NAJWYŻSZA IZBA KONTROLI
Delegatura w Szczecinie

LSZ.410.002.02.2019

Pan Andrzej Kondaszewski
Szpital Wojewódzki
im. Mikołaja Kopernika w Koszalinie,
ul. Tytusa Chałubińskiego 7,
75-581 Koszalin

WYSTĄPIENIE POKONTROLNE

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

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

I. Dane identyfikacyjne

Jednostka kontrolowana	Szpital Wojewódzki im. Mikołaja Kopernika w Koszalinie, ul. T. Chałubińskiego 7, 75-581 Koszalin.
Kierownik jednostki kontrolowanej	Andrzej Kondaszewski, Dyrektor Szpitala, od 1 września 2009 r.
Zakres przedmiotowy kontroli	1. Opracowanie wymaganej dokumentacji oraz procedur związanych z ochroną przetwarzanych danych osobowych. 2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych.
Okres objęty kontrolą	Od 25 maja 2018 r. do dnia zakończenia czynności kontrolnych.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[1].
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Szczecinie
Kontroler	Krzysztof Szczepaniak, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LSZ/41/2019 z 12.02.2019 r. (akta kontroli str. 1-3)

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

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

W Szpitalu dane osobowe nie były w pełni prawidłowo chronione i przetwarzane.

Szpital wywiązał się z obowiązku powołania Insektora Ochrony Danych[3] i zgłoszenia tego faktu Prezesowi Urzędu Ochrony Danych Osobowych. Zagwarantowano niezależność wyznaczonemu IOD w sprawowaniu jego funkcji. Stanowisko to nie było uwzględnione w regulaminie organizacyjnym szpitala. Przeprowadzono wymaganą analizę ryzka procesów przetwarzania danych osobowych. Zapewniono całemu personelowi Szpitala szkolenia związane z wejściem w życie RODO, a części pracowników szkolenia związane z bezpieczeństwem danych. Zaprowadzono rejestr czynności przetwarzania lecz prowadzono go tylko w formie pisemnej. Wprowadzone rozwiązania organizacyjne, zmierzające do zapewnienia ochrony danych osobowych pacjentów, z wyjątkiem Przychodni Onkologiczej, gwarantowały poszanowanie ich prywatności. Personelowi szpitala zapewniono dostęp do danych medycznych adekwatny do realizowanych zadań i obowiązków.

Szpital nie opracował i nie wdrożył dokumentacji oraz procedur dotyczących ochrony danych osobowych w oparciu o ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych[4] oraz przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[5]. Do dnia kontroli NIK[6], powołany przez Dyrektora Szpitala zespół do opracowania projektu Polityki Ochrony Danych Osobowych, nadal pracował nad jego treścią.

Wystąpiły przypadki nadania zbyt dużych uprawnień użytkownikom komputerów, braku skutecznej ochrony antywirusowej oraz logowanie do sieci szpitala jednego byłego pracownika co stanowiło naruszenie art. 5 pkt 1 lit. f RODO oraz § 20 ust. 2 pkt 7 i 12 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]. Dostawcy oprogramowania wysłano w zgłoszeniu serwisowym nadmiarowe dane pacjenta, co nie było konieczne do naprawy usterki. Przy rejestracji pacjentów w Przychodni Onkologicznej nie zapewniono w pełni prawa pacjenta do zachowania w tajemnicy informacji z nim związanych co stanowiło naruszenie art. 13 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta[8]. Nie przestrzegano w pełni zasad przechowywania dokumentacji medycznej pacjentów w gabinecie lekarskim na jednym z oddziałów, a pacjentów zaopatrywano w opaski zawierające ich pełne dane czym naruszono art. 36 ust. 5 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej[9].

[2] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.
[3] Dalej: IOD.
[4] Dz. U. z 2018 r., poz. 1000 ze zm.; dalej: u.o.d.o.
[5] Dz. Urz. UE L 119 z 4 maja 2016 r., str. 1, ze zm.; dalej: RODO.
[6] 28 marca 2019 r.
[7] Dz. U. z 2017 r. poz. 2247; dalej: KRI.
[8] Dz. U. z 2017 r. poz. 1318, ze zm.
[9] Dz. U. z 2018 r., poz. 2190 ze zm.; dalej: ustawa o działalności leczniczej.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[10] kontrolowanej działalności

OBSZAR

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

Opis stanu faktycznego

1.1. Szpital z dniem 25 maja 2018 r. wyznaczył IOD, wywiązując się tym samym z obowiązku określonego w art. 8 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[11]. Osoba ta do 24 maja 2018 r. pełniła obowiązki Administratora Bezpieczeństwa Informacji w Szpitalu[12]. W myśl art. 8 i art. 10 u.o.d.o., Szpital terminowo wywiązał się z obowiązku zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu IOD (19 czerwca 2018 r. formularzem elektronicznym). Przekazane zawiadomienie zawierało wszystkie elementy określone w art. 10 ust. 3 u.o.d.o. Dane IOD oraz sposób i formę kontaktu udostępniono na stronie internetowej Szpitala – wymóg art. 37 ust. 7 RODO. W zakresie obowiązków IOD wskazano wszystkie zadania określone w art. 39 RODO. IOD umożliwiono wykonywanie obowiązków w sposób niezależny, stosownie do art. 38 ust. 3 RODO. Samodzielne stanowisko IOD, podległe było bezpośrednio Dyrektorowi Szpitala. Nie zostało ono wyodrębnione w strukturze organizacyjnej Szpitala co szerzej zostało opisane w dalszej części wystąpienia w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 4-54, 57-58)

Zgodnie z wymogami art. 37 ust. 5 RODO, IOD miał należyte przygotowanie i kwalifikacje zawodowe do pełnienia swojej funkcji. Wcześniej był Administratorem Bezpieczeństwa Informacji w Szpitalu, posiadał ukończone w 2017 r. studia podyplomowe w zakresie administratora bezpieczeństwa informacji[13]. Ponadto posiadał certyfikat potwierdzający uzyskanie w 2017 r. kompetencji audytora wewnętrznego systemu zarządzania.

(akta kontroli str. 59-66)

Do dnia zakończenia kontroli (28 marca 2019 r.) do Szpitala nie wpłynęła decyzja właściwego organu do spraw cyberbezpieczeństwa o uznaniu Szpitala za operatora usługi kluczowej, o której mowa w art. 5 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[14].

(dowód: akta kontroli str. 72)

1.2. W dniu wejścia w życie przepisów RODO oraz u.o.d.o. (25 maja 2018 r.) Szpital nie posiadał aktualnej dokumentacji wewnętrznej, uwzględniającej powyższe przepisy. W Szpitalu funkcjonowała Polityka bezpieczeństwa (PB) oraz Instrukcja zarządzania systemem informatycznym (IZSI) przyjęta zarządzeniem Dyrektora Szpitala w dniu 6 listopada 2013 r.[15] PB określała: zakres oraz zasady zabezpieczenia danych osobowych, obowiązki osób pełniących funkcje Administratorów, przetwarzanie danych osobowych, postępowanie w przypadku naruszenia ochrony danych osobowych oraz sposób sprawowania kontroli nad przestrzeganiem ochrony danych osobowych. Powyższe dokumenty opracowane

[10] 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.

[11] Dz. U. z 2018 r. poz. 1000, ze zm.; dalej: u.o.d.o.

[12] Powołana na to stanowisko w dniu 1 lutego 2016 r.

[13] Akademia Marynarki Wojennej w Gdyni.

[14] Dz. U. poz. 1560, dalej: ustawa o cyberbezpieczeństwie.

[15] Zarządzenie nr 161/13 Dyrektora Szpitala z 6.11.2013 r. w sprawie Polityki Bezpieczeństwa, Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz Regulaminu korzystania ze sprzętu, oprogramowania oraz infrastruktury będących na wyposażeniu Szpitala.

zostały w oparciu o przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz o akty wykonawcze wydane na podstawie tej ustawy. Do dnia kontroli powyższe dokumenty były zmieniane trzykrotnie:
- dwukrotnie w 2016 r. - dopisano do załącznika nr 4 system ESKULAP oraz zamieszczono informację o wygasaniu systemu SOLMED, dopisano program MARCEL do załącznika nr 5 i nr 6[16], w zakresie treści § 10 dotyczącego lokalizacji obszarów przetwarzania danych oraz wprowadzono załącznik nr 11 określający rozmieszczenie programów i systemów informatycznych[17],
- w 2017 r. – w związku z nowelizacją ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych dokonano zmiany treści rozdziału 5 – Przetwarzanie danych osobowych i dopisano do PB załącznik nr 11 (Ramowy program szkoleń)[18], w związku ze zmianą ustawy z dnia 23 marca 2017 r. o zmianie ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta dokonano zmiany[19] Rozdziału 5 – Przetwarzanie danych osobowych oraz dopisano załączniki nr 8A[20] i 8B[21].

(akta kontroli str. 73-146)

IZSI zawierała :
- procedury nadawania i zmiany uprawnień do przetwarzania danych,
- stosowane techniki i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem,
- procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu,
- sposób i miejsce przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz wydruków,
- sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest dostęp lub uszkodzenie systemu informatycznego,
- zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych,
- procedury wykonywania przeglądów i konserwacji systemu.

Zmiany do IZSI wprowadzono w 2017 r. Dokonano zmiany treści rozdziału 2 Procedury nadawania i zmiany uprawnień do przetwarzania danych[22], w związku z dostosowaniem systemu bezpieczeństwa informacji Szpitala do wymogów rozporządzenia KRI.

