NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.410.002.02.2019

00089519

Pani
Danuta Zawadzka
Dyrektor Samodzielnego Publicznego
Zakładu Opieki Zdrowotnej w Augustowie
ul. Szpitalna 12, 16-300 Augustów

WYSTĄPIENIE POKONTROLNE

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

NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku
ul. Akademicka 4, 15-267 Białystok
T +48 85 874 81 00, F +48 85 874 81 33
lbi@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Samodzielny Publiczny Zakład Opieki Zdrowotnej w Augustowie, ul. Szpitalna 12, 16-300 Augustów (dalej: *Szpital* lub *ZOZ*)
Kierownik jednostki kontrolowanej	Danuta Zawadzka, dyrektor od 12 stycznia 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, tj. do 27 marca 2019 r. Badania kontrolne mogły dotyczyć działań sprzed tego okresu, jeśli miały związek z zagadnieniami będącymi przedmiotem kontroli.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[1]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Białymstoku
Kontrolerzy	1. Wojciech Zambrzycki, starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LBI/12/2019 z 14 stycznia 2019 r. i LBI/33/2019 z 1 marca 2019 r. 2. Beata Palinowska, starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LBI/34/2019 z 4 marca 2019 r. (akta kontroli str. 1-6)

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

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

Najwyższa Izba Kontroli ocenia negatywnie podjęte przez Szpital działania w celu zapewnienia prawidłowej ochrony i przetwarzania danych osobowych.

Uzasadnienie oceny ogólnej

Stwierdzono bowiem nieprawidłowości, polegające m.in. na:

- przekazaniu – z naruszeniem art. 5 ust. 1 lit. c RODO[3] – podmiotowi świadczącemu usługi serwisowe danych osobowych ośmiu pacjentów Szpitala, w tym danych medycznych czterech z nich, co nie było konieczne do przeprowadzenia procesu obsługi zgłoszenia serwisowego,
- udostępnieniu dokumentacji medycznej pacjenta z naruszeniem art. 26 ust. 1 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta[4] oraz przyjętych procedur wewnętrznych w tym zakresie,
- niedostosowaniu regulacji wewnętrznych do przepisów RODO oraz nieprzeszkoleniu pracowników Szpitala z zakresu ochrony danych osobowych i danych medycznych – co uczyniono dopiero w trakcie kontroli NIK,
- dopuszczeniu 22 (z 30) objętych badaniem pielęgniarek i położnych do przetwarzania danych osobowych pacjentów z oddziałów lub poradni, na których nie świadczyły pracy, co naruszało art. 5 pkt 1 lit. c RODO,
- niewprowadzeniu odpowiednich środków technicznych i organizacyjnych zapewniających właściwą ochronę danych osobowych oraz minimalizację ryzyka ujawnienia informacji osobom postronnym w procesie rejestracji i leczenia pacjentów,
- niezabezpieczeniu miejsc przechowywania podręcznej dokumentacji pielęgniarskiej, zawierającej dane osobowe pacjentów w trzech objętych badaniem dyżurkach pielęgniarskich oraz dokumentacji medycznej w trzech poddanych oględzinom gabinetach lekarskich (za wyjątkiem nielicznych zamykanych szuflad), co stanowiło naruszenie art. 24 ust. 1 RODO,
- niezapewnieniu 11 (z 30 badanych) osobom personelu właściwych uprawnień w systemach operacyjnych oraz ochrony antywirusowej w czterech z 30 komputerów, a także niezastosowania w takiej samej ich liczbie środków uwierzytelniających podczas rozpoczynania pracy (loginu i hasła), co było niezgodne z § 20 ust. 2 pkt 4, pkt 7 lit. a i pkt 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[5],
- nieuzupełnianiu rejestru naruszeń ochrony danych osobowych oraz incydentów zagrażających bezpieczeństwu danych, chociaż takie stwierdzono w trakcie oględzin NIK.

---

[2] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.

[3] Rozporządzenie 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 (Dz. Urz. UE L 119 z 2016 r., str. 1, ze zm.).

