NAJWYŻSZA IZBA KONTROLI
Delegatura w Olsztynie

LOL.411.5.05.2023

Iwona Chełchowska
Prezes zarządu
Szpital Powiatowy spółka z o. o. w Pasłęku
ul. Kopernika 24A
14 – 400 Pasłęk

WYSTĄPIENIE POKONTROLNE

I/23/003 – Ochrona 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 Powiatowy spółka z o. o. w Pasłęku[1], ul. Kopernika 24A, 14-400 Pasłęk.

Kierownik jednostki kontrolowanej

Iwona Chełchowska, Prezes zarządu[2], od dnia 1 stycznia 2014 r.

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.

(akta kontroli str.5-6)

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[3].

Jednostka przeprowadzająca kontrolę

Najwyższa Izba Kontroli
Delegatura w Olsztynie

Kontrolerzy

1. Leszek Żywucki, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LOL/162/2023 z 30 listopada 2023 r. oraz LOL/1/2024 z 3 stycznia 2024 r.
2. Cezary Kasznicki, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LOL/167/2023 z 5 grudnia 2023 r.
3. Bartosz Kościukiewicz, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LOL/174/2023 z 21 grudnia 2023 r.
4. Zbigniew Wołodko, doradca techniczny, legitymacja nr 22213.

(akta kontroli str.1-4)

II. Ocena ogólna[4] kontrolowanej działalności

OCENA OGÓLNA

Przyjęte rozwiązania m.in. w Polityce bezpieczeństwa pozwoliły m.in. na właściwe wyznaczenie Inspektora Ochrony Danych Osobowych[5] wraz z odpowiednim wskazaniem jego zadań, tj. w sposób określony w Rozporządzeniu 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[6]. Ponadto wewnętrzne uregulowania we właściwy sposób określały też kompetencje Administratora Systemów Informatycznych oraz zasady zarządzania incydentami związanymi z bezpieczeństwem informacji. Zgodnie z przyjętymi umową o dofinansowanie założeniami zrealizowano podniesienie poziomu bezpieczeństwa systemów teleinformatycznych. Jednak funkcjonujące w Szpitalu rozwiązania w zakresie zapewnienia bezpieczeństwa informacji, w tym danych osobowych

[1] Dalej: Szpital.
[2] Dalej: Prezes.
[3] Dz. U. z 2022 r. poz. 623, dalej: ustawa o NIK.
[4] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.
[5] Dalej: IODO.
[6] Dz. Urz. UE L 119 z 4 maja 2016 r., str. 1, dalej: rozporządzenie RODO.

i medycznych pacjentów, nie zostały opracowane w sposób określony w § 20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[7].

Przetwarzanie danych pacjentów odbywało się w sposób prawidłowy, z uwzględnieniem uregulowań wewnętrznych i obowiązujących przepisów prawa, w szczególności rozporządzenia KRI i rozporządzenia RODO. Pracownikom Szpitala we właściwy sposób nadano uprawnienia dostępu w systemach informatycznych. Były one bowiem adekwatne do zakresu nadanych im upoważnień do przetwarzania danych osobowych i wykonywanych obowiązków. Zapewniono skuteczną ochronę bezpieczeństwa informacji stosując do tego właściwe środki sprzętowe i programowe, z których najistotniejszym była usługa Active Directory.

Do dnia 1 lutego 2024 r. nie przeszkolono natomiast 50 pracowników Szpitala z zakresu bezpieczeństwa informacji oraz przepisów rozporządzenia RODO. Niezgodnie z przepisami rozporządzenia RODO, dotyczącymi zasady adekwatności i minimalizacji, odbyło się odbieranie byłym pracownikom dostępu do systemów informatycznych. Dostęp ten został odebrany dopiero po upływie od 2 do 653 dni, licząc od daty rozwiązania stosunku pracy lub umowy cywilnoprawnej.

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

OBSZAR

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

Opis stanu faktycznego

1. Zarządzeniem z dnia 28 maja 2018 r.[9] Prezesa wdrożono w Szpitalu regulacje wewnętrzne dotyczące ochrony danych osobowych, w tym przetwarzanych w systemie informatycznym. Regulacje te dotyczyły Polityki Bezpieczeństwa, Instrukcji Zarządzania Systemem Informatycznym oraz Procedury alarmowej.

