 pkt 9 Instrukcji (opisano w sekcji Stwierdzone nieprawidłowości),
- maksymalna liczba błędnych logowań – 5,
- czas ważności hasła – 30 dni,
- minimalna liczba znaków – 8,
- minimalna liczba dużych liter – 1,
- minimalna liczba małych liter – 1,
- minimalna liczba cyfr – 1,
- minimalna liczba znaków specjalnych – 0.

(akta kontroli str. 967-972)

2.6. Z prowadzonej w Szpitalu dokumentacji nie wynikało, aby w okresie objętym kontrolą wystąpiły incydenty zagrażające bezpieczeństwu systemu informacyjnego.

(akta kontroli str. 973-974)

2.7. Szpital w okresie objętym kontrolą zawarł jedną umowę[44] dotyczącą powierzenia przetwarzania danych osobowych. Analiza umowy wykazała m.in., że: zawierała ona wszystkie postanowienia wymagane art. 28 RODO i stanowiła integralną część umowy na świadczenie usług. Zakres danych osobowych powierzonych przez Szpital wynikał z rodzaju usług, które zgodnie z umową miały być realizowane na rzecz Szpitala.

(akta kontroli str. 975-983)

Stwierdzone nieprawidłowości

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

1. Wg stanu na 14 grudnia 2023 r. nie zaktualizowano 15 pisemnych upoważnień[45] (50%) nadanych pracownikom Szpitala w latach 2016-2018, mimo wprowadzenia 25 stycznia 2019 r. nowej Polityki. W upoważnieniach tych w sposób ogólny określono uprawnienia do przetwarzania danych osobowych, tj. w zakresie pełnionych obowiązków na zajmowanym stanowisku. Po wprowadzeniu z dniem 25 stycznia 2019 r. nowej PBI wymagane było natomiast doprecyzowanie ww. zapisów, m.in. z podaniem nazwy systemu informatycznego, do którego nadano upoważnienie. Z dniem 15 grudnia 2023 r., tj. w trakcie kontroli wszystkie upoważnienia zostały zaktualizowane i dostosowane do wymogów określonych we wzorze ujętym w załączniku nr 5 IZSI.

Dyrektor wyjaśnił, że za nadawanie upoważnień odpowiedzialny był IOD. Zostało to określone w rozdziale 10 Polityki Bezpieczeństwa Informacji, wprowadzonej 30 listopada 2014 r., jak i 25 stycznia 2019 r.

(akta kontroli str. 125, 142, 374-375, 415-440, 453-489)

2. Jedenaście upoważnień do przetwarzania danych osobowych wydanych pracownikom medycznym[46] (z 30 objętych badaniem), tj. 37% w okresie 2020-2023 r. (I półrocze) nie było zgodnych ze wzorem określonym w załączniku nr 5 do Instrukcji zarządzania systemem informatycznym służącym do przetwarzania Danych Osobowych, wprowadzonej 25 stycznia 2019 r.

[44] Załącznik do umowy nr ZP/153/2020 z 22 lipca 2020 r.

[45] 1/2016/A, 7/2016/A, 13/2016/A, 14/2016/A, 17/2016/A, 21/2016/A, 23/2016/A, 25/2016/A, 26/2016/A, 35/2016/A, 36/2016/A, 37/2016/A, 38/2016/A, 2/2018/A, 305/2018/M.

[46] 398/2021/M, 386/2021/M, 377/2021/M, 421/2022/M, 477/2022/M, 511/2023/M, 367/2020/M, 349/2020/M, 356/2020/M, 459/2022/M, 445/2022/M.

Dyrektor wyjaśnił, że upoważnienia zostały sporządzone na błędnym wzorze z uwagi na pomyłkę IOD.

(akta kontroli str. 142, 364-373, 453-489)

3. Według stanu na 14 grudnia 2023 r. 435 pracowników Szpitala posiadało dostęp do danych medycznych w systemach informatycznych bez nadanych pisemnych upoważnień, co było niezgodne z wymogami określonymi w punkcie 4 rozdziału 10 Polityki Bezpieczeństwa Informacji. Na podstawie analizy 837 upoważnień z lat 2016 – 2023 (do 6 listopada 2023 r.) ujętych w ewidencji tych dokumentów ustalono, że 435 upoważnień (52%), w których zawarto informację, że zostały nadane pracownikom Szpitala w latach 2016-2018 (do 10 maja 2018 r.) faktycznie zostały sporządzone dopiero w toku kontroli NIK.

IOD zeznał, że z uwagi na fakt, że miał duże luki w dokumentacji lub nie sporządzał upoważnień w ogóle, dokonał tego (tj. sporządził upoważnienia) na potrzeby obecnej kontroli NIK, w listopadzie 2023 r.