[4] Dz. U. z 2017 r. poz. 1318 ze zm. Ustawa zwana dalej: *ustawą o prawach pacjenta.*

[5] Dz. U. z 2017 r. poz. 2247. Rozporządzenie zwane dalej: *rozporządzeniem KRI.*

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

OBSZAR

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

Opis stanu faktycznego

1.1. Wywiązując się z obowiązku określonego w art. 8 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[7] w związku z art. 37 RODO, zarządzeniem[8] z 23 maja 2018 r. Dyrektor Szpitala powołała na stanowisko IOD pracownika, który do tego dnia pełnił funkcję Administratora Bezpieczeństwa Informacji (dalej: *ABI*). Był on jednocześnie Kierownikiem Działu Organizacji i Kontroli oraz Zamówień Publicznych, przy czym funkcje te były rozdzielone i pełnienie ich przez jedną osobę nie powodowało konfliktu interesów. W tym samym dniu zawarte zostało porozumienie zmieniające umowę o pracę i aneks do zakresu obowiązków z określeniem zadań IOD. W myśl art. 8 i art. 10 u.o.d.o., Szpital terminowo wywiązał się z obowiązku zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych (dalej: *PUODO*) o wyznaczeniu IOD (7 czerwca 2018 r. formularzem elektronicznym), przy czym Szpital nie dysponował kopią zgłoszenia, zatem nie było możliwe ustalenie, czy zgłoszenie do PUODO było kompletne. Zgodnie z wymogiem określonym w art. 37 ust. 7 RODO, na stronie internetowej Szpitala[9] zamieszczono informację m.in. o: danych Administratora Danych Osobowych (dalej: *ADO*), danych kontaktowych do IOD, celu przetwarzane danych osobowych oraz o zasadach przekazywania takich danych (komu i kiedy), jak też o prawie pacjenta do dostępu do tych danych. (akta kontroli str. 10-23)

IOD był członkiem Komitetu ds. Bezpieczeństwa, powołanego na mocy zarządzenia[10] z 10 kwietnia 2015 r. W skład tego komitetu wchodził IOD (ówcześnie jako ABI), Administrator Bezpieczeństwa Teleinformatycznego, Administrator Bezpieczeństwa Fizycznego i Audytor Wewnętrzny. Zadaniami tego komitetu było m.in. doprowadzenie do właściwego funkcjonowania struktur bezpieczeństwa informatycznego i fizycznego oraz audyt tych struktur. (akta kontroli str. 20)

W regulaminie organizacyjnym[11] Szpitala wymieniony został IOD, jako jedno ze stanowisk pracy. W zarządzeniu o jego powołaniu oraz w zakresie obowiązków wskazano wszystkie zadania przypisane temu stanowisku, wymienione w art. 39 RODO. (akta kontroli str. 24-48)

Zgodnie z wymogami art. 37 ust. 5 RODO, IOD miał należyte przygotowanie i kwalifikacje zawodowe do pełnienia swojej funkcji. Wcześniej był ABI w kontrolowanym Szpitalu, uczestniczył w szkoleniach dotyczących zagadnień związanych z ochroną danych osobowych oraz ze stosowania RODO w ochronie zdrowia. (akta kontroli str. 336-338)

Do zakończenia kontroli NIK Szpital nie otrzymał decyzji administracyjnej w sprawie uznania go za świadczącego usługę kluczową[12] na podstawie ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[13]. (akta kontroli str. 577)

1.2. Przed wejściem w życie RODO w Szpitalu funkcjonowała Polityka Bezpieczeństwa Informacji i Instrukcja Zarządzania Systemem Informatycznym (dalej: *PBI*), wprowadzona 10 grudnia 2015 r.[14], zastąpiona PBI, sporządzoną przez IOD 14 czerwca 2018 r. W PBI, mimo jej aktualizacji, nie zawarto regulacji wynikających z wejścia w życie RODO, a dokumentację spełniającą wymogi tego rozporządzenia opracowano dopiero w trakcie

---

[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] Dz. U. poz. 1000, ze zm. Ustawa zwana dalej: *u.o.d.o.*

[8] Zarządzenie Nr 13/2018 Dyrektora Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Augustowie z dnia 23 maja 2018 r. w sprawie powołania Inspektora Ochrony Danych.

[9] http://www.spzoz.augustow.pl/rodo

[10] Zarządzenie Nr 14/2015 Dyrektor Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Augustowie z dnia 10 kwietnia 2015 r. w spawie powołania Komitetu ds. Bezpieczeństwa.

[11] Regulamin Organizacyjny Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Augustowie z 4 czerwca 2012 r. ze zm. z 13 maja 2015 r., 19 marca 2018 r. i 12 czerwca 2018 r.