Polityka Bezpieczeństwa przetwarzania danych osobowych, w tym w Systemie Informatycznym[10], określała środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych, sposób przepływu tych danych pomiędzy poszczególnymi systemami, zawierała wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, a także tryb postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych, w tym w systemach informatycznych lub kartotekach albo w sytuacji powzięcia podejrzenia o takim naruszeniu. W Instrukcji Zarządzania Systemem Informatycznym[11] określono zasady i tryb postępowania przy przetwarzaniu danych osobowych w systemie informatycznym Szpitala. Procedura alarmowa wskazywała na możliwe zagrożenia

[7] Dalej: Dz.U. z 2017 r. poz. 2247, dalej: rozporządzenie KRI.
[8] Oceny cząstkowe to oceny działalności w poszczególnych obszarach badań kontrolnych. Ocena cząstkowa może być sformułowana jako ocena pozytywna, ocena negatywna albo ocena w formie opisowej.
[9] Nr 5/05/2018.
[10] Dalej: Polityka bezpieczeństwa.
[11] Dalej: Instrukcja zarządzania.

oraz definiowała wiązane z niewłaściwym przetwarzaniem danych osobowych lub ich wyciekiem. Celem było skatalogowanie możliwych uchybień i zagrożeń oraz opisanie procedur działania w przypadku ich wystąpienia, jak również ograniczenie ich powstania w przyszłości.

Ww. regulacje odwoływały się do przepisów rozporządzenia RODO, ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[12] oraz do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych[13].

Regulacje te nie odnosiły się i nie tworzyły Systemu Zarządzania Bezpieczeństwem Informacyjnym[14], określonego w rozporządzeniu w sprawie KRI, ponieważ nie zostały opracowane na podstawie § 20 ust. 1 tego rozporządzenia w sposób określony w § 20 ust. 3 tego rozporządzenia, tj. na podstawie Polskiej Normy PN-ISO/IEC 27001 – Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Systemy zarządzania bezpieczeństwem informacji – Wymagania.

(akta kontroli str.7-58)

2. Według Polityki bezpieczeństwa osobami odpowiedzialnymi za bezpieczeństwo informacji oraz danych osobowych byli:

- IODO, którego zadaniem było sprawowanie nadzoru nad przestrzeganiem obowiązujących zasad bezpieczeństwa danych osobowych (szerzej opisane w punkcie 4 wystąpienia pokontrolnego),
- Administrator Systemu Informatycznego[15] do zadań, którego należało dbanie o bezpieczeństwo oraz utrzymanie ciągłości działania sieci teleinformatycznych oraz systemów i oprogramowania używanego w Szpitalu, a także administrowanie siecią komputerową, uprawnieniami użytkowników i pocztą elektroniczną.

(akta kontroli str.7-24, 56-58)

3. W Szpitalu określono zasady postępowania dotyczące stwierdzania i dokumentowania incydentów w zakresie naruszeń ochrony danych osobowych wymagających analizy i zgłoszenia ich do Prezesa Urzędu Ochrony Danych Osobowych, w tym incydentów zaistniałych w systemie informatycznym Szpitala. W Procedurze Alarmowej skatalogowano możliwe uchybienia i zagrożenia wraz z tabelaryczną instrukcją postępowania. Opisano sposób postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych nakładając na pracowników, posiadających upoważnienie do przetwarzania danych osobowych, obowiązek niezwłocznego ich zgłaszania, jak również wyszczególniono zadania IODO i ASI w przypadku stwierdzenia incydentu. Przewidziano, że uchybienia i zagrożenia będą rejestrowane w Dzienniku Uchybień i Zagrożeń, a szczegółowy ich opis, przyczyny powstania, zaistniałe skutki oraz podjęte działania naprawcze lub zapobiegawcze będą dokumentowane odpowiednio w Protokole Zagrożenia lub Protokole Uchybienia.

(akta kontroli str.7-8, 34-40, 56-58)

4. Z dniem 28 maja 2018 r., zgodnie z wymogami art. 37 ust. 1 rozporządzenia RODO, Prezes Szpitala na podstawie zarządzenia Nr 3/05/2018 utworzyła

[12] Dz. U. z 2019 r. poz. 1781, dalej: ustawa o ochronie danych osobowych.
[13] Dz. U. Nr 100, poz. 1024.
[14] Dalej: SZBI.
[15] Funkcję tę pełnił Informatyk, pełniący równolegle funkcję Administratora Systemu Informatycznego (dalej: ASI).

w strukturze organizacyjnej Szpitala stanowisko IODO. Osoba, będąca z zawodu radcą prawnym, spełniała wymagania określone w art. 37 ust. 5 RODO, tj. posiadała odpowiednie kwalifikacje zawodowe, jak i wiedzę na temat prawa i praktyk w dziedzinie ochrony danych osobowych.

