NAJWYŻSZA IZBA KONTROLI

Delegatura w Olsztynie

LOL.411.5.4.2023

Brygida Schlueter – Górska
Prezes Zarządu
Szpital Mrągowski
im. Michała Kajki Sp. z o.o.
ul. Wolności 12
11-700 Mrągowo

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 Mrągowski im. Michała Kajki Sp. z o.o., ul. Wolności 12, 11-700 Mrągowo (dalej: Szpital).

Kierownik jednostki kontrolowanej

Brygida Schlueter – Górska, Prezes Zarządu, od 19 listopada 2013 r. (dalej: Prezes Szpitala).

(akta kontroli str. 7)

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. Bartosz Kościukiewicz, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LOL/147/2023 z 17 listopada 2023 r.
2. Rafał Dmytrenko, specjalista kontroli państwowej, upoważnienie do kontroli nr LOL/153/2023 z 24 listopada 2023 r.
3. Sebastian Helbrecht, specjalista kontroli państwowej, upoważnienie do kontroli nr LOL/163/2023 z 4 grudnia 2023 r.

(akta kontroli str. 1-6)

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

W Szpitalu na ogół prawidłowo realizowano rozwiązania dotyczące zapewnienia bezpieczeństwa informacji, w tym danych pacjentów. Po uznaniu Szpitala za operatora usługi kluczowej (dalej: OUK), wprawdzie podjęto wymagane przepisami ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[3] działania, wskutek których ustanowiono Zintegrowany System Zarządzania (dalej: ZSZ), to

[1] Dz. U. z 2022 r. poz. 623, dalej: ustawa o NIK.
[2] NIK formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.
[3] Dz. U. z 2023 r. poz. 913, ze zm., dalej: ustawa o cyberbezpieczeństwie.

realizacja przyjętych w nim postanowień w zakresie zapewnienia bezpieczeństwa informacji odbywała się w sposób odbiegający od niektórych wymagań lub w sposób nierzetelny.

Należycie wywiązano się z ustawowych obowiązków OUK określonych w art. 16 ustawy o cyberbezpieczeństwie. We właściwy sposób powołano wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo, w skład których wszedł m.in. Zespół ds. cyberbezpieczeństwa. Jednakże w pierwszych miesiącach funkcjonowania tego zespołu nie zrealizowano obowiązku comiesięcznej organizacji jego posiedzeń. Zgodnie z art. 37 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[4], we właściwy sposób wyznaczono Inspektora Ochrony Danych (dalej: IOD). Posiadał on odpowiednie kwalifikacje oraz prowadził szkolenia pracowników w zakresie ochrony danych osobowych pacjentów.

W Szpitalu nie były przestrzegane niektóre wymogi określone w sekcji 3 – podstawowe zasady dostępu, ujęte w polityce dostępu do środowiska teleinformatycznego. Przeprowadzone przez NIK oględziny wykazały bowiem, że rozwiązania sprzętowe i systemowe umożliwiały pracownikom medycznym Szpitala (pielęgniarkom i lekarzom) dostęp do informacji, w tym m.in. plików z danymi osobowymi i medycznymi pacjentów, które znajdowały się na dyskach twardych tych stanowisk komputerowych. Było to możliwe niezależnie od tego, który z pracowników wygenerował, przetworzył i zapisał te informacje z danymi pacjentów. Powyższy stan stwierdzony w toku oględzin przeprowadzonych przez kontrolerów NIK wskazuje, że podjęte w Szpitalu w ramach nadzoru nad przestrzeganiem przez pracowników zasad określonych w ZSZ działania nie były w pełni skuteczne.

Personel niemedyczny, przy nadzorze ze strony Sekcji Informatyki, realizując swoje obowiązki przestrzegał postanowień ZSZ, przy czym uprawnienia dostępu do informacji zawierających dane pacjentów, w niezbędnym zakresie posiadali tylko ci pracownicy, którzy wykonywali zadania związane z przetwarzaniem danych pacjentów. Jedynym ustalonym w kontroli NIK przypadkiem niezgodności w wypełnianiu postanowień ZSZ w odniesieniu do pracowników niemedycznych była sytuacja ustawienia przez pracownika archiwum hasła dostępu, które zawierało mniej znaków niż było to wymagane postanowieniami ZSZ.

Przy korzystaniu przez Szpital z zewnętrznych usług, m.in. z usług IT, zlecania prac serwisowych aparatury medycznej oraz usług diagnostycznych, w sposób zgodny z art. 28 rozporządzenia RODO, zawierano umowy powierzenia przetwarzania danych osobowych.

Podkreślić należy także, że w okresie objętym kontrolą, a przed uznaniem Szpitala za OUK, funkcjonował w nim System Zarządzania Bezpieczeństwem Informacji (dalej: SZBI), o którym mowa w rozporządzeniu 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[5]. SZBI wbrew wymogowi §20 ust. 3 rozporządzenia KRI nie został jednak w pełnym zakresie opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001 – Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Systemy zarządzania bezpieczeństwem informacji – Wymagania.

[4] Dz. Urz. UE L 119 z 4 maja 2016 r., str. 1, dalej: rozporządzenie RODO.
[5] Dz. U. z 2017 r. poz. 2247, dalej: rozporządzenie KRI.

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

OBSZAR

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

Opis stanu faktycznego

1.1. W dniu 11 lipca 2022 r. Szpital otrzymał decyzję wydaną przez Ministra Zdrowia[7], w której został on uznany za OUK w sektorze ochrony zdrowia[8]. Po 4 miesiącach i 14 dniach od dnia otrzymania ww. decyzji dokonano zmiany w Regulaminie Organizacyjnym Szpitala przez dodanie zapisów dotyczących ZSZ[9]. Wprowadzone zmiany określiły, że polityka ZSZ realizowana była przez system zarządzania bezpieczeństwem informacji obejmujący dokumentację polityk, procedur oraz regulacji zewnętrznych. Do przestrzegania zasad bezpieczeństwa wynikających z przyjętych rozwiązań zobowiązani zostali pracownicy, współpracownicy oraz dostawcy. W strukturze Szpitala w zakresie spraw związanych z ochroną danych pacjentów wyodrębniono m.in. Sekcję Informatyki, Administratora Systemu Informatycznego, Pełnomocnika ds. cyberbezpieczeństwa, a także IOD.