[12] Usługa kluczowa to taka, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienioną w wykazie usług kluczowych.

[13] Dz. U. poz. 1560.

[14] Zarządzeniem Dyrektora Szpitala nr 44/2016.

kontroli NIK, tj. 12 lutego 2019 r. (PBI i dokumentację spełniającą wymogi RODO wprowadzono 20 marca 2019 r.)[15]. Żaden z tych dokumentów nie zawierał informacji o zapoznaniu pracowników z ich treścią, co opisano też w dalszej części wystąpienia pokontrolnego, w sekcji *Stwierdzone nieprawidłowości.* (akta kontroli str. 50-126)

Opracowanymi 12 lutego 2019 r. dokumentami były w szczególności: [1] Polityka ochrony danych osobowych, [2] Instrukcja zarządzania RODO – wykaz zabezpieczeń, [3] Regulamin ochrony danych osobowych, [4] Procedura postępowania w sprawie naruszeń ochrony danych, w tym wzór rejestru naruszeń, [5] Arkusze przeprowadzonej analizy ryzyka z zabezpieczeniami, [6] Rejestr czynności przetwarzania, [7] Dokumentacja techniczna zawierająca wykaz posiadanego sprzętu i jego konfigurację, [8] Wzory klauzul informacyjnych dla pacjentów, pracowników i kandydatów do pracy. Dokumenty te spełniały wymogi RODO i zawierały zapisy o: prawie do ograniczenia przetwarzania (art. 18 RODO), powiadomieniu o sprostowaniu lub usunięciu danych osobowych, lub o ograniczeniu przetwarzania (art. 19 RODO), uwzględniania ochrony danych osobowych w fazie projektowania, domyślnej ochronie danych (art. 25 RODO), rejestrowaniu czynności przetwarzania (art. 30 RODO), bezpieczeństwie przetwarzania (art. 32 RODO), zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu (art. 33 RODO), wzór oceny skutków dla ochrony danych osobowych (art. 35 RODO).

W Szpitalu opracowano wszystkie procedury i dokumentację, których obowiązek sporządzenia wynikał z Polityki Ochrony Danych Osobowych z 12 lutego 2019 r.: [1] ewidencję osób upoważnionych, [2] wykaz zabezpieczeń RODO, [3] instrukcję zarządzania RODO oraz [4] plan ciągłości działania. (akta kontroli str. 127-333)

Postanowienia PBI oraz dokumentacji opracowanej w związku z wejściem w życie RODO obejmowały ochronę danych osobowych pracowników Szpitala i pacjentów oraz określały sposoby zapewnienia bezpieczeństwa danych osobowych przetwarzanych w formie papierowej oraz w systemach elektronicznych. (akta kontroli str. 127-134, 222-234)

1.3. W Szpitalu od 25 maja 2018 r. do 11 lutego 2019 r. nie prowadzono rejestru czynności przetwarzania danych, wymaganego art. 30 ust. 1 RODO, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji *Stwierdzone nieprawidłowości.* Rejestr był prowadzony przez IOD od 12 lutego 2019 r. (został założony w trakcie kontroli NIK), w formie papierowej i elektronicznej (excel). Liczył 16 pozycji i zawierał wszystkie elementy wymagane art. 30 ust. 1 RODO. (akta kontroli str. 124, 179-196)

1.4. IOD przeprowadził, stosownie do art. 32 ust. 2 RODO, ocenę ryzyka związanego z przetwarzaniem danych oraz określił rodzaje zabezpieczeń dla poszczególnych ryzyk. Miało to miejsce 12 lutego 2019 r., tj. 263 dni po wejściu w życie przepisów RODO (szerzej opisano ten problem w dalszej części wystąpienia pokontrolnego, w sekcji *Stwierdzone nieprawidłowości*). Określone zostało prawdopodobieństwo i skutki incydentu (w skali od jednego do trzech), ryzyko jego wystąpienia (w skali od jednego do dziewięciu) oraz plan działania z ryzykiem. Za akceptowalne uznano ryzyka o wartości od jednego do dwóch pkt, na poziomie opcjonalnym (tj. akceptujemy albo obniżamy) ryzyka o wartości od trzech do sześciu pkt, a za nieakceptowalne przyjęto ryzyka o wartości dziewięciu pkt. Zidentyfikowano 55 ryzyk, w tym:

- na poziomie nieakceptowalnym – ryzyko związane z działaniem szkodliwego oprogramowania *ransomeware*[16];
- na poziomie opcjonalnym – 14 ryzyk, m.in.: zalanie, awaria zasilania i sprzętu, łamanie haseł, awarię oprogramowania, wirusy, nieprzestrzeganie procedur;
- na poziomie akceptowalnym – 40 ryzyk, m.in.: wyłudzanie informacji, nieuprawniony dostęp lub włamanie do pomieszczeń, nieuprawniona modyfikacja lub usunięcie, kopiowanie danych, kradzież danych, nośników i danych dostępowych.