Przypisane zadania i obowiązki IODO były zgodne z katalogiem czynności określonym w art. 39 rozporządzenia RODO, tj. dotyczyły m.in:

- informowania administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia RODO oraz innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie,
- monitorowania przestrzegania RODO, innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podziału obowiązków, działań zwiększających świadomość, szkoleń personelu uczestniczącego w operacjach przetwarzania oraz powiązanych z tym audytów,
- udzielania na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowania jej wykonania zgodnie z art. 35 rozporządzenia RODO,
- współpracy z organem nadzorczym,
- pełnienia funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 rozporządzenia RODO oraz w stosownych przypadkach prowadzenia konsultacji we wszelkich innych sprawach.

(akta kontroli str.59-65)

5. W badanym okresie 158 pracowników spośród 208 biorących udział w przetwarzaniu danych osobowych było przeszkolonych z przepisów rozporządzenia RODO oraz z bezpieczeństwa informacji.

Szkolenia z przepisów rozporządzenia RODO przeprowadzone były przez dwa podmioty zewnętrzne, a ich tematyka obejmowała m.in.:

- Ochronę danych osobowych dla pracownika upoważnionego do przetwarzania danych osobowych zgodnie z rozporządzeniem RODO. Celem szkolenia było zdobycie wiedzy i umiejętności z zakresu przetwarzania i zabezpieczania danych osobowych zgodnie z rozporządzeniem RODO.
- Ochronę danych osobowych i praktyczne aspekty rozporządzenia RODO w podmiotach leczniczych.

Tematyka szkoleń prowadzonych przez IODO obejmowała ochronę danych osobowych oraz przepisy rozporządzenia RODO. W okresie objętym kontrolą IODO przeprowadził następujące szkolenia pracowników Szpitala:

- RODO w służbie zdrowia – odpowiedzi na najczęściej pojawiające się problemy i pytania w systemie ochrony zdrowia.
- Obowiązki informacyjne Administratora Danych Osobowych (ADO) wobec Pacjentów i najczęstsze błędy oraz naruszenia danych osobowych popełniane przez personel medyczny.
- Sposób postępowania w przypadku zagrożenia, incydentu i naruszenia systemu ochrony danych osobowych w Szpitalu.

Szkolenia były też realizowane w zakresie bezpieczeństwa informacji. Odbywały się one zarówno stacjonarnie jak i online. Obejmowały tematykę dotyczącą świadomości cyberbezpieczeństwa dla kadry i pracowników, świadomość cyberbezpieczeństwa

dla kadry zarządzającej, oraz bezpieczeństwo sieci z wykorzystaniem Firewall i wprowadzenie do bezpieczeństwa w Active Directory.

W toku kontroli NIK 127 pracowników Szpitala zostało przeszkolonych z przepisów rozporządzenia RODO oraz 84 z bezpieczeństwa informacji. Odbyło to się w formie samokształcenia, tj. poprzez zapoznanie się z materiałem szkoleniowym w formie instrukcji przygotowanej przez IODO. Materiał ten został przygotowany we współpracy z ASI, a podstawą jego opracowania były zasady zawarte w obowiązujących w Szpitalu dokumentach wewnętrznych, tj. w Polityce Bezpieczeństwa i Instrukcji Zarządzania oraz Procedurze Alarmowej. Szkolenia z RODO dotyczyły m.in. podstawowych zasad przetwarzania i ochrony danych osobowych w Szpitalu, natomiast szkolenia z bezpieczeństwa informacji obejmowały m.in. podstawowe zasady bezpieczeństwa dla użytkowników systemów informatycznych, posiadających dostęp do danych osobowych przetwarzanych przez Szpital jako Administratora.

(akta kontroli str.66-129)

Wg stanu na 31 stycznia 2024 r. do przeszkolenia zarówno z RODO jak i bezpieczeństwa informacji pozostało 50 pracowników, tj. 24% pracowników biorących udział w przetwarzaniu informacji (szerzej opisane w punkcie 2 w sekcji stwierdzone nieprawidłowości).