(akta kontroli str. 73, 99-115, 125-128)

Treść PB oraz IZSI była przekazana w formie papierowej do kierowników wszystkich komórek organizacyjnych Szpitala z obowiązkiem zapoznania z ich treścią podległych pracowników. Kolejne zmiany wprowadzane zarządzeniami Dyrektora upowszechniane były drogą mailową do wszystkich kierowników komórek organizacyjnych oraz zostały udostępniane w wersji elektronicznej w Intranecie.

(akta kontroli str. 73, 116, 122-123, 125, 129, 135)

Po wejściu w życie RODO, zaktualizowano PB w zakresie zmiany załącznika nr 8 dotyczącego upoważnienia do przetwarzania danych oraz dodano postanowienie o zachowaniu poufności i nie ujawnianiu informacji[23].

W Szpitalu opracowano także procedury wewnętrzne:

[16] Zarządzenie nr 58/2018 z 25.04.2016 r.

[17] Zarządzenie nr 79/2016 z 7.06.2016 r.

[18] Zarządzenie nr 26.17 z 25.01.2017 r.

[19] Zarządzenie nr 135.2017 z 13.07.2017 r.

[20] Wzór upoważnienia do przetwarzania danych osobowych dla osób, o których mowa w § 41 ust. 2 PB.

[21] Wzór upoważnienia do przetwarzania danych osobowych dla osób odbywających zajęci praktyczne i praktyki zawodowe.

[22] Zarządzenie nr 25.17 z 25.01.2017 r.

[23] Zarządzenie nr 78/2018 z 5.06.2018 r.

- instrukcję postępowania w sytuacji naruszenia bezpieczeństwa informacji[24],
- zasady udostępniania indywidualnej dokumentacji medycznej pacjentów[25],
- Rejestr Czynności Przetwarzania z instrukcją jego prowadzenia[26],
- powierzenie przetwarzania danych osobowych/informacji[27].

(akta kontroli str. 162-170, 191-206, 448-453, 525-541)

1.3. Zarządzeniem nr 79/2018 Dyrektora Szpitala z 6 czerwca 2018 r. wprowadzono Rejestr Czynności Przetwarzania w Szpitalu. Obowiązek prowadzenia Rejestru nałożony został na kierowników komórek organizacyjnych Szpitala, zgodnie z przypisanymi do stanowiska pracy czynnościami związanymi z przetwarzaniem danych osobowych i prowadzony był wg stanowisk pracy. Nadzór nad prowadzeniem Rejestru powierzono IOD. Rejestr zawierał wszystkie informacje wymagane art. 30 ust. 1 RODO, z wyjątkiem informacji zawierającej imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, co opisano w dalszej części wystąpienia w sekcji *Stwierdzone nieprawidłowości.*. Informacje zawarte w Rejestrze stanowiły w Szpitalu m.in. podstawę do określenia zakresu upoważnienia pracownika do przetwarzania danych osobowych, w tym uprawnień do systemu informatycznego zgodnie z opisem czynności przetwarzania danych osobowych wykazanym w Rejestrze.

(akta kontroli str. 162-187)

1.4. W ramach Procedury Zintegrowanego Systemu Zarządzania Jakością wg normy PN-EN ISO 9001:2015, w związku z wdrożeniem postępowania w zakresie zarządzania ryzykiem[28] zespół pracowników Szpitala dokonał analizy[29] zachodzących procesów pod kątem analizy i oceny zidentyfikowanego ryzyka w tym dotyczących przetwarzania danych osobowych. W rejestrze ryzyk zidentyfikowano m.in. sześć procesów związanych z przetwarzaniem danych osobowych, tj. przetwarzanie danych z naruszeniem przesłanek zgodności przetwarzania z prawem (art. 6 ust. 1 RODO); przetwarzanie danych z naruszeniem przesłanek dopuszczających legalność przetwarzania (art. 9 ust. 1 i 2 RODO); niewłaściwe zabezpieczenie danych osobowych; brak upoważnień do przetwarzania danych; naruszenie zasad powierzenia danych osobowych oraz naruszenie bezpieczeństwa danych osobowych. Prawdopodobieństwo wystąpienia tych zagrożeń określono na poziome trzecim w pięciostopniowej skali (z wyjątkiem braku upoważnień do przetwarzania danych, dla którego prawdopodobieństwo określono na poziomie drugim). Dla pierwszych pięciu zagrożeń oszacowano skutek na poziomie od trzeciego do czwartego w pięciostopniowej skali, a dla ostatniego czynnika ryzyka na maksymalnym piątym poziomie. Analizowane zagrożenia mieściły się w obszarze ryzyka kontrolowanego wymagającego monitorowania procesów, a tylko w indywidualnych wypadkach podjęcia dalszych działań. Podejmowane działania zaradcze polegały na prowadzeniu szkoleń, monitorowaniu przez IOD przestrzegania zgodności przetwarzania danych osobowych z wymogami RODO, sprawdzeniach doraźnych prowadzonych przez IOD, nadzorze przez IOD nad rejestrem czynności przetwarzania oraz ewidencją osób upoważnionych, konsultacjach w fazie projektowania umów powierzenia oraz prowadzeniu postępowań wyjaśniających w sytuacji naruszenia bezpieczeństwa danych osobowych.

(akta kontroli str. 219-265)

[24] Zarządzenie nr 44.2019 Dyrektora Szpitala z 21.02.2019 r.

[25] Zarządzenie nr 1.2019 Dyrektora Szpitala z 3.01.2019 r., zmienione zarządzeniami nr 11.2019 i 58.2019.

[26] Zarządzenie nr 79.2018 Dyrektora Szpitala z 6.06.2018 r.

[27] Zarządzenie nr 73.2018 Dyrektora Szpitala z 24.05.2018 r.

[28] Zarządzenie nr 48.2018 Dyrektora Szpitala z 28.03.2018 r. w sprawie wdrożenia sposobu postępowania w zakresie zarządzania ryzykiem.

[29] Zatwierdzona przez Dyrektora Szpitala 2 lipca 2018 r.

IOD wyjaśniła, że od 2016 r. jako Administrator Bezpieczeństwa Informacji prowadziła sprawdzenia zgodności przetwarzania danych osobowych na podstawie art. 36a ust. 2 ustawy o ochronie danych osobowych, w ramach których od 9.09.2016 r. kontrolowane były m.in. zbiory danych przetwarzanych w Szpitalu pod kątem rodzaju zbieranych danych i jego celu oraz podstawy prawnej ich zbierania, sposób zabezpieczenia zbiorów zawierających dane osobowe na nośnikach papierowych, umowy powierzenia, proces rekrutacji w zakresie zbioru danych osobowych, zakres danych rejestrowanych w monitoringu wizyjnym, zakres danych zawartych w fakturach. Zgodnie z §3 ust. 6 rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji[30], sprawdzenia dokonuje się co najmniej raz na pięć lat. Od sprawdzenia upłynęły niecałe 3 lata. Obecnie, powołany przez Dyrektora Szpitala Zespół do Opracowania Projektu Oceny Skutków Ochrony Danych pracuje nad projektem analizy zachodzących procesów przetwarzania danych osobowych oraz oszacowaniem ryzyka.

(akta kontroli str. 217)

W sprawie sposobu określenia listy procesów związanych z przetwarzaniem danych osobowych IOD wyjaśniła, że lista procesów związanych z przetwarzaniem danych osobowych powstała na podstawie własnych przemyśleń oraz obserwacji sposobu przetwarzania danych osobowych. Ponadto źródłem informacji była treść pytań zadawanych z poszczególnych komórek organizacyjnych Szpitala przetwarzających dane osobowe. Lista procesów nie została zamknięta i podlega corocznej aktualizacji i uzupełnieniom.

(akta kontroli str. 217-218)

1.5. Szpital nie przeprowadzał oceny skutków dla operacji przetwarzania danych osobowych, o której mowa w art. 35 RODO[31]. Obowiązek wykonania tej oceny dotyczy bowiem planowanych operacji przetwarzania dla ochrony danych osobowych przed rozpoczęciem ich przetwarzania, a Szpital, wraz z wejściem w życie RODO, nie rozpoczął przetwarzania nowych kategorii danych, w szczególności z użyciem nowych technologii. Również Prezes Urzędu Ochrony Danych Osobowych[32] w komunikacie[33] wydanym na podstawie art. 35 ust. 4 RODO wśród rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony, nie wskazał danych medycznych przetwarzanych w szpitalach, jako wymagających przeprowadzenia takiej oceny. Pojedyncza (bieżąca) ocena operacji wiążących się z wysokim ryzykiem jest również fakultatywna, przy czym Grupa Robocza Art. 29 ds. Ochrony Danych[34] zdecydowanie zalecała dokonanie DPIA dla operacji przetwarzania już trwających przed 25 maja 2018 r.[35] oraz w przypadkach, gdy nie jest jasne, czy wymagana jest DPIA, ponieważ jest ona „przydatnym narzędziem, które może pomóc administratorom danych w zapewnieniu zgodności z prawem ochrony danych".

[30] Dz.U. poz. 745; uchylone z dniem 6.02.2019 r.

[31] Dalej: DPIA.

[32] Dalej: Prezes UODO.

[33] Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 sierpnia 2018 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (M. P. poz. 827).

[34] Grupa Robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Była ona niezależnym organem doradczym w zakresie ochrony danych i prywatności. Zadania grupy określone są w art. 30 dyrektywy 95/46/WE oraz art. 15 dyrektywy 2002/58/WE.

[35] Dokument pt.: Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) oraz ustalenia, czy przetwarzanie „z dużym prawdopodobieństwem może powodować wysokie ryzyko", do celów rozporządzenia 2016/679 https://www.giodo.gov.pl/1520281/id_art/9957/j/pl.