Szpital po otrzymaniu decyzji o uznaniu go za OUK w terminie:

– trzech miesięcy m.in. wyznaczył osoby kontaktowe z właściwym Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego oraz powołał wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo,
– sześciu miesięcy m.in. wdrożył środki techniczne i organizacyjne w ramach ZSZ, zbierał informacje o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego, stosował środki zapobiegające i ograniczające wpływ incydentów na bezpieczeństwo systemu informacyjnego,
– roku zapewnił przeprowadzenie audytu bezpieczeństwa systemu informacyjnego[10], co było zgodne z art. 16 pkt 3 ustawy o cyberbezpieczeństwie.

(akta kontroli str. 8-103, 387-455)

1.2. Zgodnie z art. 22 ust. 1 pkt 4 ustawy o cyberbezpieczeństwie, Szpital zapewnił pacjentom, zarówno tym, którzy trafili do poradni jak i na oddział szpitalny, dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami. Obowiązek ten został wykonany przez opublikowanie informacji w powyższym zakresie na stronie internetowej Szpitala[11]. Informacja taka była także przedstawiana pacjentom w formie papierowej, która była zamieszczona na tablicach informacyjnych w Szpitalu.

(akta kontroli str. 456-467)

1.3. Prezes Szpitala w dniu 2 maja 2023 r. w trybie zarządzenia wprowadziła procedurę analizy ryzyka ogólnego i oceny skutków dla przetwarzanych danych, a także zatwierdziła oszacowane według tej procedury wspomniane ryzyka. Proces szacowania ryzyka realizacji usługi kluczowej został oparty m.in. na normach ISO[12]

---

[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] Decyzja wydana w dniu 7 lipca 2022 r.

[8] Usługa ta polegała na udzielaniu świadczeń opieki zdrowotnej oraz na obrocie i dystrybucji produktów leczniczych.

[9] Zmiany wprowadzone uchwałą nr 03/11/2022 Zarządu Szpitala z 25 listopada 2022 r.

[10] Audyt przeprowadzony została w dniach 21-23.06.2023 r.

[11] https://szpital-mragowo.pl/cyberbezpieczenstwo/ stan na 4 grudnia 2023 r.

[12] PN-EN ISO/IEC 27002:2017 Technika Informatyczna – Technika Bezpieczeństwa – Praktyczne zasady zabezpieczania informacji, PN-ISO/IEC 27005:2014-01 Technika Informatyczna – Technika bezpieczeństwa – Wsparcie do Normy PN-EN ISO/IEC 27001:2017.

oraz komunikacie Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony. Celem procedury było zidentyfikowanie obszarów, które mogły mieć istotny wpływ na osobę, której przetwarzanie danych osobowych dotyczyło. Określała ona szczegółowo proces szacowania ryzyka oparty na identyfikacji aktywów podstawowych i wspierających[13].

Szpital posiadał ponadto analizę ryzyka stanowiącą załącznik do Polityki ochrony danych wprowadzonej zarządzeniem nr 23/2018 z dnia 25 maja 2018 r. Uwzględniono w niej incydenty związane m.in. z instalacją szkodliwego oprogramowania, ataków na sprzęt komputerowy, włamania z sieci zewnętrznej do sieci wewnętrznej oraz nieuprawniony dostęp lub włamanie do pomieszczeń.

(akta kontroli str. 468-535)

1.4. W Szpitalu, zgodnie z art. 10 ustawy o cyberbezpieczeństwie, opracowano dokumentację dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej. W ramach przyjętego ZSZ określono w szczególności zasady ujęte m.in. w procedurach dotyczących ciągłości działania, pracy zdalnej, zarządzania nośnikami informacji, przeglądu i naprawy sprzętu komputerowego oraz oprogramowania, nadawania i zarządzania upoważnieniami i uprawnieniami, nadzoru nad udokumentowaną informacją, zarządzania incydentami bezpieczeństwa, oraz zarządzania podatnościami. Poza tymi procedurami, w ramach ZSZ określono także wewnętrzne polityki w szczególności w zakresie stref dostępu i zabezpieczeń, bezpieczeństwa informacji dla wykonawców/dostawców, dostępu do środowiska teleinformatycznego, bezpieczeństwa informacji oraz ciągłości działania. W ZSZ ujęte też były zasady postępowania z informacjami oraz instrukcja zarządzania systemem informatycznym Szpitala.

Analiza niektórych dokumentów przyjętych w ramach ZSZ i sposobu ich realizacji wykazała m.in., że Szpital realizował zadania ujęte w tych dokumentach. W szczególności opracowano harmonogram/plan testów ciągłości działania systemów informatycznych, posiadano w formie elektronicznej topologię sieci, prowadzono rejestr wejść i wyjść wykonawców/dostawców na teren Szpitala, a także prowadzono rejestr nadawanych uprawnień do systemów informatycznych, rejestr zniszczonych nośników informacji, rejestr nadawania i odbierania upoważnień do przetwarzania danych osobowych.

Szpital w dniu 16 października 2023 r. otrzymał z Ministerstwa Zdrowia pismo z rekomendacją przeprowadzenia działań w czterech obszarach mających na celu wdrożenie rozwiązań dotyczących wyeliminowania określonych podatności w systemie bezpieczeństwa. Dotyczyło to poczty elektronicznej, dostępu do serwerów VPN lub proxy, zablokowania portów USB oraz zablokowania wykonywania komend i makr. Prezes Szpitala wyjaśniła, że w okresie od dnia otrzymania rekomendacji do 15 listopada 2023 r. przeprowadzono działania dotyczące analizy i możliwości wprowadzenia otrzymanych rekomendacji. Skutkiem tego było zablokowanie portów USB we wszystkich komputerach w Szpitalu w sposób systemowy lub z użyciem fizycznej plomby. Komisja ds. cyberbezpieczeństwa Szpitala rozważyła oferty firm outsourcingowych na obsługę poczty elektronicznej i stwierdziła, że Szpital był w złej kondycji finansowej i nie było go stać na poniesienie dodatkowych kosztów wynikających z otrzymanych ofert. Ponadto ww. komisja ustaliła, że na początku 2024 r. zostanie zablokowana możliwość wykonania poleceń z linii komend takich jak

[13] Aktywa podstawowe: informacje o danych osobowych i operacje ich przetwarzania. Aktywa wspierające: sprzęt, nośniki danych papierowe i elektroniczne, oprogramowanie, okablowanie, personel i lokalizacja.

CMD i PowerShell oraz zablokowana zostanie możliwość dostępu do sieci takich jak TOR i innych serwerów proxy i VPN.