(akta kontroli str.130-139)

6. W kwietniu 2023 r. Szpital zawarł z Prezesem Narodowego Funduszu Zdrowia (dalej: Fundusz lub NFZ) umowę na finansowanie, ze środków pochodzących z Funduszu Przeciwdziałania covid-19, podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców. W umowie wskazano, że Fundusz sfinansuje ww. działania maksymalnie do kwoty 400 tys. zł. Kwota wykorzystanego dofinansowania wyniosła łącznie 365,3 tys. zł, w wyniku czego uzyskano następujące efekty rzeczowe:

- zautomatyzowanie procesu archiwizacji, rozszerzenie zakresu archiwizacji, zwielokrotnienie miejsc składowania kopii, unowocześnienie urządzeń składujących (odniesienie jakości wykonywanych kopii zapasowych),
- unowocześnione zostały elementy systemu Firewall,
- rozszerzono zakres działania oprogramowania antywirusowego,
- unowocześniono system monitorowania incydentów bezpieczeństwa,
- uzyskano aktualną kontrolę zewnętrznych podatności,
- system EDR (system bezpieczeństwa komputerowego, który koncentrował się na zabezpieczaniu punktów końcowych sieci), podniesienie poziomu ochrony systemu poczty elektronicznej,
- systemowe narzędzia zabezpieczające: SPF[16], DKIM[17], DMARC[18].

(akta kontroli str.140-205)

W okresie objętym kontrolą Szpital poniósł też wydatki związane z utrzymaniem systemów teleinformatycznych w łącznej kwocie 708,0 tys. zł. Dotyczyły one realizacji umów na: utrzymanie systemu finansowo-księgowego, utrzymanie systemu Eurosoft oraz usług informatycznych.

(akta kontroli str.206-241)

[16] SPF - weryfikuje autoryzowane serwery pocztowe, które mogą wysyłać e-maile w imieniu domeny.

[17] DKIM - rodzaj zabezpieczeń antyphishingowych, który weryfikuje domenę nadawcy wiadomości email.

[18] DMARC - protokół uwierzytelniania, polityki i raportowania wiadomości e-mail, który jest ustawiony w ustawieniach DNS domeny jako rekord TXT.

Stwierdzone nieprawidłowości

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

1. Do 1 lutego 2024 r. nie opracowano systemu SZBI na podstawie Polskiej Normy PN-ISO/IEC 27001 – Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Systemy zarządzania bezpieczeństwem informacji – Wymagania.

   Prezes Zarządu mi.in. z uwagi na upływ czasu nie potrafiła podać przyczyn powyższej nieprawidłowości. Wskazała, że osobą odpowiedzialną za opracowanie SZBI była IODO. Również IODO nie potrafiła wyjaśnić i wskazać przyczyn ww. nieprawidłowości.

   (akta kontroli str.5-58, 242-244, 304-306)

2. Do 1 lutego 2024 r. nie przeszkolono z bezpieczeństwa informacji 50 spośród 208 pracowników Szpitala (tj. 24,0%) zaangażowanych w proces przetwarzania informacji. Było to niezgodne z § 20 ust. 2 pkt 6 rozporządzenia KRI, który stanowił, że zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień jak zagrożenia bezpieczeństwa informacji, skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna oraz stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

3. Do 1 lutego 2024 r. nie przeszkolono 50 spośród 208 pracowników Szpitala (tj. 24,0%) zaangażowanych w proces przetwarzania informacji z przepisów rozporządzenia RODO.

   W wyjaśnieniach dotyczących przyczyn braku przeszkolenia wszystkich pracowników Szpitala z RODO i bezpieczeństwa informacji, IODO podała, że spowodowane to było m.in. stanem zagrożenia epidemicznego, wywołanego zakażeniami wirusem SARS-CoV-2, a następnie stanem epidemii, panującymi w kraju w latach 2020 – 2023, w czasie którego ryzyko rozpowszechniania się wirusa w placówce medycznej było bardzo wysokie, a ograniczenia dotyczyły przede wszystkim zakazu zgromadzeń czy skupisk ludzkich.