[15] Zarządzeniem Dyrektora Szpitala nr 9/2019.

[16] Typ szkodliwego oprogramowania blokującego dostęp do systemu komputerowego lub uniemożliwiającego odczyt zapisanych w nim danych, które następnie żąda okupu za przywrócenie stanu pierwotnego.

Najwyższa Izba Kontroli zwraca uwagę, że akceptowanie nieuprawnionej modyfikacji, usunięcia, kopiowania i kradzieży danych nie jest sytuacją właściwą z punktu widzenia obowiązku zapewnienia bezpieczeństwa przechowywanych danych wrażliwych.

W celu ograniczenia ryzyk określone zostały rodzaje zabezpieczeń, tj. m.in.: systemy firewall, antywirusowe i antyspamowe, backupy i archiwizacja, regulamin dla pracowników i współpracowników, szkolenia personelu, zabezpieczenie dostępu do pomieszczeń, serwerowni i archiwum, polityka kluczy, zabezpieczanie pracy użytkowników, zarządzanie uprawnieniami, uwierzytelnianie.

NIK zwraca uwagę, że zabezpieczenie przed oprogramowaniem *ransomeware* planowano wdrożyć do 31 grudnia 2019 r., a podczas przeprowadzonych 14 i 15 marca 2019 r. oględzin stwierdzono, że część zabezpieczeń nie była stosowana, co szerzej opisano w sekcji *Stwierdzone nieprawidłowości*, w punkcie nr 2 niniejszego wystąpienia.

(akta kontroli str. 167-178, 541-545)

1.5. W Szpitalu opracowano wzór formularza oceny skutków dla ochrony danych (dalej: *DPIA*). DPIA, o której mowa w art. 35 RODO, nie została wykonana, bowiem jak wskazano w prowadzonym przez IOD rejestrze czynności przetwarzania *po przeprowadzeniu oceny ryzyka podjęto decyzję, że nie jest wymagana.*

Obowiązek wykonania tej oceny dotyczy bowiem planowanych operacji przetwarzania 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. Pojedyncza (bieżąca) ocena operacji wiążących się z wysokim ryzykiem także była fakultatywna, chociaż Grupa Robocza Art. 29 ds. Ochrony Danych[17] zdecydowanie zalecała dokonanie DPIA dla operacji przetwarzania już trwających przed 25 maja 2018 r. [18] i 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.* (akta kontroli str. 179-191)

1.6. W szkoleniach przeprowadzonych w związku z wejściem w życie RODO uczestniczyło 80% pracowników Szpitala (240 z 299). I tak:

- przed wejściem w życie przepisów dotyczących RODO (od 10 października 2017 r. do 17 maja 2018 r.) pięciu pracowników administracyjnych uczestniczyło w czterech szkoleniach i seminariach, których zakres uwzględniał wymogi RODO (m.in. zmiany w przepisach dotyczących ochrony danych osobowych, ochronę danych osobowych w działalności medycznej, zagadnienia dotyczące powierzenia danych osobowych i dostępu do dokumentacji medycznej);
- od 25 maja 2018 r. do 17 stycznia 2019 r. dwóch pracowników administracyjnych Szpitala uczestniczyło w szkoleniach zewnętrznych z zakresu RODO (zakres szkoleń obejmował m.in. obowiązkowe klauzule informacyjne dotyczące ochrony danych osobowych, zasady przetwarzania i udostępniania danych, zgodę na przetwarzanie danych, obowiązki ADO, powołanie IOD);
- 18 i 23 stycznia 2019 r. dla 240 z 299[19] (tj. 80 %) pracowników przeprowadzono szkolenie wewnętrzne związane z wejściem w życie przepisów dotyczących RODO, które obejmowało również zasady bezpiecznego użytkowania sprzętu IT, oprogramowania, Internetu i poczty elektronicznej oraz odpowiedzialność prawną w przypadku naruszenia bezpieczeństwa informacji. Nie obejmowało ono natomiast zagadnień określonych w § 20 ust. 2 pkt 6 lit a i c KRI, nie uczestniczyli w nim pracownicy zatrudnieni na umowy zlecenia i kontrakty, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji *Stwierdzone nieprawidłowości.* (akta kontroli str. 335-354)