(akta kontroli str. 19-21, 104-382, 536-567)

1.5. W dniu 14 lipca 2023 r. Szpital zawarł umowę, w której ustanowiono pełnomocnika ds. cyberbezpieczeństwa. Wskazano w niej, że realizacja zadań pełnomocnika obejmowała m.in. kontakt z podmiotami Krajowego Systemu Cyberbezpieczeństwa. Było to zgodne z art. 9 ust. 1 pkt 1 ustawy o cyberbezpieczeństwie, który stanowił, że OUK wyznacza osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. W warunkach ww. umowy wskazano, że pełnomocnik będzie realizował jej przedmiot w wymiarze 10 godzin w miesiącu, z tytułu czego będzie mu przysługiwać wynagrodzenie w kwocie 3,0 tys. zł. Za okres od lipca do grudnia 2023 r. Szpital wypłacił łącznie w ramach ww. umowy kwotę 21,4 tys. zł, z czego 3,4 tys. zł stanowiło rozliczenie za dodatkowe godziny świadczenia usługi pełnomocnika ponad wskazane 10 godzin, co było zgodne z §6 ust. 3 ww. umowy.

Przed zawarciem ww. umowy, funkcję Pełnomocnika ds. cyberbezpieczeństwa pełnił pracownik Szpitala, wyznaczony w ramach jego struktury wewnętrznej. W zakresie czynności tego pracownika, jako Pełnomocnika ds. cyberbezpieczeństwa, było również realizowanie zadania polegającego na kontakcie z podmiotami Krajowego Systemu Cyberbezpieczeństwa. Pracownik ten wyjaśnił, że przestał pełnić funkcję Pełnomocnika ds. cyberbezpieczeństwa z uwagi na zbyt duże obciążenie zakresem obowiązków wynikających zarówno z pełnienia funkcji Kierownika Sekcji Informatyki i Administratora Systemów Informatycznych, które nie pozwalało mu na rzetelne wykonywanie dodatkowych obowiązków w zakresie funkcji Pełnomocnika ds. cyberbezpieczeństwa.

(akta kontroli str. 568-601)

1.6. W Szpitalu powołano wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo, o których mowa w art. 16 pkt 1 w związku z art. 14 ust. 1 ustawy o cyberbezpieczeństwie. Struktury te obejmowały powołany w dniu 7 sierpnia 2019 r. Zespół ds. bezpieczeństwa informacji, którego działanie określał regulamin funkcjonowania tego zespołu. W dniu 30 listopada 2022 r. do ww. struktur powołany został Pełnomocnik ds. cyberbezpieczeństwa, a dnia następnego, tj. 1 grudnia 2022 r. Zespół ds. cyberbezpieczeństwa[14]. W skład tego zespołu weszli m.in. Pełnomocnik ds. Cyberbezpieczeństwa jako przewodniczący oraz jako członkowie – Kierownik Sekcji Informatyki, IOD, Kierownik Sekcji Technicznej, Kierownik Sekcji Służb Pracowniczych. Od dnia 1 grudnia 2022 r. do dnia 31 czerwca 2023 r. odbyło się 13 takich posiedzeń, przy czym w okresie od 1 grudnia 2022 r. do 5 maja 2023 r. nie były organizowane takie posiedzenia, podczas gdy zgodnie z §2 ust. 1 zarządzenia Prezes Szpitala nr 83/2022 z dnia 1 grudnia 2022 r.[15], posiedzenia Zespołu miały odbywać się co najmniej raz na miesiąc, zaś każde posiedzenie miało zostać udokumentowane notatką z jego przebiegu, podjętych ustaleń i rekomendacji.

W sprawie nieodbycia posiedzeń Zespołu ds. cyberbezpieczeństwa w okresie od 1 grudnia 2022 r. do 5 maja 2023 r., Prezes Szpitala wyjaśniła, że pierwsze spotkania były spotkaniami organizacyjnymi oraz, że nie wszystkie spotkania były protokołowane. W kwietniu 2023 r. Pełnomocnik ds. cyberbezpieczeństwa zasugerował, żeby z każdego spotkania sporządzać protokół gdyż w Szpitalu nie ma dowodów na to, że dotychczasowe spotkania się odbyły.

NIK nie podziela jednak powyższych wyjaśnień, bowiem Prezes Szpitala wyjaśniła, że w tym okresie obyły się tzw. spotkania organizacyjne. Wskazane wyżej

[14] Jednocześnie straciło moc zarządzenie nr 35/2019 w sprawie powołania Zespołu ds. bezpieczeństwa informacji.
[15] W sprawie powołania Zespołu ds. cyberbezpieczeństwa.

zarządzenie nr 83/2022 nie przewiduje w swojej treści trybu „spotkań organizacyjnych", nie określa zwoływania spotkań organizacyjnych i nie wskazuje, że z takich spotkań organizacyjnych nie sporządza się dokumentu potwierdzającego ich przeprowadzenie. Zgodnie z tym zarządzeniem, jednym przewidzianym w nim trybem były posiedzenia Zespołu ds. cyberbezpieczeństwa. Miały one odbywać się co najmniej raz na miesiąc (§2 ust. 1), a kierujący zespołem (§1 ust. 2 – Pełnomocnik ds. cyberbezpieczeństwa) miał obowiązek informowania wszystkich członków, podając datę i godzinę posiedzeń (§2 ust. 2). Posiedzenia te miały odbywać się w jednym z dwóch miejsc, tj. w gabinecie Prezes Szpitala lub pokoju Sekcji Informatyki (§2 ust. 3), a każde posiedzenie miało zostać udokumentowane notatką (§2 ust. 4). Zatem, zdaniem NIK, wskazane w wyjaśnieniach Prezes Szpitala spotkania organizacyjne nie mogą zostać potraktowane jako wypełnienie obowiązku organizacji posiedzeń Zespołu ds. cyberbezpieczeństwa, o którym mowa w ww. zarządzeniu.

(akta kontroli str. 602-678)

1.7. W okresie objętym kontrolą w Szpitalu, po uznaniu go za OUK, został przeprowadzony jeden audyt bezpieczeństwa systemu informacyjnego (w czerwcu 2023 r.) Celem audytu było potwierdzenie zgodności bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej z wymaganiami ustawy o cyberbezpieczeństwie. Koszt przeprowadzenia audytu wyniósł 18,5 tys. zł. W wyniku przeprowadzonego audytu wydana została opinia pozytywna oraz rekomendacje w obszarze:

– organizacji zarządzania bezpieczeństwem informacji – rozważenie weryfikacji oraz dodania klasyfikacji przetwarzanych informacji w dokumentach systemowych,
– procesów zarządzania bezpieczeństwem informacji – rozważenie przeprowadzenia dedykowanego szkolenia z zakresu cyberbezpieczeństwa dla Sekcji Informatyki w celu podniesienia ich kompetencji,
– utrzymania systemów informacyjnych – rozważenie przeprowadzenia akcji informacyjnej/przypominającej dotyczącej ochrony haseł w Szpitalu.