   (akta kontroli str.66-139, 242-244, 304-306)

OCENA CZĄSTKOWA

Stworzone rozwiązania organizacyjne i techniczne dotyczące bezpieczeństwa informacji, w tym danych pacjentów obejmowały m.in.: właściwe wyznaczenie IODO wraz z odpowiednim określeniem jego zadań, określenie kompetencji ASI oraz odpowiednie opracowanie zasad zarządzania incydentami związanymi z bezpieczeństwem informacji. Zgodnie z założeniami zrealizowano podniesienie poziomu bezpieczeństwa systemów teleinformatycznych w ramach uzyskanego dofinansowania. Do 1 lutego 2024 r. nie opracowano jednak systemu SZBI na podstawie Polskiej Normy PN-ISO/IEC 27001 – Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Systemy zarządzania bezpieczeństwem informacji – Wymagania. Nie zrealizowano również, szkoleń niektórych pracowników Szpitala z zakresu bezpieczeństwa informacji oraz przepisów rozporządzenia RODO.

OBSZAR

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

Opis stanu faktycznego

1. W okresie od 1 stycznia 2020 r. do 31 grudnia 2023 r. w Szpitalu funkcjonowały trzy systemy medyczne, których Szpital był administratorem danych. Były to:

- System HIS (Hospital Information System) Eurosoft Przychodnia – System informatyczny do obsługi ZOZ, którego głównym zadaniem była obsługa pacjenta w poradniach i na oddziałach, tworzenie elektronicznej dokumentacji medycznej,
- EDM – Elektroniczna Dokumentacja Medyczna (Electronic Health Record),
- Cyfrowy System RTG służący opisywaniu, przechowywaniu i katalogowaniu obrazów cyfrowego obrazowania medycznego.

Ponadto Szpital miał dostęp, nie będąc administratorem, do następujących systemów informatycznych:

- SZOI – System Zarządzania Obiegiem Informacji służący do dwukierunkowej komunikacji między Oddziałem Wojewódzkim NFZ i podmiotami zewnętrznymi: świadczeniodawcami, aptekami, podwykonawcami.
- SIMP – System Informatyczny Monitorowania Profilaktyki – narzędzie informatyczne służące do realizacji niżej wymienionych programów profilaktycznych, udostępniane świadczeniodawcom przez Narodowy Fundusz Zdrowia, w zakresie następujących programów profilaktyki:
  - chorób układu krążenia,
  - raka szyjki macicy – etap podstawowy – pobranie materiału do przesiewowego badania cytologicznego,
  - raka szyjki macicy – etap diagnostyczny,
  - raka szyjki macicy – etap pogłębionej diagnostyki,
  - raka piersi – etap podstawowy – w pracowni stacjonarnej,
  - raka piersi – etap podstawowy – w pracowni mobilnej,
  - raka piersi – etap pogłębionej diagnostyki,
  - program opieki koordynowanej nad kobietą w ciąży (KOC).
- AP-DILO – Moduł obsługi karty diagnostyki leczenia onkologicznego,
- AP-KOLCE – Moduł Kolejki Centralne,
- EZWM – Aplikacja internetowa przeznaczona do wystawiania wniosków, weryfikowania ich i wydawania przedmiotów zaopatrzenia medycznego bezpośrednio u dostawcy z pominięciem konieczności wizyty w NFZ,
- EWUŚ – Aplikacja internetowa przeznaczona do weryfikacji aktualności ubezpieczenia zdrowotnego Pacjenta,
- OPTIMED Elbląg – system HIS na potrzeby Szpitala Miejskiego w Elblągu,
- NIZP-PZH – raportowanie karty statystycznej MZ/Szp-11,
- ZUS – wystawianie zaświadczeń eZLA.

(akta kontroli str.247-252)

2. W okresie od 1 stycznia 2020 r. do 31 grudnia 2023 r. Szpital posiadał wdrożoną usługę katalogową – Active Directory. Spośród 47 pracowników niemedycznych Szpitala[19], trzech posiadało uprawnienia dostępu do danych medycznych w systemie

[19] W tym 14 pracowników administracji z Panią Prezes, 20 salowych, 3 sprzątaczki, 4 pomoce opiekunek, 4 pracowników gospodarczych i technicznych, 2 kierowców.

informatycznym. Była to Pani Prezes[20], informatyk[21] oraz specjalista ds. rachunków kosztów[22].W trakcie kontroli ustalono, że każdy z ww. pracowników, który miał dostęp do danych medycznych:

- otrzymał stosowne upoważnienie do przetwarzania danych osobowych,
- miał dostęp do systemu medycznego wyłącznie po odpowiednim przeprowadzeniu autoryzacji (podaniu loginu i hasła),
- miał dostęp do danych medycznych wyłącznie w zakresie wydanego upoważnienia i przetwarzał je w ramach wykonywanych obowiązków.