Dyrektor wyjaśnił, że upoważnienia powinny być przygotowane przez IOD[47]. Nie miał wiedzy o ich braku. Inspektor Ochrony Danych zapewniał go o prawidłowym prowadzeniu spraw związanych m.in. z nadawaniem upoważnień do przetwarzania danych osobowych dla pracowników Szpitala.

(akta kontroli str. 142, 453-489, 960-961)

4. W trzech przypadkach (z 30 objętych badaniem) upoważnienia były wydane od 371 do 1580 dni po dacie nadania uprawnień do systemu Optimed NXT. Stanowiło to naruszenie regulacji wewnętrznych, określonych w rozdziale 10 Instrukcji, tj. IOD przekazuje upoważnienie informatykowi (ASI) celem nadania identyfikatora oraz uprawnień użytkownika w systemach informatycznych i aplikacjach. Dotyczyło to upoważnień o nr:

- 459/2022/M – data wydania upoważnienia 1 lipca 2022 r. – data nadania uprawnień do systemu Optimed NXT – 4 marca 2018 r.;
- 445/2022/M – data wydania upoważnienia 11 kwietnia 2022 r. – data nadania uprawnień do systemu Optimed NXT – 4 marca 2018 r.;
- 349/2020/M – data wydania upoważnienia 2 czerwca 2020 r. – data nadania uprawnień do systemu Optimed NXT – 28 maja 2019 r.

Jak wyjaśnił Dyrektor, wynikało to z błędów popełnionych przez IOD.

(akta kontroli str. 142,364-367, 453-489)

5. Spośród 80 osób, które w okresie od 1 stycznia 2022 r. do 30 czerwca 2023 r., zakończyły pracę w Szpitalu – 78 (97,5%) dostęp do systemu informatycznego Optimed NXT został odebrany dopiero w okresie od 4 do 691 dni po ustaniu zatrudnienia, z tego 48 osobom dopiero 23 listopada 2023 r., tj. w trakcie kontroli NIK. Takie postępowanie było działaniem nierzetelnym oraz niezgodnym z art. 29 i art. 32 ust. 4 RODO. W przepisach tych określono bowiem, że administrator danych podejmuje działania w celu zapewnienia, by każda osoba fizyczna mająca dostęp do danych osobowych, przetwarzała je wyłącznie na podstawie upoważnienia administratora i na jego polecenie. Jednocześnie zgodnie z art. 5 pkt 1 lit. f RODO dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem,

[47] Zadanie określone w rozdziale 10 Polityki Bezpieczeństwa Informacji, wprowadzonej 30 listopada 2014 r., jak i 25 stycznia 2019 r.

za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

Nieodebranie w odpowiednim czasie uprawnienia do dostępu do sytemu Optimed NXT umożliwiło dwóm osobom zalogowanie się do niego po wcześniejszym ustaniu stosunku pracy. Miało to miejsce odpowiednio: 4 oraz 32 dni po tym zakończeniu stosunku pracy lub kontraktu.

Dyrektor wyjaśnił, że nieodebranie dostępu do systemu medycznego osobom, które zakończyły pracę w Szpitalu, wynikało w jednym przypadku z przeoczenia, natomiast w drugim wskazał, że nastąpiło to po udzieleniu przez IOD jednorazowej zgody.

NIK nie w pełni zgadza się z wyjaśnieniami Dyrektora. Wskazana zgoda została bowiem udzielona 22 sierpnia 2022 r., a z ewidencji logowań do systemu Optimed NXT wynika natomiast, że osoba ta dokonywała tego również wcześniej, a więc przed tą datą m.in. w dniu 1 sierpnia 2022 r. dokonała niepoprawnego logowania (pomyłka w haśle).

(akta kontroli str. 964-966, 984-991)

6. Przeprowadzone w dniu 4 stycznia 2024 r. oględziny wykazały, że pracownicy medyczni Szpitala (lekarze i pielęgniarki) posiadali niezabezpieczony dostęp do systemu Windows, co było sprzeczne z postanowieniami rozdziału 5 pkt 3 lit. c Instrukcji, który stanowił, że dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, ma być zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika (login) oraz hasła.

Dyrektor wyjaśnił, że ze względu na wnioski personelu medycznego dotyczącego optymalizacji czasu obsługi pacjentów, logowanie za pomocą loginu i hasła zostało wyłączone. Nie dokonano zmian w tym zakresie w Instrukcji. Obecnie podejmowane są działania w zakresie zmian w procedurze wewnętrznej.

(akta kontroli str. 967-969, 992-993)

7. W trakcie oględzin ustalono, że nie dokonano blokady portów USB na komputerach Szpitala (w przypadku pracowników medycznych dotyczyło to 11 stanowisk, a pracowników administracyjnych – 5 stanowisk[48]). Obowiązek takiego blokowania portów USB był wymagany zapisami rozdziału 5 pkt 2 lit. e Instrukcji.