W sprawie wdrożenia ww. rekomendacji Prezes Szpitala wyjaśniła, że w zakresie pierwszej z nich, w Szpitalu dokonano przeglądu dokumentacji ochrony danych osobowych oraz włączono ją do systemu cyberbezpieczeństwa. Odnośnie wspomnianych wyżej szkoleń, Prezes Szpitala wyjaśniła, że po dokonaniu rozeznania rynku otrzymała ofertę szkoleniową, której kwota wynosiła 7,2 tys. zł, jednakże Szpital nie otrzymał wsparcia finansowego z NFZ na dofinansowanie projektu cyberbezpieczeństwa. W związku z tym zaplanowano udział w darmowym szkoleniu w zakresie kursu cyberbezpieczeństwa, na które rejestracja uczestników była otwarta do końca 2023 r. W sprawie prowadzenia akcji informacyjnej/przypominającej dotyczącej ochrony haseł Prezes Szpitala wyjaśniła, że zagadnienia te były każdorazowo omawiane przy przyjmowaniu pracowników do pracy, a fakt ten był potwierdzany w karcie adaptacji. Dodatkowo podała, że Pełnomocnik ds. cyberbezpieczeństwa opracuje informację przypominającą pracownikom Szpitala zasady ochrony haseł.

(akta kontroli str. 679-753)

1.8. W okresie objętym kontrolą, przed otrzymaniem decyzji o uznaniu Szpitala za OUK, tj. przed dniem 11 lipca 2022 r., w Szpitalu funkcjonował System Zarządzania Bezpieczeństwem Informacji (dalej: SZBI)[16]. Było to zgodne z §20 ust. 1

[16] Wprowadzony i zmieniany zarządzeniami: nr 23/2018 z 25 maja 2018 r., nr 26/2019 z 22 maja 2019 r., nr 34/2019 z 1 sierpnia 2019 r., nr 35/2019 z 7 sierpnia 2019 r., nr 37/2019 z 8 sierpnia 2019 r., nr 41/2019 z 30 września 2019 r., nr 69/2019 z 23 grudnia 2019 r., nr 70/2019 z 23 grudnia 2019 r. oraz nr 71/2019 z 27 grudnia 2019 r.

rozporządzenia KRI. Przepis ten stanowił, że podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. W dokumentacji stanowiącej ww. SZBI ujęto m.in. polityki ochrony danych, zasady tworzenia i aktualizacji aktów prawnych, wyznaczenie IOD, powołanie Zespołu ds. Bezpieczeństwa Informacji oraz instrukcję postępowania w przypadku incydentów bezpieczeństwa danych osobowych.

Funkcjonujący w Szpitalu ww. SZBI nie został jednak w pełnym zakresie opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001[17], do czego zobowiązywały postanowienia §20 ust. 3 rozporządzenia KRI. Zgodnie z tym przepisem wywiązanie się przez podmiot realizujący zadania publiczne z wymagań określonych w §20 ust. 1 i 2 tego rozporządzenia uznaje się za spełnione, jeżeli SZBI został opracowany na podstawie wspominanej normy. W zarządzeniu nr 23/2018 z 25 maja 2018 r. w sprawie wprowadzenia polityki ochrony danych w Szpitalu oraz w załączniku nr 1 do tego zarządzenia stanowiącym politykę ochrony danych nie powołano się na tę normę i nie wskazano, że dokumentacja ta opracowana została na jej podstawie.

Prezes Szpitala w wyjaśnieniach potwierdziła, że tylko niektóre elementy funkcjonującego do 11 lipca 2022 r. SZBI zostały opracowane na podstawie ww. normy. Były nimi m.in. rejestr upoważnień do przetwarzania danych osobowych, rejestr nadanych/odebranych uprawnień do systemów informatycznych, inwentaryzacja sprzętu informatycznego, instrukcja zarządzania RODO (zabezpieczenia fizyczne, techniczne, i środowiskowe, a także tworzenie kopii zapasowych oraz utylizacja elektronicznych nośników i wydruków), umowy powierzenia przetwarzania danych osobowych, procedura wykonywania przeglądów i konserwacji.

(akta kontroli str. 392-403, 605-609, 754-757)

1.9. W okresie poprzedzającym uznanie Szpitala za OUK, w sierpniu 2019 r. powołano Zespół ds. bezpieczeństwa informacji, określając jego skład i strukturę, a także wskazując zadania i podział obowiązków członków tego zespołu powołanych do jego struktury. Do obowiązków Przewodniczącego Zespołu należało m.in. zwoływanie i prowadzenie posiedzeń Zespołu lub kierowanie pracami w trybie obiegowym. W okresie funkcjonowania Zespołu ds. bezpieczeństwa informacji zwołano cztery posiedzenia tego zespołu. Jednym z obowiązków członków zespołu był m.in. systematyczny przegląd i uaktualnianie wdrożonych polityk ochrony danych. Pracownicy Szpital będący członkami Zespołu, w swoich zakresach czynności posiadali stosowne postanowienia obejmujące obowiązki i odpowiedzialność wynikające z pełnienia funkcji członka Zespołu.

(akta kontroli str. 605-609, 660-678, 758-783)

1.10. Przed uznaniem Szpitala za OUK, od 23 grudnia 2019 r. w Szpitalu obowiązywała instrukcja postępowania w przypadku incydentów bezpieczeństwa danych osobowych, stanowiąca integralną część polityki ochrony danych. Zapoznanie się z tą instrukcją zostało potwierdzone przez 38 pracowników Szpitala, w szczególności zajmujących stanowiska kierownicze. Instrukcja ta określała przypadki naruszenia ochrony danych osobowych, charakterystykę zagrożeń z tym związanych, postępowanie w przypadku wystąpienia incydentu, a także zgłaszanie naruszenia ochrony danych organowi nadzorczemu, zawiadamianie osób, których

[17] Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Systemy zarządzania bezpieczeństwem informacji – Wymagania.

dane dotyczą oraz określała również odpowiedzialność personelu za naruszenie ochrony danych i wskazywała działania zapobiegawcze.