Ustalono również, że pozostałych 44 pracowników, którzy nie wykonywali zadań związanych z przetwarzaniem ww. danych, nie posiadało uprawnień dostępu do danych medycznych pacjentów w systemie informatycznym.

(akta kontroli str.253-262)

3. Analiza uprawnień dostępu nadanych w systemach informatycznych oraz upoważnień do przetwarzania danych osobowych 17 spośród 79 pracowników medycznych Szpitala (16 pielęgniarek i jedna położna) wykazała że:

- posiadały one wydane przez ADO stosowne upoważnienia do przetwarzania danych osobowych pacjentów Szpitala,
- miały dostęp do danych medycznych wyłącznie w zakresie wskazanym w upoważnieniu do przetwarzania danych osobowych,
- dostęp do systemu medycznego posiadały wyłącznie po odpowiednim przeprowadzeniu autoryzacji (podaniu loginu i hasła),
- przetwarzały dane medyczne pacjentów w ramach wykonywanych przez siebie obowiązków.

Ustalono ponadto, że żaden z pracowników Szpitala, który nie był zaangażowany w proces przetwarzania danych medycznych pacjentów[23], nie miał nadanego upoważnienia do przetwarzania takich danych, ani nie miał nadanych uprawnień do dostępu do systemów medycznych Szpitala.

(akta kontroli str.263-273)

4. Analiz obejmująca byłych pracowników Szpitala dotycząca odbierania im uprawnień dostępu do systemów informatycznych wykazała m.in., że:

- w okresie od 1 stycznia 2022 r. do 31 grudnia 2023 r. rozwiązano stosunek pracy lub umowę cywilnoprawną z 52 osobami,
- 18 osobom odebrano uprawnienia dostępu do systemów informatycznych w tym samym dniu,
- 26 osobom od 2 do 653 dni[24], licząc od dnia rozwiązania z nimi stosunku pracy bądź umowy cywilnoprawnej,
- 8 osobom odebrano uprawnienia przed rozwiązaniem z nimi stosunku pracy bądź umowy cywilnoprawnej,
- nie wystąpiły przypadki, aby po dacie rozwiązania stosunku pracy, pracownik zalogował się do systemu,

[20] Dostęp do Active Directory, HIS Eurosoft Przychodnia, SZOI, AP-KOLCE, EWUŚ.

[21] Dostęp do wszystkich programów informatycznych wskazanych w punkcie II.1 niniejszego wystąpienia pokontrolnego, poza Optimed Elbląg i ZUS., do których dostęp mieli lekarze podczas obsługi pacjentów oraz podczas m.in. wystawiania zaświadczeń lekarskich o niezdolności do pracy.

[22] Dostęp do Active Directory, HIS Eurosoft Przychodnia.

[23] W tym 20 salowych, 3 osoby sprzątające. W Szpitalu nie zatrudniano sanitariuszy.

[24] W tym siedmiu byłym pracownikom w okresie do 10 dni, siedmiu w okresie od 29 do 74 dni, pięciu w okresie od 104 do 443 dni, siedmiu w okresie od 604 do 653 dni.

– wszystkie konta osób, którym odebrano uprawnienia zostały zablokowane.

(akta kontroli str.274-278)

5. W toku oględzin NK przeprowadzonych 7 lutego 2024 r., którymi objęto siedem stanowisk komputerowych[25] ustalono m.in., że:

– Każdy z komputerów włączony był do systemu Active Directory i umożliwiał użytkownikom zalogowanie się do systemu szpitalnego zgodnie z nadanymi uprawnieniami (każdy komputer umożliwiał zalogowanie się użytkownikowi w ramach posiadanego upoważnienia i nadanych uprawnień do systemu medycznego Szpitala).
– Użytkownicy logowali się do sytemu Windows podając nazwę użytkownika i hasło. Wpisywane hasła posiadały długość od 8 do 15 znaków.
– Cztery osoby będące użytkownikami komputerów poddanych oględzinom (Prezes, specjalista ds. kosztów, lekarz, pielęgniarka) posiadały uprawnienia i dostęp do systemu Eurosoft Przychodnia. Logując się do tego systemu podawali swój login (ciąg znaków, na które składała się pierwsza litera imienia oraz nazwisko bez polskich znaków) oraz hasło, o liczbie znaków nie mniejszej niż osiem. Pracownicy ci mieli dostęp w tym systemie wyłącznie do danych, co do których posiadali stosowne upoważnienie.
– Na każdym komputerze zainstalowany był program antywirusowy Eset, z aktualną bazą wirusów na dzień przeprowadzonych oględzin.
– Na każdym komputerze zainstalowany był system Windows 10.
– Zapis na nośnikach pamięci podłączonych do portów USB był systemowo zablokowany w przypadku każdego stanowiska (wymagał uprawnień administratora).
– Wygaszacz ekranu był aktywowany po czasie od 5 do 20 minut braku aktywności, który do odblokowania ekranu wymagał podania hasła użytkownika.
– Na żadnym z komputerów, żaden z pracowników nie posiadał uprawnień administratora i nie mógł zainstalować żadnego oprogramowania. Podczas próby zainstalowania programu system żądał hasła administratora.
– Nie stwierdzono przypadków aby login i/lub hasło użytkownika zapisane i pozostawione w otoczeniu miejsca pracy.

(akta kontroli str.279-284)

6. W okresie objętym kontrolą w Szpitalu prowadzono rejestr incydentów, w formie Dziennika Uchybień i Zagrożeń jako załącznika nr 1 do Procedury Alarmowej w Szpitalu. W analizowanym okresie nie odnotowano zapisów, z których wynikałoby, że w Szpitalu miały miejsc incydenty. W książce skarg i wniosków nie odnotowano również skarg związanych z ujawnianiem danych osobowych.

(akta kontroli str.285)

7. W okresie od 1 stycznia 2020 r. do 31 grudnia 2023 r. Szpital zawarł z podmiotami zewnętrznymi dwie umowy, których przedmiotem było powierzenie przetwarzania danych osobowych, przy czym w latach 2018-2019, w związku z wejściem w życie przepisów rozporządzenia RODO, zawartych zostało 14 umów powierzenia przetwarzania danych osobowych z podmiotami, z którymi stała współpraca była nadal kontynuowana. Zawierane umowy dotyczyły w szczególności:

– wykonywania badań diagnostycznych i laboratoryjnych czy mikrobiologicznych skierowanych pacjentów,

[25] Użytkowanych przez wybranych losowo pracowników (Prezes zarządu, cztery osoby z administracji (w tym m. in. gł. księgowa i specjalista ds. rachunków kosztów), jeden lekarz oraz jedna pielęgniarka pracująca w Zakładzie Opiekuńczo – Leczniczym w dniu i godzinach przeprowadzania oględzin).

- wykonywania badań z zakresu obrazowej diagnostyki medycznej, takich jak badania rezonansem magnetycznym, tomografii komputerowej, badania RTG, USG, mammografii, itp.,
- udzielania świadczeń zdrowotnych w postaci specjalistycznych konsultacji lekarskich (m.in. konsultacji neurologicznych, laryngologicznych, okulistycznych),
- usług w zakresie transportu medycznego i sanitarnego pacjentów,
- prowadzenia usług finansowo-księgowych i ewidencyjnych czy przechowywania papierowej dokumentacji archiwalnej,
- realizacji umów serwisowych oraz aktualizacji systemów informatycznych Szpitala poprzez utrzymanie i wsparcie techniczne programów / baz danych zawierających dane osobowe i medyczne Pacjentów,
- publikacji artykułów zawierających wizerunki i dane osobowe osób fizycznych na stronie internetowej Starostwa Powiatowego w Elblągu (dane pracowników, osób trzecich, itp.).