Dyrektor wyjaśnił, że ze względu na wnioski personelu medycznego, który używał cyfrowych certyfikatów ZUS przenoszonych na nośnikach USB, odstąpiono od blokady portów. Nie dokonano zmian w tym zakresie w Instrukcji. Obecnie podejmowane są działania w zakresie zmian w procedurze wewnętrznej.

NIK nie podziela wyjaśnień Dyrektora Szpitala, ponieważ w przypadku wczytania na serwer Szpitala cyfrowego certyfikatu ZUS można z niego korzystać do końca jego ważności. Poza tym pięciu pracowników administracyjnych (100% objętych badaniem) również nie posiadało blokady portów USB na stanowiskach.

(akta kontroli str. 967-969, 992-993)

8. Według stanu na 4 stycznia 2024 r., mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych, uruchamiał się po 15 minutach nieaktywności pracy użytkownika, co było niezgodne

[48] Trzech pracowników Działu ewidencji i rozliczeń usług medycznych, po jednym pracowniku z Działu informatyki i Działu kadr.

z postanowieniami rozdziału 6 pkt 9 Instrukcji, w której określono, że blokada taka powinna nastąpić po 5 minutach.

Dyrektor wyjaśnił, że wydłużono czas wylogowywania z 5 do 15 minut ze względu na wnioski personelu medycznego. Wskazał, że praktyka wykazała, że wielokrotne logowanie się w trakcie realizacji świadczeń znacząco wydłużało obsługę pacjentów.

(akta kontroli str. 967-969, 984-987)

OCENA CZĄSTKOWA

NIK negatywnie ocenia funkcjonowanie przyjętych rozwiązań i ich wpływ na ochronę danych o pacjentach. Przetwarzanie danych pacjentów, w niektórych przypadkach, odbywało się w sposób nierzetelny i nieprawidłowy. Nie były bowiem w pełni przestrzegane wymogi określone w Polityce i Instrukcji, m.in. w zakresie nadawania upoważnień, odbierania uprawnień dostępu do systemów informatycznych oraz korzystania przez pracowników Szpitala z tych systemów. Personelowi Szpitala zapewniono odpowiedni dostęp do danych medycznych, zgodnie z zajmowanymi stanowiskami. Wystąpiły jednak także sytuacje, że uprawienia nadawane do systemów medycznych nie były poprzedzone wydaniem upoważnień wymaganych wewnętrznymi uregulowaniami określonymi w punkcie 4 rozdziału 10 Polityki lub wydawano je niegodnie ze wzorem określonym w załączniku nr 5 IZSI. Ponadto nie był rzetelnie realizowany obowiązek odbierania dostępu do systemów informatycznych. Stwierdzono bowiem, że dostęp ten był odbierany dopiero od 4 do aż 691 dni po ustaniu zatrudnienia. Takie postępowania nie było zgodne z postanowieniami określonymi w art. 29 oraz art. 32 ust. 4 RODO. Nieodebranie we właściwym czasie prawa dostępu do systemu umożliwiało w dwóch przypadkach logowanie się do niego byłym pracowników Szpitala.

Wbrew postanowieniom Instrukcji (co wykazały oględziny) nie były blokowane porty USB (na 16 stanowiskach), nie zapewniono mechanizmu automatycznej blokady (po 5 minutach nieaktywności) dostępu do systemu informatycznego służącego do przetwarzania danych osobowych, a pracownicy medyczni posiadali niezabezpieczony dostęp do systemu Windows.

IV. Uwagi i wnioski

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

Wnioski

1. Dokonanie w PBI zmian jej postanowień, odnoszących się do zadań IOD, w celu wyeliminowania konfliktu interesów, stosownie do wymogu określonego w art. 38 ust. 6 RODO.
2. Dokonanie aktualizacji Instrukcji zarządzania systemem informatycznym służącym do przetwarzania Danych Osobowych m.in. w zakresie korzystania z systemów informatycznych.
3. Egzekwowanie składania przez pracowników Szpitala oświadczeń użytkowania o zachowaniu poufności informacji.
4. Stworzenie mechanizmu skutecznego odbierania uprawnień dostępu do systemów informatycznych Szpitala z dniem ustania stosunku pracy/wygaśnięcia kontraktu.

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

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 21 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.

Olsztyn, 19 lutego 2024 r.

Najwyższa Izba Kontroli
Delegatura w Olsztynie
Dyrektor
z up.
Piotr Wanic
Wicedyrektor

.....
podpis

Kontroler
Beata Saba
Specjalista kontroli państwowej

.....
podpis