(akta kontroli str. 784-800)

1.11. Przez cały okres objęty kontrolą w Szpitalu był wyznaczony IOD[18]. Osoby pełniące tę funkcję, zgodnie z art. 37 ust. 5 RODO posiadały wyższe wykształcenie w zakresie prawa i administracji publicznej, przeszły przeszkolenie dotyczące ochrony danych osobowych w formie studiów podyplomowych oraz odbyły specjalistyczne szkolenia[19]. W zakresie obowiązków IOD były zadania określone w art. 39 RODO, tj.:

- informowanie 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,
- monitorowanie przestrzegania rozporządzenia RODO, innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,
- współpraca z organem nadzorczym.

(akta kontroli str. 801-822)

1.12. W okresie objętym kontrolą w sposób stacjonarny przeprowadzono szkolenia pracowników Szpitala w zakresie ochrony danych osobowych. W 2020 r. szkolenia w tym zakresie odbyło 257 osób, zaś w 2023 r. – 272 osoby[20]. Uczestniczyli w nich pracownicy wszystkich komórek organizacyjnych Szpitala. Tematyka szkoleń obejmowała m.in. zasady ochrony danych zawartych w dokumentacji medycznej, przetwarzania danych określonych w RODO, postępowania w przypadku naruszenia ochrony danych osobowych. W latach 2021-2022 na terenie szpitala nie odbyły się szkolenia stacjonarne z powyższego zakresu, czego przyczyną był obowiązek przestrzegania reżimu sanitarnego w związku z pandemią covid-19[21].

Nowo zatrudniani pracownicy w Szpitalu byli obligatoryjnie szkoleni z zakresu przestrzegania przepisów ochrony danych osobowych zgodnie z instrukcją adaptacji zawodowej dla osób nowozatrudnionych. W 2020 r. takie szkolenie wstępne odbyło 76 nowo zatrudnionych pracowników, zaś w 2023 r. – 78 osób[22].

(akta kontroli str. 823-860)

1.13. W 2022 i 2023 r. Szpital wystąpił do NFZ o wsparcie na dofinansowanie infrastruktury teleinformatycznej. Skutkiem tych działań było otrzymanie dofinansowania na podstawie umowy zawartej dnia 18 lipca 2022 r. na podniesienie poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców. Dofinansowanie to otrzymano ze środków pochodzących z Funduszu Przeciwdziałania covid-19. Otrzymana kwota dofinansowania wyniosła 393,6 tys. zł, przy czym wnioskowano o kwotę 400,0 tys. zł. W wyniku realizacji tej umowy uzyskano następujące efekty rzeczowe: zakupiono macierz dyskową w celu podniesienia poziomu bezpieczeństwa teleinformatycznego, a także system ochrony poczty FortiMail oraz system zarządzania infrastrukturą IT eAuditor.

(akta kontroli str. 861-867)

[18] Na podstawie umowy po pełnienie funkcji IOD z dnia 1 sierpnia 2019 r., 29 lipca 2022 r. oraz 3 lipca 2023 r.
[19] Tytuł szkolenia: Inspektor ochrony danych po zmianach ustawy o ochronie danych osobowych.
[20] Według stanu na grudzień 2023 r.
[21] Zgodnie z poleceniem Wojewody Warmińsko-Mazurskiego z dnia 5 kwietnia 2020 r. wydanym szpitalom samorządowym i państwowym położonym na terenie województwa warmińsko-mazurskiego.
[22] Według stanu na 4 grudnia 2023 r.

Stwierdzone nieprawidłowości

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

1. W okresie od grudnia 2022 r. do maja 2023 r. nie zorganizowano posiedzeń Zespołu ds. cyberbezpieczeństwa w trybie przewidzianym w §2 zarządzenia Prezes Szpitala nr 83/2022 z dnia 1 grudnia 2022 r. (opisane w punkcie 1.6. wystąpienia pokontrolnego).
2. Tylko niektóre elementy SZBI funkcjonującego w okresie objętym kontrolą, tj. przed uznaniem Szpitala za OUK, zostały opracowane na podstawie Polskiej Normy PN-ISO/IEC 27001 (opisane w punkcie 1.8. wystąpienia pokontrolnego).

OCENA CZĄSTKOWA

W Szpitalu po uznaniu go za OUK zostały stworzone odpowiednie rozwiązania organizacyjne w ramach przyjętego ZSZ mające na celu zapewnienie bezpieczeństwa informacji, w tym ochronę danych pacjentów. Wywiązano się we właściwy sposób z ustawowych obowiązków nałożonych na OUK. Wśród powołanych struktur odpowiedzialnych za cyberbezpieczeństwo funkcjonował Zespół ds. cyberbezpieczeństwa, w przypadku którego w początkowym okresie jego funkcjonowania nie odbyły się posiedzenia tego zespołu w sposób do tego przewidziany. We właściwy sposób wyznaczono IOD, który posiadał odpowiednie kwalifikacje oraz prowadził szkolenia pracowników w zakresie ochrony danych osobowych pacjentów. Zanim Szpital został uznany na OUK, wprowadzony w nim SZBI był tylko częściowo opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001.

OBSZAR

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

Opis stanu faktycznego

2.1. Według stanu na 4 grudnia 2023 r. w Szpitalu funkcjonowało 14 systemów informatycznych. Systemy te były przeznaczone do:

- obsługi pacjentów na oddziałach, w poradniach i pracowniach oraz apteki szpitalnej – system Hospital Information System (dalej: HIS),
- obsługi pacjentów w pracowniach RTG – system RIS/PACS,
- obsługi pacjentów w pracowni endoskopowej,
- obsługi pacjentów w pracowni serologii,
- zarządzania trybami obsługi pacjenta w szpitalnym oddziale ratunkowym,
- planowania grafików pracy pracowników,
- funkcjonowania państwowego ratownictwa medycznego,
- obsługi części administracyjnej – kadry, płace, księgowość, magazyn,
- rozliczeń z Narodowym Funduszem Zdrowia,
- realizacji programów profilaktycznych: chorób układu krążenia, raka szyjki macicy, raka piersi, opieki koordynowanej nad kobietą w ciąży,
- diagnostyki i leczenie onkologicznego,
- prowadzenia list oczekujących na wybrane świadczenia,
- obsługi procesu elektronicznego weryfikowania i potwierdzania zlecenia na zaopatrzenie w wyroby medyczne,
- weryfikacji ubezpieczenia pacjenta.