IOD wyjaśniła, że ocena skutków dla ochrony danych została przeprowadzona kompleksowo w ramach Zintegrowanego Systemu Zarzadzania Jakością, która objęła czynniki ryzyka, prawdopodobieństwo wystąpienia, ocenę skutków oraz określono reakcję na ryzyko. Dla każdego procesu w Polityce zamieszczono opis podjętych działań oraz osoby odpowiedzialne.

(akt kontroli str. 217-218)

IOD w wyjaśnieniu powołał się na analizy i oceny ryzyka działalności Szpitala sporządzone na potrzeby Zintegrowanego Systemu Zarzadzania Jakością. Zdaniem NIK, nie miały one cech wymaganych przy ocenie skutków dla ochrony danych, o których mowa w art. 35 RODO, w szczególności określonych w art. 35 ust. 7 RODO.

1.6. Szkoleniami obejmującymi zagadnienia z zakresu RODO, klasyfikacji informacji w Szpitalu, procedur bezpieczeństwa informacji obowiązujących w Szpitalu, zagrożeń bezpieczeństwa danych osobowych, form naruszenia bezpieczeństwa danych osobowych / informacji objęto wszystkich pracowników Szpitala:
- w ramach adaptacji zawodowej w 2017 r. - 214 osób (43 szkolenia), w 2018 r. - 274 osoby (51 szkoleń) oraz 55 osób w 2019 r. (17 szkoleń) (do 15 marca 2019 r.);
- szkolenie uzupełniające podstawowe w 2018 r. - 288 osób – 37 szkoleń (ponadto 214 osób z zakresu zasad bezpiecznej pracy w sieci komputerowej Szpitala jako element środków organizacyjno technicznych ochrony danych osobowych – 41 szkoleń), w 2019 r. – 21 osób (1 szkolenie);
- szkolenie okresowe w formie testu w 2018 r. - 451 osób.

Według stanu na 28.02.2019 r. w Szpitalu było zatrudnionych 1 226 osób. Szkoleniami z realizacji zadań w sposób uwzględniające wymogi RODO objęto 100% pracowników, tj. za lata 2018 - 2019 łącznie 1 277 osób, tj. 538 osób w ramach adaptacji zawodowej (pracownicy nowo zatrudnieni), 288 osób w ramach szkolenia uzupełniającego oraz 451 w formie szkolenia okresowego.
W okresie objętym kontrolą (od 25 maja 2018 r.) przeszkolono łącznie 939 osób (76,6% z liczby 1 226 osób), tj. 451 w ramach szkolenia okresowego w formie testu, 217 w ramach adaptacji zawodowej oraz 271 w ramach szkolenia uzupełniającego.
Szkolenia osób zaangażowanych w proces przetwarzania informacji (o których mowa w § 20 ust. 2 pkt 6 rozporządzenia KRI), które uwzględniały zagadnienia w pełnym zakresie obejmującym zagrożenia bezpieczeństwa informacji, skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawną oraz stosowanie środków zapewniających bezpieczeństwo informacji (np. szyfrowanie dysków, szyfrowanie kluczy USB, dostęp do systemów IT po podaniu hasła) przeprowadzono dla 214 osób.

(akta kontroli str. 266-267)

1.7. W sprawie stosowania w Szpitalu kodeksów dobrych praktyk *Kodeksu postępowania dla sektora ochrony zdrowia* lub wskazówek zawartych w przewodniku po RODO dla służby zdrowia, opublikowanych 24 września 2018 r. na stronie Ministerstwa Cyfryzacji[36] IOD wyjaśnił, że kodeksy postępowania dla sektora służby zdrowia znajdują się w fazie projektów przekazanych pod opinię Prezesa Urzędu Ochrony Danych Osobowych. Do chwili ich akceptacji, Szpital nie może stosować projektów. W praktyce Szpital korzysta ze wskazówek zawartych w przewodniku po RODO w służbie zdrowia. Treść przewodnika i komunikat z zaleceniem stosowania wskazówek zawartych w tym dokumencie został rozpowszechniony w Intranecie. Ponadto zalecenie do stosowania przewodnika zostało przekazane na spotkaniu kierowników komórek organizacyjnych Szpitala

[36] https://www.gov.pl/cyfryzacja/rodo-w-sluzbie-zdrowia-po-pierwsze-pacjent, dostęp z dnia 3 października 2018 r.

zaraz po publikacji na stronie Ministerstwa Cyfryzacji. Na szkoleniach adaptacyjnych IOD omawiał zagadnienia zawarte w przewodniku i zalecał ich stosowanie.

(akta kontroli str. 268)

Stwierdzone nieprawidłowości

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

1. W strukturze organizacyjnej Szpitala, określonej regulaminem organizacyjnym nie uwzględniono stanowiska IOD, jak również nie określono jego zadań oraz stopnia podległości. Zgodnie z treścią § 12 ust. 2 Statutu Szpitala nadanego uchwałą nr XXVIII/437/17 Sejmiku Województwa Zachodniopomorskiego z dnia 21 listopada 2017 r. i zmienionego uchwałą nr XXV/545/18 z dnia 26 września 2018 r., szczegółową strukturę organizacyjną określa regulamin organizacyjny Szpitala ustalany przez Dyrektora. W dniu 19 czerwca 2018 r. zawiadomiono Prezesa Urzędu Ochrony Danych Osobowych o pełnieniu funkcji Inspektora Ochrony Danych przez Annę Kobusińską, która poprzednio pełniła funkcję Administratora Bezpieczeństwa Informacji. W treści Regulaminu Organizacyjnego Szpitala wprowadzonego zarządzeniem nr 179/12 Dyrektora Szpitala z 5 grudnia 2012 r. wraz ze zmianami (ostatnia zmiana dokonana zarządzeniem nr 149/15 z 15 października 2015 r.) nie figurowało stanowisko Inspektora Ochrony Danych.

(akta kontroli str. 4-56)

Dyrektor Szpitala wyjaśnił, że pracownik merytorycznie odpowiedzialny za aktualizowanie zapisów w regulaminie organizacyjnym, przedstawił wyjaśnienie w sprawie nieuwzględnienia tego stanowiska w strukturze organizacyjnej Szpitala. W dniu 25 lutego 2019 r. przeprowadzono z pracownikiem rozmowę dotyczącą aktualizowania treści regulaminu organizacyjnego (…) w chwili obecnej trwają prace nad projektem nowego regulaminu organizacyjnego, których zakończenie planowane jest do końca marca 2019 r. Inspektor ds. Organizacyjnych Szpitala wyjaśniła, że zaległość w aktualizacji regulaminu organizacyjnego spowodowana była różnorodnością dziedzin i szerokim zakresem merytorycznym obowiązków i zadań oraz dynamicznymi zmianami priorytetów podejmowanych działań na jej stanowisku pracy.

(akta kontroli str. 148-156)

2. Do dnia zakończenia kontroli NIK nie opracowano i nie wprowadzono do stosowania polityki ochrony danych osobowych opartej o przepisy u.o.d.o. oraz przepisy rozporządzenia RODO. Dyrektor 14 czerwca 2018 r.[37] powołał zespół do opracowania projektu Polityki Ochrony Danych Osobowych, który do 31 sierpnia 2018 r. miał opracować przedmiotowy Projekt. Pomimo upływu 9 miesięcy od daty powołania zespołu, do dnia zakończenia kontroli NIK nie opracowano odpowiedniej aktualizacji PB oraz IZSI. Stanowiło to naruszenie przepisów art. 24 ust. 1 i 2 RODO, zgodnie z którymi do obowiązków ADO należało m.in. poddawanie przeglądom i aktualizacja przyjętych polityk ochrony danych i regulacji wewnętrznych w tym zakresie.

(akta kontroli str. 142-147)

Dyrektor Szpitala wyjaśnił, że *ze względu na złożoność zagadnień prawnych, brak aktów wykonawczych, okres urlopowy pracowników, a także dużą ilość przetwarzanych w Szpitalu danych osobowych opracowanie projektu zostało opóźnione.*
Wobec braku wytycznych Urzędu Ochrony Danych Osobowych co do układu treści i istotnych elementów, jakie powinna zawierać polityka, członkowie Zespołu

[37] Zarządzeniem 89/2018 z 14.06.2018 r.

dokonali przeglądu środków organizacyjno – technicznych i opracowali projekt, który w założeniu obejmuje zagadnienia ochrony danych osobowych uregulowane również polityką bezpieczeństwa. (…).
Przygotowany projekt został przedstawiony do zaopiniowania Zespołowi Radców Prawnych. W chwili obecnej trwają prace nad wprowadzeniem zmian zgodnie z opinią Zespołu Radców Prawnych. Po wdrożeniu Polityki Ochrony Danych Osobowych zostanie uaktualniona PB i IZSI, w oparciu o rekomendacje Centrum Systemów Informacyjnych Ochrony Zdrowia w zakresie bezpieczeństwa oraz rozwiązań technologicznych stosowanych podczas przetwarzania dokumentacji medycznej w postaci elektronicznej.

(akta kontroli str. 148-149, 151-154)

3. Zarówno we wzorze rejestru, stanowiącym załącznik do zarządzenia 79/2018 z 6.06.2018 r. jak też w prowadzonym rejestrze nie uwzględniono elementu wymaganego przepisami art. 30 ust 1 lit. a) RODO, tj. informacji zawierającej imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie - przedstawiciela administratora oraz inspektora ochrony danych.