1.7. W Szpitalu nie stosowano kodeksu dobrych praktyk, *Kodeksu postępowania dla sektora ochrony zdrowia* oraz nie kierowano się wskazówkami zawartymi w *Przewodniku po RODO*

---

[17] Grupa ta powołana została na mocy art. 29 dyrektywy 95/46/WE. Była ona niezależnym organem doradczym w zakresie ochrony danych i prywatności.

[18] 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 – dostęp z 4 marca 2019 r.

[19] Stan na 31 stycznia 2019 r.

dla służby zdrowia, opublikowanym 24 września 2018 r.[20], co stwierdzono w trakcie oględzin przeprowadzonych 17 stycznia 2019 r. i opisano w pkt 2.1 wystąpienia pokontrolnego i w opisie nieprawidłowości w punkcie nr 2. niniejszego wystąpienia.

Dyrektor Szpitala wyjaśniła, że *są to dokumenty zalecane, a nie wymagane i nie uznałam za konieczne ich formalnego przyjęcia do stosowania w szpitalu.*

(akta kontroli str. 124, 547-550)

Stwierdzone nieprawidłowości

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

1. Szpital w sporządzonej 14 czerwca 2018 r. PBI nie w pełni uwzględnił zmiany stanu prawnego wynikające z wejścia 25 maja 2018 r. w życie przepisów RODO, a dokumentację związaną z ochroną danych osobowych spełniającą wymogi tego rozporządzenia opracował dopiero 12 lutego 2019 r., natomiast do stosowania wprowadził ją zarządzeniem[21] z 20 marca 2019 r. Nieopracowanie takiej dokumentacji do 12 lutego 2019 r. stanowiło naruszenie art. 24 ust. 1 RODO, w myśl którego wdrożone przez ADO środki techniczne i organizacyjne, w tym obowiązujące w Szpitalu dokumenty, procedury i instrukcje, należało poddać przeglądom i dokonać stosownych zmian. Tymczasem w PBI:
   - nie zamieszczono zapisów dotyczących: prawa do ograniczenia przetwarzania (art. 18 RODO); obowiązku powiadomienia o sprostowaniu lub usunięciu danych osobowych, lub o ograniczeniu przetwarzania (art. 19 RODO), uwzględnianiu ochrony danych osobowych w fazie projektowania; domyślnej ochrony danych (art. 25 RODO),
   - kilkunastokrotnie pojawia się w niej określenie Administrator Bezpieczeństwa Informacji, mimo że podstawa prawna jego wyznaczenia utraciła ważność[22], a w jego miejsce powołano IOD,
   - treść zapisów odnosiła się do Generalnego Inspektora Ochrony Danych Osobowych, którego od 25 maja 2018 r. zastąpił PUODO,
   - nie zostały sporządzone załączniki, do których nawiązuje treść PBI.

   W dokumentacji nie zamieszczono informacji potwierdzających zapoznanie pracowników z nowo przyjętymi regulacjami wewnętrznymi.

   Dyrektor Szpitala wyjaśniła, że: *nasza interpretacja art. 24 RODO była odmienna niż interpretacja NIK. W natłoku innych obowiązków umknęło mojej uwadze wydanie zarządzenia w tej spawie.*

   IOD wyjaśnił, że: *Polityka z 14 czerwca 2018 r. była wzorowana na poprzedniej polityce, był to dokument wyjściowy. Nie została niestety do końca spójnie poprawiona. W trakcie kontroli została uzupełniona o wymagane informacje. Zapoznanie pracowników z treścią powyższych dokumentów nastąpiło na szkoleniach, jakie dobyły się w styczniu 2019 r. Ze względów organizacyjnych nie zawsze jest możliwe przeprowadzenie takich szkoleń w szybszym terminie. Projekt nowej Polityki był znany i na szkoleniach omawiano jego treść.* (akta kontroli str. 86-126, 339, 547-554)

2. Od 25 maja 2018 r. do 11 lutego 2019 r. w Szpitalu nie był prowadzony rejestr czynności przetwarzania danych osobowych, wbrew wymogom art. 30 ust. 1 RODO. Zgodnie z tym przepisem każdy administrator oraz – gdy ma to zastosowanie – przedstawiciel administratora prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają.