(akta kontroli str. 868)

2.2. W Szpitalu według stanu na 7 grudnia 2023 r. zatrudnionych było 32 pracowników stanowiących personel niemedyczny. Dostęp do danych medycznych w systemie Medicus posiadali wyłącznie pracownicy, którzy w zakresie swoich zadań wykorzystywali go do realizacji swoich obowiązków. W szczególności dotyczyło to personelu odpowiedzialnego za: dietetykę, archiwum, rozliczenia i kontraktowanie świadczeń medycznych, informatykę. Największe uprawnienia do systemów medycznych funkcjonujących w Szpitalu posiadali Kierownik Sekcji Informatyki oraz

pracownicy tej sekcji, a także Kierownik Sekcji Rozliczeń i Kontraktowania Świadczeń Medycznych. W rejestrze nadanych uprawnień nie stwierdzono danych świadczących o nadaniu uprawnień pracownikom nierealizującym zadań związanych z danymi pacjentów.

W Szpitalu zarządzanie siecią informatyczną i dostępem do oprogramowania odbywało się bez usługi Active Directory, tj. bez centralnego zarządzania przez administratora sieci.

(akta kontroli str. 869-903)

2.3. W Szpitalu zatrudnionych było łącznie 224 pracowników stanowiących grupę pielęgniarek, pielęgniarzy i położnych[23]. Oględziny przeprowadzone na stanowisku pracy Kierownika Sekcji Informatyki w zakresie weryfikacji nadanych uprawnień 30 losowo wytypowanych pracowników z ww. grupy oraz analiza dokumentacji stanowiącej upoważnienia do przetwarzania danych osobowych oraz wniosku o nadanie uprawnień dostępu do systemów informatycznych wykazały, że ww. pracownicy uczestniczyli w procesie przetwarzania danych pacjentów w stopniu adekwatnym do realizowanych obowiązków. Zakres nadanych im upoważnień i uprawnień, jaki widniał w systemie informatycznym, w każdym przypadku dotyczył oddziałów i miejsc pracy, w których dany pracownik świadczył swoją pracę. W niektórych przypadkach, takich jak np. pracownicy szpitalnego oddziału ratunkowego czy oddziału anestezjologii i intensywnej opieki medycznej lub zespoły wyjazdowe, posiadali oni uprawnienia w systemach informatycznych do wszystkich Oddziałów Szpitala.

W przypadku jednego pracownika – pielęgniarki zatrudnionej na Bloku Operacyjnym, która zakończyła świadczenie pracy z dniem 31 grudnia 2021 r., według stanu na 19 grudnia 2023 r. nie odebrano jej uprawnień użytkownika w systemie Medicus, pomimo odnotowania w dokumentacji prowadzonej w formie papierowej, że z dniem 31 grudnia 2021 r. wygaszono jej upoważnienie nr 642/2020 do przetwarzania danych osobowych oraz wygaszono uprawnienia użytkownika w systemie informatycznym. Prezes Szpitala wyjaśniła, że wynikało to z przeoczenia. Według historii użytkownika wygenerowanej przez Sekcję Informatyki, ww. pracownik ostanie logowanie do systemu Medicus wykonał 25 lutego 2020 r., tj. w dniu kiedy posiadał upoważnienie do przetwarzania danych osobowych oraz uprawnienie dostępu do systemów informatycznych. W toku kontroli NIK uprawnienia dostępu ww. byłego pracownika do systemów informatycznych Szpitala zostały mu odebrane przez Kierownika Sekcji Informatyki.

(akta kontroli str. 869, 904-999)

2.4. Byłym pracownikom Szpitala odbierano dostęp do systemów informatycznych zawierających dane pacjentów, poza jednym przypadkiem opisanym w punkcie 2.3. wystąpienia pokontrolnego. Oględziny przeprowadzone na próbie 10 losowo wytypowanych byłych pracowników wykazały, że w przypadku sześciu z nich nie wystąpiło nieuprawnione logowanie do systemu Medicus oraz EWUŚ, zaś w pozostałych czterech przypadkach byłych pracowników, Szpital zawarł z nimi kolejne umowy w przedmiocie nawiązania stosunku pracy. W systemie informatycznym nie odnotowano logowań tych pracowników w okresie między kolejnymi umowami.

(akta kontroli str. 869, 1000-1018)

2.5. Stosowane w Szpitalu środki sprzętowe i programowe wykorzystywane w celu ochrony przetwarzanych informacji w toku kontroli zostały poddane oględzinom w dniach 18-19 grudnia 2023 r. Objęto nimi łączenie 15 stanowisk komputerowych,

[23] Według stanu na 6 grudnia 2023 r.

z czego 10 stanowisk obsługiwanych przez pracowników medycznych oraz 5 przez pracowników niemedycznych.

2.5.1. W toku ww. oględzin w przypadku stanowisk komputerowych wykorzystywanych przez pielęgniarki (5 stanowisk) oraz przez lekarzy[24] (5) ustalono m.in., że:

- systemem operacyjnym był Windows 10, zapewniony był dostęp do systemu Medicus, dziewięć stanowisk posiadało plomby zabezpieczające porty USB przed możliwością podłączenia nośników pamięci, zaś w dziesiątym przypadku port ten był zablokowany w systemie operacyjnym,
- w przypadku ośmiu z ww. stanowisk dostęp do pulpitu systemu Windows nie wymagał podania danych uwierzytelniających (loginu i hasła), a w pozostałych dwóch przypadkach[25] rozpoczęcie pracy na komputerze wymagało podania hasła do zabezpieczenia „bitlocker". Wszyscy użytkownicy komputerów poddanych oględzinom korzystali z tego samego konta Windows, na którym włączone było automatyczne logowanie. W toku oględzin przy dwóch stanowiskach[26] nie było obecnych ich użytkowników, a komputery te były włączone i możliwy był dostęp do pulpitu systemu Windows bez konieczności podania hasła do zabezpieczenia „bitlocker",
- dziewięć stanowisk posiadało konta typu lokalnego, zaś w jednym przypadku[27] było to konto typu administrator. Kierownik Sekcji Informatyki w toku oględzin dokonał zmiany typu tego konta ustawiając je jako konto typu lokalnego,
- siedem stanowisk posiadało dostęp do internetu oraz program antywirusowy Eset z aktualną bazą wirusów,
- w toku oględzin w przypadku ośmiu stanowisk, przy których byli obecni lekarze lub pielęgniarki[28], zostali oni poproszeni o wpisanie swojego loginu i hasła do systemu Medicus. Wpisane loginy odpowiadały pierwszym literom nazwiska i imienia tych lekarzy i pielęgniarek, tj. użyli oni loginów im przypisanych. Liczba znaków wpisanych haseł wynosiła od 8 do 13 znaków. Po zalogowaniu się do systemu Medicus w przypadku lekarzy interfejs tego sytemu prezentował widok przeznaczony do pracy lekarzy, zaś w przypadku pielęgniarek prezentował on widok przeznaczony do pracy pielęgniarek.