IOD wyjaśniła, że w trakcie prac nad treścią tego zarządzenia, zespół pracujący pod przewodnictwem Pielęgniarki Naczelnej i jego udziałem przeoczył ten element, skupiając się na pozostałych elementach. W trakcie prac nad wzorem rejestru korzystano ze wzorów zamieszczonych na stronie UODO, w których również nie było wskazanej w art. 30 ust. 1 lit. a RODO informacji. Zbiór kart[38] prowadzonych dla stanowisk w poszczególnych komórkach organizacyjnych Szpitala, zawiera stronę tytułową z podaniem nazwy administratora, tj. Szpital Wojewódzki im. Mikołaja Kopernika w Koszalinie wraz z nazwą komórki organizacyjnej, której dotyczy ten fragment Rejestru. Na pieczątce podano dane kontaktowe do komórki organizacyjnej wraz z numerami telefonów i adresem Szpitala.

(akta kontroli str. 188)

NIK nie podziela stanowiska IOD w powyższej sprawie gdyż przywołany w wyjaśnieniu wzór, zamieszczony na stronie UODO[39] zawiera wszystkie elementy wymagane przepisami art. 30 ust. 1 RODO.

4. ADO nie prowadził Rejestru Czynności Przetwarzania w formie elektronicznej. Zgodnie zaś z treścią art. 30 ust. 3 rejestr powinien mieć formę pisemną w tym formę elektroniczną. Rejestr prowadzony indywidualnie dla każdej komórki organizacyjnej Szpitala nie był przekazywany w formie elektronicznej do IOD, stąd inspektor nieposiadając takiej postaci rejestru – nie agregował danych do jednego dokumentu elektronicznego (np. excel lub word)[40].

   IOD, nadzorująca prowadzenie rejestru wyjaśniła, że Szpital nie posiada systemu umożliwiającego prowadzenie rejestru w formie elektronicznej. Zakupiony przed 2018 r. program ENOVA nie zawierał możliwości rejestrowania czynności przetwarzania danych osobowych w oparciu o obowiązkowe składniki rejestru. Urząd Ochrony Danych Osobowych we „Wskazówkach i wyjaśnieniach dotyczących obowiązku rejestrowania czynności i kategorii przetwarzania określonego w art. 30 ust. 1 i 2 RODO" na stronie 13 wskazuje, iż RODO nie narzuca wymagań dotyczących postaci,

[38] Kierownicy komórek organizacyjnych Szpitala prowadzili rejestr czynności przetwarzania zgodnie z przypisanymi do stanowiska pracy czynnościami związanymi z przetwarzaniem danych.

[39] https://uodo.gov.pl/pl/123/214 znajduje się rejestr czynności przetwarzania prowadzony w Excelu - przykład dla szkoły. W pierwszym arkuszu „Informacje" są dane administratora i IOD, w drugim zaś arkuszu jest rejestr czynności przetwarzania z danymi.

[40] Na stronie internetowej UODO https://uodo.gov.pl/pl/123/214 wzór rejestru ma formę dokumentu excel.

w jakiej rejestry powinny być prowadzone, wskazując, że może to być postać zarówno papierowa, jak i elektroniczna". Mając na względzie powyższe, w Szpitalu przyjęto do prowadzenia formę papierową rejestru."

(akta kontroli str. 189-190)

Najwyższa Izba Kontroli wskazuje na treść 30 ust. 3 RODO, zgodnie z którą rejestry oprócz formy pisemnej mają formę elektroniczną co wskazuje jednoznacznie na obowiązek prowadzenia ich również w formie elektronicznej. Wzór rejestru podany na stronie UODO pod adresem https://uodo.gov.pl/pl/123/214 jest w formie excela. Nie jest oczekiwane używanie specjalistycznego oprogramowania do prowadzenia rejestru, wystarczy posiadany pakiet oprogramowania biurowego.

OCENA CZĄSTKOWA

Szpital nie opracował i nie wdrożył dokumentacji oraz procedur dotyczących ochrony danych osobowych w oparciu o u.o.d.o. oraz przepisy RODO – pomimo powołania do tego celu zespołu. Prawidłowo powołano IOD i terminowo przesłano do Prezesa Urzędu informacje o jego powołaniu. Zagwarantowano niezależność wyznaczonemu IOD w sprawowaniu jego funkcji. Stanowisko to nie było uwzględnione w regulaminie organizacyjnym Szpitala. Dokonano oceny skutków dla ochrony danych osobowych pacjentów. Zapewniono całemu personelowi Szpitala szkolenia związane z wejściem w życie RODO oraz części pracowników szkolenia związane z bezpieczeństwem danych. Zaprowadzono rejestr czynności przetwarzania lecz prowadzono go tylko w formie pisemnej.

OBSZAR

2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych.

Opis stanu faktycznego

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

- na żadnym z pięciu badanych oddziałach Szpitala[41] na łóżkach szpitalnych nie było kart pacjentów z ich nazwiskiem i wynikami pomiarów temperatury ciała, ciśnienia tętniczego lub innymi informacjami o stanie zdrowia;
- pacjenci badanych oddziałów posiadali na nadgarstkach opaski z zawierające ręcznie wypisane pełne dane dotyczące imienia, nazwiska i numer PESEL. Szpital nie posiadał specjalistycznej drukarki do wydruków opasek;
- w dyżurkach pielęgniarskich na objętych oględzinami oddziałach szpitalnych ruch chorych prowadzony był elektronicznie z wykorzystaniem modułu RUCH CHORYCH w ramach eksploatowanego w Szpitalu systemu ESKULAP. Podręczna dokumentacja (karty gorączkowe) przechowywane były w szafkach lub szufladach biurek zamykanych na klucz. Z wyjątkiem gabinetu lekarskiego Oddziału Laryngologii, dokumentacja medyczna w gabinetach lekarskich na pozostałych czterech oddziałach znajdowała się w szafkach zamykanych na klucz;
- personel pielęgniarski we wszystkich objętych oględzinami oddziałach szpitalnych, opuszczając dyżurkę pielęgniarek, każdorazowo blokował dostęp do komputerów.

(dowód: akta kontroli str. 279-295)

Proces rejestracji do poradni specjalistycznych Szpitala podzielony został funkcjonalnie wg zakładów leczniczych oraz specyfiki wybranych poradni. Rejestracje funkcjonowały w zakładzie leczniczym „Ambulatoryjna Opieka

[41] Oddział Ginekologiczno-Położniczy, Oddział Patologii Ciąży, Oddział Dermatologii, Oddział Laryngologii z Pododdziałem Chirurgii Stomatologicznej z Blokiem Operacyjnym, Oddział Chirurgii Dziecięcej i Urazowo – Ortopedycznej z Blokiem Operacyjnym, łącznie 31 sal dysponujących 78 łóżkami oraz 46 zaobserwowanych pacjentów.

Specjalistyczna", w ośmiu indywidualnych poradniach specjalistycznych[42], Przychodni Kompleksowej Rehabilitacji oraz w Przychodni Onkologicznej. Oględziny trzech wybranych rejestracji[43] wykazały, że:

- Przychodnia Kompleksowej Rehabilitacji - proces rejestracji odbywał się w sposób uniemożliwiający przez osoby oczekujące na rejestrację usłyszenia danych osobowych lub wglądu w dokumenty osoby obsługiwanej w pokoju rejestracji. Na tablicy wywieszono klauzulę informacyjną o przetwarzaniu danych osobowych.

- Przychodnia Onkologiczna - proces rejestracji odbywał się przy dwóch okienkach, przy pierwszym pacjent zgłaszający się do rejestracji znajdował się w bezpośrednim sąsiedztwie innych pacjentów stojących w kolejce bez zapewnienia odstępu pomiędzy osobą obsługiwaną a pacjentami w kolejce tak aby pacjenci w kolejce nie mogli słyszeć treści rozmowy pacjenta z personelem rejestrującym. Przy okienku tym brakowało zasłony (przepierzenia) uniemożliwiającej uzyskanie wglądu przez kolejną osobę w kolejce w dokumenty osoby obsługiwanej przy okienku. W drugim okienku również nie zapewniono odstępu pomiędzy osobą obsługiwaną a pacjentami w kolejce tak aby pacjenci w kolejce nie mogli słyszeć treść rozmowy pacjenta z personelem rejestrującym, natomiast zastosowano przepierzenia oddzielające obsługiwanego pacjenta od pozostałych w kolejce tak, że uniemożliwiono innym osobom bezpośredni wgląd w dokumenty osoby obsługiwanej. Problem ten zostanie opisany w dalszej części wystąpienia w sekcji *Stwierdzone nieprawidłowości.*

Na tablicy ogłoszeń wywieszono klauzulę informacyjną o przetwarzaniu danych osobowych.

- Ambulatoryjna Opieka Specjalistyczna[44] – rejestracja odbywała się w się w dwóch (z trzech dostępnych) okienkach. Zapewniono odstęp pomiędzy osobą obsługiwaną a pacjentami w kolejce do rejestracji poprzez umieszczenie linii na podłodze w odległości ok. 1 m od okienka, za którą pacjenci powinni oczekiwać. Pacjenci obsługiwani przy okienkach oddzieleni byli po bokach nieprzezroczystymi przepierzeniami, które uniemożliwiały uzyskanie wglądu w dokumenty osoby obsługiwanej przy okienku.

Klauzula informacyjna o przetwarzaniu danych osobowych wywieszona była na szybie przy obu okienkach.