Na podstawie analizy wybranych losowo pięciu umów powierzenia przetwarzania danych osobowych ustalono, że spełniały one wymogi art. 28 rozporządzenia RODO. I tak, ww. umowy stanowiły, że podmiot, któremu powierzone zostało przetwarzanie danych, m.in.:

- dokonuje tego wyłącznie na udokumentowane polecenie administratora,
- zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy,
- podejmuje wszelkie niezbędne środki bezpieczeństwa dla ochrony przetwarzania danych,
- przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o ile dysponuje szczegółową i pisemną zgodą ADO na dalsze powierzenie,
- w miarę możliwości wspiera ADO w wywiązywaniu się przez niego z obowiązków związanych z ochroną danych osobowych oraz udostępnia ADO wszelkie informacje niezbędne do wykazania spełnienia powyższych obowiązków,
- uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32-36 rozporządzenia RODO,
- po zakończeniu świadczenia usług związanych z przetwarzaniem, zależnie od decyzji ADO, usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich kopie, chyba że prawo nakazuje przechowywanie danych osobowych,
- umożliwia ADO lub audytorowi upoważnionemu przez ADO przeprowadzanie audytów, w tym inspekcji.

(akta kontroli str.286-303)

Stwierdzone nieprawidłowości

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

W okresie od 1 stycznia 2020 r. do 31 grudnia 2023 r. w Szpitalu 26 byłym pracownikom odbierano dostęp do systemów informatycznych zawierających dane osobowe pacjentów w terminie od 2 do 653 dni[26], licząc od dnia rozwiązania z nimi stosunku pracy bądź umowy cywilnoprawnej. Było to niezgodne z art. 5 pkt 1 lit. c w zw. z art. 29 oraz art. 32 ust. 4 rozporządzenia RODO, wg których stosownie do zasady adekwatności i minimalizacji, ADO podejmuje działania w celu

[26] W tym siedmiu byłym pracownikom w okresie do 10 dni, siedmiu w okresie od 29 do 74 dni, pięciu w okresie od 104 do 443 dni, siedmiu w okresie od 604 do 653 dni.

zapewnienia, by każda osoba fizyczna mająca dostęp do danych osobowych, przetwarzała je wyłącznie na podstawie upoważnienia ADO i na jego polecenie.

W wyjaśnieniach Prezes Zarządu z uwagi mi.in. na upływ czasu nie potrafiła podać przyczyn powyższej nieprawidłowości. Wskazała, że sprawami tymi zajmował się Informatyk, który również nie potrafił wskazać przyczyn wskazanej wyżej nieprawidłowości.

(akta kontroli str.245-246, 274-278)

OCENA CZĄSTKOWA

Przetwarzanie danych pacjentów odbywało się w sposób prawidłowy. Pracownikom Szpitala we właściwy sposób nadano uprawnienia dostępu w systemach informatycznych, tj. były one adekwatne do zakresu nadanych im upoważnień do przetwarzania danych osobowych i wykonywanych obowiązków. Prawidłowo również postąpiono w przypadku pracowników niemedycznych, tj. nie posiadali oni takich uprawnień. W Szpitalu stosowano sprzętowe i programowe środki, które zapewniły skuteczną ochronę bezpieczeństwa informacji. Na komputerach stosowana była bowiem m.in. usługa Active Directory, która umożliwiała logowanie się do systemu Windows wyłącznie użytkownikom posiadającym konto systemowe.

Niezgodnie z przepisami rozporządzenia RODO, dotyczącymi zasady adekwatności i minimalizacji, odbyło się odbieranie byłym pracownikom dostępu do systemów informatycznych. Opóźnienie w tym zakresie wystąpiło w 26 przypadkach i wyniosło od 2 do 653.

IV. Uwagi i wnioski

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, nie formułuje uwag, a wnioskuje o podjęcie działań w celu:

1. Opracowania i wdrożenie SZBI, o którym mowa w rozporządzeniu KRI.
2. Przeszkolenia z bezpieczeństwa informacji tych pracowników, którzy dotychczas nie zostali nim objęci, a są zaangażowani w proces przetwarzania informacji.
3. Przeszkolenia z RODO tych pracowników, którzy dotychczas nie zostali nim objęci, a są zaangażowani w proces przetwarzania informacji z przepisów rozporządzenia RODO.
4. Niezwłocznego odbierania dostępu do systemów informatycznych zawierających dane osobowe pacjentów, stosownie do postanowień rozporządzenia w sprawie RODO.

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.

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, 21 lutego 2024 r.

Najwyższa Izba Kontroli
Dyrektor Delegatury
w Olsztynie
z up.
Piotr Wanic
wicedyrektor

.....
podpis

Kontroler
Leszek Żywucki
Główny specjalista
kontroli państwowej

.....
podpis