W toku ww. oględzin ustalono również, że przez foldery systemowe (pulpit, obrazy, pobrane, dokumenty) stanowisk komputerowych o nr 4, 6, 12, 29, 79, 85 i 91 możliwy był swobodny dostęp każdego użytkownika danego stanowiska, a także innych osób, m.in. do znajdujących się w tych folderach plików (formatów jpeg, pdf, docx, xlsx) z informacjami zawierającymi dane osobowe pacjentów takie jak imię, nazwisko, pesel, adres zamieszkania, data urodzenia, zlecenia badań laboratoryjnych, rozpoznania, data rozpoczęcia oraz zakończenia zabiegu, rodzaj zabiegu, szczegóły opisu, zalecone badania diagnostyczne, opis uzasadnienia konieczności niezwłocznej hospitalizacji, skierowanie do szpitala, dane lekarza. Informacje zawarte w tych plikach były zapisane w postaci skanów formatu jpg (dowody osobiste, paszporty, karty ekuz), zrzutów z ekranu (informacje o pacjentach zawarte w systemu Medicus), karty segregacji medycznej (154 pliki pdf), wykazy w postaci tabelarycznych zestawień (233 strony w pliku w formacie pdf, oraz 154 pozycje wierszy w pliku w formacie xlxs), oceny ryzyka stanu odżywienia (77 plików formatu pdf). Najstarszy z tych plików został utworzony w dniu 14 listopada 2018 r., zaś najnowszy w dniu 16 grudnia 2023 r. Opisane w niniejszym akapicie ustalenia kontroli

[24] Pięć stanowisk przeznaczonych do obsługi przez pielęgniarki oraz pięć przeznaczonych do obsługi przez lekarzy.
[25] Stanowisko nr 29 i stanowisko zlokalizowane w gabinecie lekarskim Izby Przyjęć Szpitala.
[26] Stanowisko nr 92 oraz przy stanowisku zlokalizowanym w gabinecie lekarskim Izby Przyjęć Szpitala.
[27] Stanowisko nr 91.
[28] Stanowiska nr 12, 4, 79, 91, 29, 6, 18 i 85.

poczynione w toku oględzin wykazały, że w tych przypadkach nie dochowano przestrzegania wymagań określonych w ZSZ w polityce dostępu do środowiska teleinformatycznego. W dokumencie tym m.in. w sekcji 3 – podstawowe zasady dostępu określono, że dostęp do środowiska informatycznego może być przyznany w zakresie niezbędnym do realizacji zadań na rzecz Szpital, oraz że przy nadawaniu dostępu obowiązuje zasada wiedzy niezbędnej oraz zasada nieprzechodniości praw dostępu. Tymczasem funkcjonujące rozwiązania sprzętowe na stanowiskach komputerowych poddanych oględzinom, umożliwiały dostęp pracownikom korzystającym z tych samych stanowisk komputerowych do informacji, w tym m.in. plików z danymi osobowymi i medycznymi pacjentów, które znajdowały się na dyskach twardych tych stanowisk komputerowych. Było to możliwe niezależnie od tego, który z pracowników wygenerował, przetworzył i zapisał te informacje z danymi pacjentów.

W przypadku stanowiska komputerowego nr 29, znajdującego się na Izbie przyjęć, Kierownik Sekcji Informatyki oświadczył, że na tym stanowisku był wymóg uwierzytelniania użytkownika „bitlocker", tj. aby przejść do pracy na tym komputerze należało podać hasło. Oświadczył, że „bitlocker" na tym komputerze wymaga jednego hasła, które jest znane wszystkim użytkownikom tego stanowiska komputerowego. Zarówno Kierownik Sekcji Informatyki, jak i Prezes Szpitala oświadczyli, że nie pamiętali w chwili oględzin ile osób zna hasło do ww. zabezpieczenia „bitlocker" tego stanowiska komputerowego.

Prezes Szpitala wyjaśniła, że główna przyczyna ww. stanu była związana ze zidentyfikowaną potrzebą zakupu oprogramowania typu Active Directory, które zabezpieczy konta użytkowników i ograniczy dostęp do danych osobowych.

(akta kontroli str. 1019-1023, 1062-1068)

2.5.2. W toku ww. oględzin w przypadku stanowisk komputerowych wykorzystywanych przez pracowników Szpitala zatrudnionych na stanowiskach niemedycznych[29] ustalono m.in., że:

- każde stanowisko było obsługiwane przez jednego użytkownika, który posiadał swoje konto użytkowania typu lokalnego w systemie Windows 10. Wszystkie stanowiska posiadały dostęp do internetu oraz program antywirusowy Eset z aktualną bazą wirusów. W żadnym przypadku nie było możliwości podłączenia nośnika danych do portów USB, bowiem zostały one zablokowane w systemie informatycznym,
- uwierzytelnianie na każdym stanowisku odbywało się dwuetapowo, tj. w pierwszej kolejności po uruchomieniu komputera należało wprowadzić hasło do zabezpieczenia „bitlocker", zaś w drugim etapie uwierzytelniania należało wprowadzić kolejne hasło, aby zalogować się do konta użytkownika Windows. Liczba znaków haseł do systemu Windows wprowadzonych przez pracowników Szpitala wynosiła od 7 do 11 znaków. W toku oględzin na stanowisku nr 74 dokonano zmiany hasła do systemu Windows z hasła o liczbie znaków równej 7 na hasło o liczbie znaków wymaganej równej 12, tj. zgodnie z wymaganiami ZSZ, która stanowił, że minimalna liczba znaków hasła powinna wynosić 8 znaków.

  Zgodnie z punktem 3 lit. a ustęp i sekcji 6 – polityka haseł ujęta w polityce dostępu do środowiska teleinformatycznego stanowiącej element ZSZ minimalna długość hasła dla konta użytkownika wynosiła 8 znaków.
- trzech użytkowników na swoich stanowiskach komputerowych posiadało dostęp do systemów zawierających dane medyczne, tj. stanowisko nr 118 (Dietetyk), 74

[29] Stanowiska nr 72, 74, 118, 123 i 129.