We wszystkich poddanych oględzinom rejestracjach dokumentacja medyczna przechowywana była w zamykanym na klucz pomieszczeniu przy czym w rejestracji AOS w indywidulanych kopertach umieszczonych w obrotowych, wielopoziomowych bębnach kartotecznych, posortowana wg unikalnych numerów pacjentów nadawanych pacjentowi podczas jego pierwszej rejestracji w systemie ESKULAP.

W pozostałych dwóch rejestracjach dokumentacja medyczna posortowana była wg roku urodzenia oraz alfabetycznie wg nazwisk. Podczas obsługi pacjenta identyfikowano go na podstawie dowodu osobistego oraz numeru PESEL.

Rejestracji pacjentów oraz ustalenie kolejności wizyt na kolejne dni dokonywano wg kolejności zgłoszeń pacjentów do rejestracji. W pomieszczeniach rejestracji nie stwierdzono w zasięgu wzroku osoby rejestrowanej żadnej dokumentacji medycznej ani innych źródeł danych osobowych pacjentów. Ekrany komputerów zwrócone były

[42] Poradnie - Leczenia Padaczek, Położniczo-Ginekologiczna z Pracownią Kolposkopii, Patologii ciąży, Chirurgii Naczyniowej, Hepatologiczna, Chorób Zakaźnych dla Dzieci i Dorosłych, Otolaryngologiczna, Dermatologiczno – Wenerologiczna, Medycyny Pracy, Medycyny Sportowej.

[43] Rejestracja „Ambulatoryjna Opieka Specjalistyczna", Przychodna Kompleksowej Rehabilitacji oraz Przychodnia Onkologiczna.

[44] Dalej: AOS.

tyłem do osób rejestrowanych, uniemożliwiając im odczytanie wyświetlanych na ekranie informacji.

Oględziny trzech wybranych poradni[45] wykazały, że przy wywoływaniu pacjentów nie posługiwano się danymi osobowymi (wywołano wg kolejnego numeru lub pacjenci wchodzili wg kolejności przybycia do poczekalni). Dokumentację pacjentów przechowywano w sposób uniemożliwiający odczytanie danych osobowych przez nieuprawnione osoby. W trakcie oględzin gabinety lekarskie były pod nadzorem personelu medycznego. Nie stwierdzono opuszczenia gabinetu lekarskiego przez personel w trakcie trwania wizyt pacjentów.

(dowód: akta kontroli str. 270-278)

Na poddanych oględzinom oddziałach, poradniach i rejestracji stwierdzono przypadek niewłaściwego zabezpieczenia danych medycznych oraz osobowych pacjentów. Na Oddziale Laryngologii w przegródkach szafy w gabinecie lekarskim przechowywano dokumentację medyczną pacjentów bez możliwości jej zamknięcia. Będzie o tym mowa w dalszej części wystąpienia w sekcji *Stwierdzone nieprawidłowości.*

(dowód: akta kontroli str. 279-285)

W Szpitalu funkcjonował monitoring wizyjny prowadzony w celu poprawy bezpieczeństwa i wspomagania ochrony pacjentów, pracowników, osób przebywających na terenie Szpitala oraz w celu ochrony budynków, pomieszczeń, placów i ciągów komunikacyjnych, zapobiegania incydentom zagrażającym bezpieczeństwu. Na poddanych oględzinom oddziałach nie prowadzono monitoringu wizyjnego. Nagrania z kamer przechowywane były przez okres nieprzekraczający 30 dni od dnia ich zarejestrowania. Dostęp do urządzeń monitoringu oraz do nagrań miały jedynie upoważnione osoby. Zarządzeniem nr 99/2018 z 9.07.2018 r. nałożono na Kierownika Działu Administracyjno – Gospodarczego oraz Kierownika Działu Technicznego obowiązek zapoznania personelu Szpitala, osób przebywających w Szpitalu z treścią zarządzenia. Informacja o monitoringu wizyjnym została przekazana w wersji papierowej do komórek organizacyjnych Szpitala.

(akta kontroli str.303-316)

W sprawie regulaminu monitoringu Kierownik Działu Administracyjno – Gospodarczego wyjaśniła, że został opracowany projekt takiego regulaminu lecz jeszcze nie został formalnie przyjęty.

(akta kontroli str. 317)

2.2. Zarządzanie siecią Szpitala odbywało się za pomocą usługi Active Directory. Dostęp do domeny szpital.pl był możliwy jedynie po odpowiednim przeprowadzeniu autoryzacji użytkownika, tj. wprowadzeniu przez niego loginu i hasła. Obowiązujące zasady (Security settings – Account Policy) nakładały wymogi określające złożoność haseł oraz zasady ich zmiany.

Personel działów administracyjnych (niemedycznych) Szpitala liczył 520 osób, z tego 11 osób zatrudnionych w Dziale Rozliczeń i Statystyki Medycznej oraz trzy osoby w Dziale Informatyki.

Osoby te posiadały dostęp do systemu HIS na podstawie art. 24 ust. 2 pkt 2 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjentów, zgodnie z którym osoby wykonujące czynności pomocnicze przy udzielaniu świadczeń zdrowotnych, a także czynności związane z utrzymaniem systemu

[45] Poradnia Rehabilitacji Narządu Ruchu Dorosłych, Poradnia Onkologii Ogólnej, Poradnia Reumatologiczna.

teleinformatycznego są uprawnione do dostępu do danych medycznych, na podstawie upoważnień administratora danych.

Na próbie 30 osób spośród 520 zatrudnionych w działach niemedycznych, stwierdzono, że dziewięć z nich posiadało aktywny profil w domenie szpital.pl, z których pięć posiadało aktywny profil w domenie HIS. Schemat uprawnień nie zawierał informacji o zakresie dostępu do danych osobowych. Osoby te miały ograniczone prawa dostępu do HIS, w tym trzy osoby do danych oddziału (sekretarki medyczne), jedna osoba do modułu Apteka (pomoc apteczna) i jedna osoba do magazynu sprzętu jednorazowego oraz do transportu sanitarnego (Kierownik Działu Zaopatrzenia i Transportu). Pozostałe 25 osób nie posiadało aktywnego profilu w systemie HIS, w tym konwojenci, salowe, sanitariusze, referenci i inspektorzy w Dziale Administracyjno – Gospodarczym.

(akta kontroli str. 360-382)

2.3. Na próbie 30 spośród 527 pielęgniarek i położnych zatrudnionych w Szpitalu stwierdzono, że wszystkie posiadały aktywne konto w systemie HIS w obszarze w którym były zatrudnione. Dostęp do danych medycznych pacjentów został im przypisany tylko do oddziału, którego byli pracownikami.

(dowód: akta kontroli str. 328-359)

2.4. W okresie od 25 maja 2018 r. do 28 lutego 2019 r. rozwiązano stosunek pracy z 58 pracownikami. Oględziny usługi Active Directory przeprowadzone w dniu 12 marca 2019 r. wykazały, że wszystkim osobom odebrano dostęp do domeny szpital.pl oraz do systemu informatycznego HIS. Usługa Active Directory nie przechowuje daty odebrania dostępu do domeny. W sprawie stosowanego sposobu i terminu blokowania kont użytkowników, z którymi rozwiązano umowę o pracę, Informatyk wyjaśnił, że informację o dacie zwolnienia pracownika uzyskujemy z obiegówki, z którą zwalniany pracownik zgłasza się do Działu Informatyki. Konto użytkownika blokowane jest w dniu, w którym ten pracownik zgłasza się z obiegówką. Stwierdzono jednak logowanie do domeny szpitala pracownika, z którym rozwiązano stosunek pracy, co szerzej opisano w dalszej części wystąpienia w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli str. 383-389)

2.5. Szpital posiadał zintegrowany system informatyczny służący pełnej obsłudze zdarzeń medycznych i administracyjnych ESKULAP (HIS). Wdrożony został przez Konsorcjum firm z siedzibą w Poznaniu. Przedmiotem umowy było m.in. świadczenie usług nadzoru autorskiego oraz świadczenie usługi gwarancyjnej i serwisowej. W ramach świadczenia usługi serwisowej uruchomiono platformę wsparcia technicznego HELP DESK (HD) pod adresem: https://helpdesk.konsultant-it.pl/.

W okresie od 25 maja 2018 r. do dnia 14 marca 2019 r. pracownicy Szpitala oraz pracownicy wdrażający oprogramowanie dokonali łącznie 351 zgłoszeń zarejestrowanych w rejestrze HD.

Oględziny zapisów próby 50 zgłoszeń oraz treści przekazanych wraz z nimi załączników wykazały, że personel Szpitala, opisując usterkę podawał w tym opisie tylko dane ogólne bez podawania imienia lub nazwiska pacjenta. Poza jednym przypadkiem, nie posiłkował się w tym celu numerami PESEL pacjentów. Zrzuty ekranu z danymi medycznymi zawierającymi np. historię leczenia, a stanowiące załączniki do zgłoszenia, przed wysłaniem były zanonimizowane.

(akta kontroli str. 390-446)

2.6. W okresie objętym kontrolą obowiązywało 38 umów powierzenia przez Szpital przetwarzania danych osobowych oraz 147 umów powierzenia Szpitalowi

przetwarzania danych osobowych. Analiza pięciu losowo wybranych umów powierzenia przez Szpital przetwarzania danych osobowych wykazała, że zawierały one wszystkie elementy, o których mowa w art. 28 RODO. Przetwarzanie danych osobowych przez podmiot przetwarzający odbywało się na podstawie umowy, która każdorazowo określała przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora. W treści badanych umów zapisano, że podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora. Przy wykonywaniu czterech badanych umów nie przewidywano korzystania z usług innego podmiotu przetwarzającego. W przypadku jednej umowy, Przetwarzający mógł powierzyć dane osobowe objęte umową do dalszego przetwarzania jedynie w celu wykonania umowy ale po uzyskaniu uprzedniej pisemnej zgody Administratora (Szpitala).
W badanych umowach zawarto:
- zapewnienie przez Przyjmującego zamówienie o dostępie do danych osobowych wyłącznie przez osoby upoważnione do przetwarzania danych osobowych, które zobowiązały się do zachowania tajemnicy;
- zobowiązanie Przyjmującego zamówienie do podjęcia wszelkich niezbędnych środków wymaganych na mocy art. 32 RODO, do współpracy z Udzielającym zamówienia w zakresie udzielania odpowiedzi na żądania osoby, której dane dotyczą;
- zobowiązanie wspierania Udzielającego zamówienie w wywiązywaniu się z obowiązków określonych w art. 32-36 RODO;
- zobowiązanie do udostępnienia administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków spoczywających na Udzielającym zamówienie oraz do umożliwienia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i zobowiązuje się do współpracy przy działaniach sprawdzających i naprawczych;
- zapis o braku uprawnień Przyjmującego zamówienie do przechowywania danych osobowych przez czas dłuższy, niż wynikający z realizacji Umowy Głównej.
W przypadku wystąpienia zagrożeń mogących mieć wpływ na odpowiedzialność Udzielającego zamówienie za przetwarzanie powierzonych danych osobowych, Przyjmujący zamówienie każdorazowo był zobowiązany do niezwłocznego podejmowania działań w celu ich usunięcia. W umowach szczegółowo określono procedurę zgłaszania incydentów naruszenia ochrony danych osobowych.

(akta kontroli str. 448-504)

2.7. W okresie objętym kontrolą wystąpiło 9 przypadków naruszenia zasad ochrony danych osobowych, z których 5 dotyczyło danych osobowych pacjenta: (1) błąd w przekazaniu wyników badań na płycie CD, (2) pomyłkowe wysłanie danych osobowych pacjentów, (3) pozostawienie wyniku badania w urządzeniu do drukowania, (4) niezabezpieczenie danych przekazanych do przeniesienia sanitariuszowi, (5) pozostawienie w sekretariacie Szpitala niezabezpieczonej karty rozpoznania zakażenia.
Zgodnie z art. 33 ust. 5 RODO we wszystkich przypadkach IOD sporządził dokumentację zgłoszonych naruszeń, w tym okoliczności naruszenia ochrony danych osobowych. W wyniku analizy skutków odstąpiono od zgłoszenia naruszenia do organu nadzorczego. Podjęte działania naprawcze polegały na: zaleceniu weryfikacji danych osobowych przed ostatecznym przekazaniem wyników badań, wdrożeniu procedury usunięcia wysłanej wiadomości oraz przeprowadzeniu szkolenia pracowników, usunięciu i zniszczeniu wydruków, odpowiedniej modyfikacji oprogramowania do drukowania wyników, przeszkoleniu personelu w zakresie zabezpieczenia dokumentacji, przeszkoleniu pracowników w zakresie zabezpieczenia danych oraz obowiązków związanych z ochroną danych.

Instrukcja postępowania w sytuacji naruszenia bezpieczeństwa została wprowadzona w Szpitalu zarządzeniem nr 44.2019 Dyrektora Szpitala z dniem 21.02.2019 r. Ewidencja zdarzeń związanych z naruszeniem bezpieczeństwa danych osobowych nie zawierała przypadków stwierdzonych w toku oględzin NIK.

(Akta kontroli str. 191-212)

W okresie objętym kontrolą wpłynęło do Szpitala 51 skarg. Żadna z nich nie dotyczyła przypadku ujawnienia danych osobowych.

(akta kontroli str. 506-518)

2.8. Zasady udostępniania dokumentacji medycznej pacjentów uregulowane zostały zarządzeniem nr 1.2019 Dyrektora Szpitala z 3.01.2019 r. w sprawie zasad udostępniania indywidualnej dokumentacji medycznej i wyników badań pacjentów, którym udzielono świadczenia zdrowotne w komórkach organizacyjnych Szpitala oraz zasad odpłatności i miejsc wydawania, zmienianego zarządzeniami nr 11.2019 i 58.2019. W zarządzeniu określono zgodnie z treścią art. 26 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta m.in. komu i na jakich warunkach Szpital udostępnia dokumentację medyczną. Indywidualną dokumentację medyczną udostępnia się na pisemny wniosek zainteresowanego. Do wydawania dokumentacji medycznej w oryginale upoważniony był wyłącznie Dyrektor Szpitala, Zastępcy Dyrektora oraz Kierownik Działu Rozliczeń i Statystyki Medycznej. W zarządzeniu określono siedem miejsc udostępniania dokumentacji[46], w tym Dział Rozliczeń i Statystyki Medycznej. W Dziale Rozliczeń i Statystyki Medycznej prowadzony był wykaz udostępnianej dokumentacji medycznej wg wzoru określonego w załączniku nr 3 do ww. zarządzenia. Za okres od 25 maja 2018 r. do 14 marca 2019 r. Rejestr zawierał łącznie 1077 wpisów dotyczących zapytań, w tym 358 od pacjentów. Na 719 pozostałych wniosków, 155 złożyły osoby inne niż sam pacjent, 73 wnioski wpłynęły od instytucji rynku ubezpieczeniowego. Pozostałe zapytania wpływały od sądów (70 wniosków), policji i prokuratur (249 wniosków), ZUS (85) oraz od biur odszkodowań i kancelarii prawnych.

Analiza prawidłowości udostępniania dokumentacji medycznej przeprowadzona na próbie 30 zgłoszeń złożonych przez firmy ubezpieczeniowe oraz 30 zgłoszeń od osób innych niż pacjent którego ta dokumentacja dotyczyła wykazała, że Szpital właściwie udostępniał dokumentacje medyczną:

- w przypadku instytucji rynku ubezpieczeniowego w 26 sprawach złożone wnioski zawierały jako załącznik kopię polisy ubezpieczeniowej, którą podpisał pacjent i jednym z elementów tej polisy była zgoda pacjenta na to, aby firma ubezpieczeniowa wystąpiła w jego imieniu o historię leczenia lub informację o stanie zdrowia i w 25 przypadkach ją uzyskała, w jednej sprawie zakres żądania instytucji ubezpieczeniowej przekraczał zakres uzyskanej zgody i odmówiono udzielenia kopii dokumentacji medycznej. W czterech sprawach kopię upoważnienia pacjenta, który zgadzał się na to, aby firma ubezpieczeniowa wystąpiła w jego imieniu o historię leczenia i w trzech przypadkach ją uzyskała, w jednej sprawie do wniosku załączono upoważnienie do udzielenia pełnej informacji dotyczącej zdrowia innej osoby niż wymieniona we wniosku, nie załączono informacji, że zgoda została wyrażona przez rodzica lub opiekuna osoby wymienionej we wniosku i odmówiono udostepnienia informacji medycznej w tej sprawie. Jednocześnie instytucje rynku finansowego

[46] 1) Dział Rozliczeń i Statystyki Medycznej; 2) rejestracja Przyszpitalnych Poradni Specjalistycznych - w zakresie dokumentacji pacjentów, którym udzielono świadczeń ambulatoryjnych w tej lokalizacji; 3) rejestracja Przychodni Onkologicznej - w zakresie dokumentacji pacjentów, którym udzielono świadczeń ambulatoryjnych w tej lokalizacji; 4) rejestracja Przychodni Kompleksowej Rehabilitacji z Oddziałem Dziennym i Poradniami - w zakresie pacjentów, którym udzielono świadczeń ambulatoryjnych w ramach komórek organizacyjnych tej Przychodni; 5) rejestracja Zakładu Diagnostyki Obrazowej - w zakresie dokumentacji pacjentów, którym udzielono świadczeń w tej komórce; 6) rejestracja Zakładu Patomorfologii - w zakresie dokumentacji pacjentów, którym udzielono świadczeń w tej komórce; 7) rejestracja Zakładu Mikrobiologii - w zakresie dokumentacji pacjentów, którym udzielono świadczeń w tej komórce.

w swoich wnioskach podawały podstawę prawną do przekazania im powyższych informacji[47].

- w przypadku wnioskodawców innych niż pacjent, w jednym wniosku o udostępnienie kopii dokumentacji medycznej pacjent wskazywał osobę upoważnioną do uzyskania tych danych, w dwóch przypadkach do wniosku załączono upoważnienie do uzyskania kopii dokumentacji medycznej, w 16 przypadkach powoływano się na upoważnienie znajdujące się wprost na karcie historii choroby, w jednym przypadku wyrok sądu ustanawiający opiekuna prawnego. W 10 z 30 przypadków wnioskodawcą był rodzic, który występował o kopię dokumentacji medycznej dziecka niepełnoletniego na podstawie aktu urodzenia.

(akta kontroli str. 519-547)

2.9. Szpital posiadał dwie serwerownie, z których jedna zlokalizowana była na parterze budynku „A" oraz druga na pierwszym piętrze budynku SOR. Serwerownia w budynku „A" zabezpieczona była aktywnym alarmem z czujnikami ruchu. Drzwi do serwerowni płycinowe, obite były z zewnątrz blachą i wyposażone w dwa zamki na klucze patentowe. Drzwi nie posiadały konstrukcji, w tym atestu o zapewnieniu odporności na włamania oraz ognioodporność. Pomieszczenie serwerowni posiadało okna z opuszczonymi żaluzjami, od zewnątrz zabezpieczone stalowymi kratami umocowanymi w otworach okiennych, w pomieszczeniu znajdowały się czujki ruchu połączone z systemem alarmowym. Centrala systemu alarmowego znajduje się na portierni budynku „A", w której przebywają całą dobę pracownicy ochrony fizycznej szpitala. W serwerowni zamontowano czujki dymu sprzężone z system alarmu pożarowego Szpitala, a na ścianie zamontowano gaśnicę do gaszenia sprzętu elektronicznego. Serwerownię wyposażono w podwójny system klimatyzacji. Serwery, biblioteki taśmowe i inne urządzenia sieciowe zainstalowane były w specjalnie do tego przeznaczonych dwóch szafach. Na wypadek zaniku zasilania zainstalowane zostały układy podtrzymania napięcia (UPS).