(Archiwista) oraz 72 (Kierownik Sekcji Rozliczeń i Kontraktowania Świadczeń Medycznych).

(akta kontroli str. 1024-1025, 1062-1068)

2.6. Według stanu na 20 grudnia 2023 r. w Szpitalu licząc od dnia 1 stycznia 2020 r. nie stwierdzono przypadków wystąpienia incydentu zagrażającemu bezpieczeństwu systemów informacyjnych.

(akta kontroli str. 561, 1026)

2.7. W latach 2020-2023 w Szpitalu obowiązywały 22 zawarte umowy dotyczące powierzenia przetwarzania danych osobowych[30]. Ich przedmiotem były m.in. usług IT, prace serwisowe aparatury medycznej oraz usługi diagnostyczne. Szczegółowa analiza pięciu umów[31] wykazała m.in., że:

- Szpital jako administrator zobowiązany był do współdziałania z Podmiotem przetwarzającym (dalej: Procesorem lub Przetwarzającym) w wykonaniu umowy, w tym do udzielania mu pisemnych wyjaśnień w razie wątpliwości, co do legalności wydanych poleceń. Administrator lub upoważniony przez niego audytor miał prawo do przeprowadzenia audytów w zakresie sposobu przetwarzania powierzonych danych osobowych, w tym organizacyjnych i technicznych środków zastosowanych przez Procesora przy przetwarzaniu i zabezpieczeniu powierzonych danych.
- Procesor zobowiązywany był do zabezpieczenia powierzonych mu do przetwarzania danych osobowych, poprzez stosowanie odpowiednich środków technicznych i organizacyjnych, zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem, o których mowa w art. 32 RODO.
- Procesor udostępniał Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO oraz umożliwiał Administratorowi przeprowadzanie audytów, o których mowa w §3 pkt. 2-3 niniejszej umowy i przyczyniał się do nich.
- Procesor przetwarzający na podstawie dostępnych mu informacji współpracował z Administratorem przy wykonywaniu przez Administratora obowiązków określonych w art. 32-36 RODO.
- Przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych powierzonych do przetwarzania, w ciągu 24 godzin od zaistnienia naruszenia zobowiązany był poinformować o tym fakcie Administratora, za pomocą poczty elektronicznej oraz udzielić Administratorowi wyjaśnień, co do okoliczności tego zdarzenia, w tym przekazać wszelkie niezbędne dokumenty i informacje dotyczące naruszenia, co najmniej w zakresie umożliwiającym Administratorowi stwierdzenie, czy zachodzą okoliczności spełnienia obowiązku powiadomienia organu nadzorczego oraz osoby, której dane dotyczą.
- W przypadku naruszenia ochrony danych osobowych powierzonych do przetwarzania, Procesor zobowiązany był współpracować z Administratorem w podjęciu działań zaradczych, w tym w stosownych przypadkach zastosowania środków w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych osobowych.

(akta kontroli str. 1027-1061)

Stwierdzone nieprawidłowości

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

[30] Według stanu na grudzień 2023 r.

[31] Umowy z dnia 25 maja 2020 r., 26 maja 2020 r., 31 marca 2023 r., 08 września 2023 r., 3 października 2018 r., oraz z 6 listopada 2018 r.

1. W okresie od stycznia 2022 r. do 19 grudnia 2023 r. jeden były pracownik Szpitala, posiadał aktywne uprawnienia użytkownika do systemu informatycznego Medicus (opisane w punkcie 2.3. wystąpienia pokontrolnego).
2. Przetwarzanie danych osobowych pacjentów w niektórych przypadkach odbywało się niezgodnie z postanowieniami ZSZ (opisane w punktach 2.5.1. wystąpienia pokontrolnego).
3. Jeden z pracowników Szpitala, w dniu prowadzenia przez NIK oględzin stanowisk komputerowych wykorzystywanych przez pracowników Szpitala zatrudnionych na stanowiskach niemedycznych posługiwał się hasłem do systemów informatycznych o liczbie znaków niezgodnej z postanowieniami ZSZ (opisane w punktach 2.5.2. wystąpienia pokontrolnego).
4. Nadzór nad realizacją obowiązujących w Szpitalu rozwiązań w zakresie zapewnienia bezpieczeństwa informacji, w tym danych osobowych pacjentów nie był w pełni skuteczny (opisane w punktach 2.5.1. i 2.5.2. wystąpienia pokontrolnego).

OCENA CZĄSTKOWA

Zapewnienie bezpieczeństwa informacji, w tym danych pacjentów przez niektórych pracowników medycznych Szpitala odbywało się w sposób odbiegający od wymagań określonych w sekcji 3 – podstawowe zasady dostępu, ujętych w polityce dostępu do środowiska teleinformatycznego stanowiącej element ZSZ, co wykazały przeprowadzone przez NIK oględziny. Pomimo kierowania się przez Sekcję Informatyki zasadą przyznawania pracownikom dostępu do środowiska informatycznego w zakresie niezbędnym do realizacji ich zadań, funkcjonujące rozwiązania sprzętowe i systemowe umożliwiały dostęp pracownikom korzystającym z tych samych stanowisk komputerowych do informacji, w tym m.in. plików z danymi osobowymi i medycznymi pacjentów, które znajdowały się na dyskach twardych tych stanowisk komputerowych. Było to możliwe niezależnie od tego, który z pracowników wygenerował, przetworzył i zapisał te informacje z danymi pacjentów. W ocenie NIK powyższy stan wskazuje, że nadzór nad przestrzeganiem przez pracowników Szpitala zasad określonych w ZSZ był nieskuteczny. W przypadku personelu niemedycznego dochowano natomiast właściwej realizacji obowiązującego w Szpitalu ZSZ, tj. uprawnienia dostępu do informacji zawierających dane pacjentów posiadali w niezbędnym zakresie pracownicy realizujący zadania związane z przetwarzaniem danych pacjentów, jak np. statystyk, dietetyk czy archiwista. Szpital zawierał umowy powierzenia przetwarzania danych osobowych zawierające postanowienia zgodne z obowiązującymi przepisami rozporządzenia RODO.

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, nie formułuje uwag, a przedstawia następujący wniosek:

Wnioski

Zwiększenie nadzoru w zakresie realizacji przez osoby zatrudnione w Szpitalu wymogów określonych w ZSZ.

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 wniosku pokontrolnego 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, 13 lutego 2024 r.

Kontroler
Bartosz Kościukiewicz
główny specjalista kontroli państwowej

.....
podpis

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

.....
podpis