Serwerownia w budynku SOR wyposażona była w antywłamaniowe, ognioodporne drzwi wejściowe. W ramach kontroli dostępu funkcjonowała kamera monitoringu wizyjnego na korytarzu SOR. W pomieszczeniu serwerowni znajdowała się na suficie czujka dymu podłączona do systemu alarmu przeciwpożarowego Szpitala. Pomieszczenie posiadało urządzenie klimatyzacyjne. Urządzenia sieciowe oraz Tape Library[48] były zainstalowane w specjalnie do tego przeznaczonej szafie.

Informatyk wyjaśnił, że kopie bezpieczeństwa baz danych działających w Szpitalu wykonuje się na urządzeniach Tape Library: codziennie od poniedziałku do piątku (od 23:00) przyrostowo oraz raz w tygodniu wykonywana jest kopia pełnego zakresu danych obejmujących wszystkie bazy (kopie wykonywane są w nocy, tj. od 23:00). Czas przechowywania pełnej kopii wynosi 4 tygodnie. Druga zapasowa kopia wykonywana jest na innym urządzeniu taśmowym, znajdującym się w drugiej serwerowni w budynku SOR. Nośniki danych zwierające kopie (taśmy) przechowywane są wewnątrz urządzeń wykonujących kopie w obu serwerowniach. Urządzenia automatycznie dokonują weryfikacji poprawności dokonywanych zapisów na taśmach.

W Szpitalu wykorzystuje się trzy komputery przenośne. Na komputerach tych nie stosuje się ochrony kryptograficznej nośników pamięci (dysków twardych). Na

[47] Art. 26 ust. 3 pkt 7 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. 2017 r. poz. 1318), art. 38 i 40 ustawy z dnia z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz. U. z 2018 r. poz. 999), rozporządzenie Ministra Zdrowia z dnia 13 października 2016 r. w sprawie informacji udzielanych zakładom ubezpieczeń przez podmioty wykonujące działalność leczniczą oraz Narodowy Fundusz Zdrowia (Dz. U. z 2016 r. poz. 1754).

[48] Biblioteka taśmowa.

komputerach tych nie przetwarza się danych osobowych ani nie przechowuje danych medycznych o pacjentach.

Nie wykorzystywano pseudonimizacji danych osobowych polegającej na przetworzeniu danych osobowych w taki sposób, by nie można było ich przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji.

(akta kontroli str. 548-558)

Oględziny próby 30 komputerów, po 10 użytkowanych przez lekarzy, pielęgniarki i położne oraz pracowników administracji wykazały, że na każdym z nich dostęp użytkownika do systemu operacyjnego wymagał podania loginu i hasła. Hasła użytkowników posiadały odpowiednią złożoność określoną w IZSI. Zasady tworzenia loginu użytkownika nie zostały określone w przyjętej dokumentacji IZSI ani PB. Tworzony był w oparciu o przyjęte zwyczajowo zasady.
W trakcie oględzin nie stwierdzono przypadku podczas uzyskiwania dostępu do komputera wprowadzania przez użytkownika innych nie swoich danych autoryzacyjnych, przydzielonych innej osobie. Na żadnym z poddanych oględzinom komputerze nie stwierdzono plików zawierających informacje medyczne o pacjentach.

Na 26 komputerach (86,7 % z 30 objętych badaniem) zainstalowano programy antywirusowe, przy czym na 25 z nich oprogramowanie antywirusowe było aktualne (aktualna baza sygnatur wirusów z datą z dnia oględzin), na pozostałych czterech komputerach funkcjonował systemowy Windows Defender;
Na 16 komputerach (53,3% z 30 objętych badaniem) zainstalowano system windows 7, a na 11 (36,7%) windows 10. Na pozostałych trzech komputerach (10%) funkcjonował system Windows XP, dla którego producent oprogramowania zakończył wsparcie techniczne 8 kwietnia 2014 r. Najwyższa Izba Kontroli zwraca uwagę, że po tym terminie producent przestał dostarczać aktualizacje zabezpieczeń, poprawki niezwiązane z zabezpieczeniami, bezpłatne lub płatne opcje asystowanej pomocy technicznej i aktualizacje zawartości technicznej online, co znacznie wpływa na bezpieczeństwo tego systemu operacyjnego.

W sześciu przypadkach (20% z 30 objętych badaniem) komputery nie miały zabezpieczonych portów USB przed możliwością podłączenia do nich zewnętrznych nośników pamięci[49].
Kierownik Działu Informatyki wyjaśnił, że część komputerów musi mieć dostęp do odblokowanego portu USB m.in. z powodu używania podpisu Szafir, czy klucza HASP[50].

(akta kontroli str. 585-588)

W pięciu przypadkach użytkownicy komputerów posiadali uprawnienia administratora w systemie operacyjnym do instalacji dowolnego oprogramowania, co szerzej opisano w dalszej części wystąpienia w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 559-584)

Stwierdzone nieprawidłowości

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

1. W gabinecie lekarskim Oddziału Laryngologii dokumentacja medyczna pacjentów przechowywana była w otwartych przegródkach szafy meblowej, która nie posiadała możliwości zamknięcia. Zgodnie z § 47 PB użytkownicy

[49] W toku oględzin informatyk podejmował próbę otwarcia pliku tekstowego na pendrive wkładanym do portu USB sprawdzanych komputerów w celu stwierdzenia, czy porty USB komputera zostały zabezpieczone przed możliwością podłączenia do nich nośników pamięci.

[50] Rodzaj klucza sprzętowego służącego do zabezpieczenia przed naruszeniem praw autorskich oprogramowania.

zobowiązani są m.in. do zabezpieczenia dokumentów zawierających dane osobowe przed dostępem osób nieupoważnionych za pomocą środków określonych w PB, Instrukcji i innych procedurach. Zgodnie z załącznikiem nr 3 do PB zbiory danych osobowych w formie papierowej należało przechowywać w zamkniętych szafach. Zgodnie z art. 24 ust. 1 RODO administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z tym rozporządzeniem. W świetle zaś art. 5 ust. 1 lit. f RODO dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych ("integralność i poufność").

(akta kontroli str. 92, 290-295)

W sprawie przechowywania dokumentacji medycznej pacjentów Koordynator Oddziału Laryngologii z Pododdziałem Chirurgii Stomatologicznej z Blokiem Operacyjnym oraz Pracowniami: Audiologii i VNG wyjaśnił, że dokumentacja medyczna pacjentów znajduje się w pomieszczeniu zamykanym na zamek z kodem dostępu. Zlecono działowi technicznemu wykonanie montażu drzwiczek zamykanych na klucz (dostęp tylko dla personelu lekarskiego). Do tego czasu dokumentacja pacjentów została przeniesiona do szafki zamykanej na klucz znajdującej się powyżej przegródek, w których były dotychczas przechowywane.

(akta kontroli str. 300-302)

2. Rozwiązania techniczne i organizacyjne w Przychodni Onkologicznej podczas rejestracji stwarzają ryzyko ujawnienia danych medycznych oraz osobowych pacjentów. Oględziny rejestracji przeprowadzone 4 marca 2019 r. wykazały, że pacjenci obsługiwani w rejestracji znajdowali się w bezpośrednim sąsiedztwie innych pacjentów stojących w kolejce. Brak zachowania odpowiedniego dystansu w stosunku do pacjentów w kolejce stwarzał zagrożenie dla zachowania poufności informacji przekazywanych słownie przy okienku rejestracji. Ponadto przy okienku nr 1 stwierdzono brak zasłony (przepierzenia) fizycznie uniemożliwiającej uzyskanie wglądu przez kolejną osobę w kolejce w dokumenty osoby obsługiwanej przy okienku. Stosownie do treści art. 13 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, pacjent ma prawo do zachowania w tajemnicy przez osoby udzielające mu świadczeń zdrowotnych, informacji z nim związanych, a zgodnie z art. 20 ust. 1 ustawy pacjent ma prawo do poszanowania intymności i godności, w szczególności w czasie udzielania mu świadczeń zdrowotnych. Zgodnie z art. 24 ust. 1 RODO administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z tym rozporządzeniem. W zaś świetle art. 5 ust. 1 lit. f RODO dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych ("integralność i poufność").

Kierownik Przychodni Onkologicznej wyjaśniła, że zwrócono się o opinię do Inspektora ds. Ochrony Przeciwpożarowej. Po zakończeniu aktualnie prowadzonego remontu przychodni wdrożone będą jego zalecenia dotyczące m.in. zwiększenia odstępu od okienka dla kolejnego interesanta o odległość około 60 cm od obecnej.

Linie wyznaczające miejsce ustawienia kolejnego oczekującego do rejestracji wyznaczone zostaną taśmą ostrzegawczą przyklejoną do podłogi.

(akta kontroli str. 296-299)

3. Oględziny oddziałów szpitalnych wykazały, że pacjenci badanych oddziałów posiadali na nadgarstkach opaski zawierające pełne dane dotyczące imienia, nazwiska i numer PESEL. Zgodnie z art. 36 ust. 3 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej[51] pacjentów szpitala zaopatruje się w znaki identyfikacyjne, które umieszcza się m.in. na opasce[52]. Zgodnie z art. 36 ust. 5 tej ustawy – znak identyfikacyjny powinien zawierać informacje pozwalające na ustalenie imienia i nazwiska oraz daty urodzenia pacjenta ale zapisane w sposób uniemożliwiający identyfikację pacjenta przez osoby nieuprawnione. Pomimo tego, że pacjenci posiadali na nadgarstkach opaski zawierające pełne dane wypisane na wewnętrznej stronie opaski to osoby nieuprawnione mogły odczytać te dane po ich odwróceniu, a tym samym zidentyfikować osoby.

(akta kontroli str. 279-295)

4. W przypadku jednego z 58 pracowników, z którymi po 25 maja 2018 r. rozwiązano stosunek pracy – nie zablokowano mu dostępu do domeny szpital.pl, co było niezgodne z § 20 ust. 2 pkt 5 rozporządzenia KRI. W trakcie kontroli NIK stwierdzono, że data ostatniego logowania do ww. domeny przez użytkownika była późniejsza niż data rozwiązania stosunku pracy. Pracownik został zwolniony z dniem 30 września 2018 r. natomiast data ostatniego logowania to 4 października 2018 r., tj. 4 dni po rozwiązaniu umowy o pracę. Świadczyło to o aktywności tego konta w dniu logowania. Dostęp do systemu HIS został zablokowany z dniem zwolnienia, tj. 30 września 2018 r.

W sprawie przyczyn, dla których konto przedmiotowego użytkownika było aktywne po dacie rozwiązania umowy o pracę, Informatyk wyjaśnił, że nie przypomina sobie okoliczności wyjaśniających przyczynę pozostawienia aktywności konta po dacie rozwiązania umowy o pracę tego pracownika.

(akta kontroli str. 383-389)

5. W jednym przypadku nie zastosowano zasady minimalizacji danych, przekazując przy zgłoszeniu serwisowym do Help Desk systemu ESKULAP nadmiarowe dane. W opisie zgłoszenia[53] podany był numer PESEL pacjenta, a oprócz tego też numer księgi głównej[54]. Zgodnie z treścią art. 5 pkt 1 lit. c RODO dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane ("minimalizacja danych"). Podanie numeru PESEL nie było niezbędne do usunięcia usterki, gdyż Szpital mógł komunikując się z firmą serwisującą – podawać na przykład sam numer księgi głównej[55], który w innym przypadku wystarczył do usunięcia zgłaszanej usterki. Podanie numeru PESEL w tym przypadku było nadmiarowe.

(akta kontroli str. 390-399)

---

[51] Dz.U. z 2018 r., poz. 2190 ze zm.

[52] §3 rozporządzenia Ministra Zdrowia z dnia 20 września 2012 r. w sprawie warunków, sposobu i trybu zaopatrywania pacjentów szpitala w znaki identyfikacyjne oraz sposobu postępowania w razie stwierdzenia ich braku (Dz.U. z 2012 r., poz. 1098).

[53] Poz. Nr 218 rejestru zgłoszeń Help Desk pod adresem https://helpdesk.konsultant-it.pl/.

[54] W księdze głównej każdy pacjent ma przypisany mu numer ID, na podstawie którego można go jednoznacznie zidentyfikować.

[55] Jak w przypadku poz. 165 w rejestrze zgłoszeń Help Desk.

6. W poddanej oględzinom próbie 30 komputerów stwierdzono przypadki braku wystarczających działań zapewniających ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także braku odpowiedniego zabezpieczenia przetwarzanych informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie do czego zobowiązywał przepis § 20 ust. 2 pkt 7 i 9 rozporządzenia KRI w zakresie podejmowanych działań oraz § 20 ust. 2 pkt 12 tego rozporządzenia poprzez niezapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych polegające w szczególności na braku dbałości o aktualizację oprogramowania i minimalizowaniu ryzyka utraty informacji w wyniku awarii oraz ochronie przed błędami, utratą, nieuprawnioną modyfikacją. W myśl art. 5 ust. 1 lit. f RODO, dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

- Na pięciu komputerach (16,7% z 30 objętych badaniem) użytkownik posiadał uprawnienia, które umożliwiały zainstalowanie na komputerze dowolnego oprogramowania[56].
Kierownik Działu Informatyki wyjaśnił, że trzy z nich z Windowsem XP w ograniczony sposób współpracują z serwerem domenowym, a przetwarzanie zasad grupy GPO[57] nie zawsze jest skuteczne. Dwa pozostałe mają podniesione uprawienia ze względu na konieczność używania oprogramowania CryptoCard Suite.

(akta kontroli str. 585-588)

- Na jednym komputerze (3,33% z 30 objętych badaniem) zainstalowany był nieaktualny program antywirusowy[58]. Kierownik Działu Informatyki wyjaśniła, że sieć szpitalna zabezpieczona jest dwustopniowo, urządzeniami Fortigate i Fortianalyzer oraz dodatkowo oprogramowaniem antywirusowym które w czasie rzeczywistym skanują ruch w sieci, blokując niepożądany ruch wywołany przez szkodliwe oprogramowanie, jednocześnie wskazując zainfekowane jednostki.

(akta kontroli str. 585-588)

Kierownik Działu Informatyki wyjaśniła, że od kilku lat informuje Dyrekcję o konieczności wymiany sprzętu, przedstawiając wykaz komputerów z niewspieranym systemem Windows XP. Niestety z powodów finansowych proszeni są o umieszczenie w rocznym planie zakupów ograniczonej liczby komputerów, co znacznie wydłuża proces wymiany sprzętu.

(akta kontroli str. 585-588)

OCENA CZĄSTKOWA

Rozwiązania techniczne i organizacyjne nie zapewniały w pełni prawidłowego przetwarzania i ochrony danych osobowych pacjentów oraz poszanowania ich prywatności. Przy rejestracji pacjentów w Przychodni Onkologicznej nie zapewniono w pełni prawa do zachowania w tajemnicy informacji z nim związanych co stanowiło naruszenie art. 13 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta. Na jednym z oddziałów dokumentację przechowywano w niezamykanych szafkach,

[56] Przy współudziale informatyka sprawdzano czy dany pracownik z badanej próby ma możliwość instalacji dowolnego oprogramowania – na zalogowanym koncie użytkownika informatyk podejmował próbę instalacji oprogramowania. (firmy ADOBE READER 9.5 - powszechnie znane oprogramowanie darmowe, które nie zakłóci pracy komputerów).

[57] Zbiór reguł i ustawień określających zakres działania komputera oraz użytkowników danego komputera.

[58] G Data Security Client z datą ostatniej aktualizacji 24.03.2017 r.

a pacjentów zaopatrywano w opaski zawierające ich pełne dane czym naruszono art. 36 ust. 5 ustawy o działalności leczniczej. Prawidłowo reagowano na ujawnione przypadki naruszenia ochrony danych osobowych i podejmowano odpowiednie środki zaradcze. Personel medyczny Szpitala adekwatnie do swoich uprawnień przetwarzał dane medyczne pacjentów zgodnie z art. 24 u.o.p.p. Zapewniono mu odpowiedni dostęp do danych medycznych, jednak wystąpiły przypadki nadania nadmiernych uprawnień na wybranych komputerach, brak ochrony antywirusowej na jednym urządzeniu i logowanie do sieci szpitala jednego byłego pracownika, co stanowiło naruszenie art. 5 ust. 1 lit. f RODO oraz § 20 ust. 2 pkt 5, 7 i 12 rozporządzenia KRI. Dostawcy oprogramowania wysłano w zgłoszeniu serwisowym nadmiarowe dane pacjenta, co nie było konieczne do naprawy usterki.

IV. Uwagi i wnioski

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

Wnioski

1. Opracowanie Polityki Bezpieczeństwa Informacji, o której mowa w § 2 pkt 15 rozporządzenia KRI, spełniającej wymogi § 20 ust. 1 tego rozporządzenia.
2. Zapewnienie podczas rejestracji w Przychodni Onkologicznej prawo pacjenta do zachowania w tajemnicy informacji z nim związanych.
3. Zapewnienie aktualnej ochrony antywirusowej na komputerach, w których dokonuje się przetwarzania danych osobowych.
4. Dostosowanie poziomu uprawnień użytkowników komputerów do wymogów IZSI.
5. Bezzwłoczne odbieranie uprawnień w systemach informatycznych pracownikom, z którymi rozwiązano stosunek pracy.
6. Zaopatrywanie pacjentów Szpitala w znaki identyfikacyjne uniemożliwiające ich identyfikację przez osoby nieuprawnione.
7. Przestrzeganie zasady minimalizacji przekazywanych danych przy zgłoszeniach serwisowych w ramach HelpDesk.
8. Zaprowadzenie elektronicznego rejestru czynności przetwarzania.

Najwyższa Izba Kontroli nie formułuje uwag.

V. Pozostałe informacje i pouczenia

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden dla kierownika jednostki kontrolowanej, drugi do akt kontroli.

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 ustawy o NIK kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do dyrektora Delegatury NIK w Szczecinie. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Obowiązek poinformowania NIK o sposobie wykonania wniosków

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

Szczecin, 15 kwietnia 2019 r.

Kontroler	Najwyższa Izba Kontroli
Krzysztof Szczepaniak	Delegatura w Szczecinie
Główny specjalista kontroli państwowej	
.....	.....
podpis	*podpis*