   Dyrektor Szpitala wyjaśniła, że nie wiedziała, że są jakieś problemy w sporządzeniu takiego rejestru.

---

[20] Opracowany przez zespół zadaniowy ds. ochrony zdrowia działający w ramach Grupy Roboczej ds. Ochrony Danych Osobowych, utworzonej w Ministerstwie Cyfryzacji; https://www.gov.pl/cyfryzacja/rodo-w-sluzbie-zdrowia-po-pierwsze-pacjent – dostęp z 3 października 2018 r.

[21] Zarządzenie Nr 9/2019 Dyrektora Samodzielnego Publicznego Zakładu Opieki Zdrowotnej w Augustowie z dnia 20 marca 2019 r.

[22] Art. 36a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U.2016 poz. 922, ze zm.).

IOD wyjaśnił, że: *rejestr był prowadzony w formie „zubożonej" i dopiero po audycie (...) rejestr ten uzupełniono i faktycznie dopiero 12 lutego 2019 r. jest w formie właściwej. Wcześniej nie miałem wiedzy, jakie dane należy prowadzić w tym rejestrze.*
(akta kontroli str. 179-196, 547-554)

3. Analiza procesów przetwarzania wraz z ryzykami i odpowiednimi zabezpieczeniami została przeprowadzona przez IOD 12 lutego 2019 r., tj. 263 dni po wejściu w życie przepisów RODO. Ponadto zgodnie z przyjętym planem postępowania z ryzykiem zabezpieczenia przed oprogramowaniem *ransomeware*, w postaci firewall planowano wdrożyć 31 grudnia 2019 r., podczas gdy ryzyko związane z tym zagrożeniem określono na poziomie nieakceptowalnym, przyznając mu dziewięć pkt. Wymóg przeprowadzenia analizy oraz wdrożenia zabezpieczeń wynika z art. 32 RODO, zgodnie z którym do obowiązków administratora należy wdrożenie odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający stwierdzonemu ryzyku.

   IOD wyjaśnił, że: *analiza taka przekraczała moją wiedzę, a także jest pracochłonna. Nie mogłem oderwać od obowiązków jedynego informatyka ze szpitala, stąd dopiero po nawiązaniu współpracy z audytorem zewnętrznym analiza została sporządzona. Nie negowałem terminów zaproponowanych przez audytora zewnętrznego. Dotyczy to jednak też kwestii finansowych i sprzętowych. Asekuracyjnie ustalono taki termin, natomiast zakup firewall został już zrealizowany.*

   Dyrektor Szpitala wyjaśniła, że: *nie sygnalizowano mi problemów z wywiązaniem się z tego obowiązku nałożonego nowym rozporządzeniem. Do chwili nawiązania współpracy z* audytorem zewnętrznym (przyp. NIK) *nie wiedziałam, że na rynku lokalnym jest firma, która mogłaby nam pomóc w kwestii wdrożenia RODO.*
   (akta kontroli str. 167-178, 547-554)

   NIK wskazuje, że w trakcie oględzin, przeprowadzonych 14 i 15 marca 2019 r., stwierdzono, że nie wdrożono części wymaganych zabezpieczeń, w tym na trzech (z 30 analizowanych) komputerach nie było zainstalowanego programu antywirusowego i firewalla, a na jednym program antywirusowy nie był aktualny (co szerzej opisano w opisie nieprawidłowości w punkcie 2. wystąpienia). Wskazuje to na konieczność szybszego niż do końca 2019 roku podjęcia działań w celu wyeliminowania zagrożeń typu *ransomeware*. (akta kontroli str. 541-545)

4. IOD nie wywiązał się w pełni z obowiązku przeprowadzenia szkoleń personelu uczestniczącego w przetwarzaniu danych, wynikającego z art. 39 ust. 1 lit b RODO. Po wejściu w życie tych przepisów (od 25 maja 2018 r.) nie zorganizowano niezwłocznie szkoleń i dopiero w trakcie kontroli NIK 240 z 299 (tj. 80%) pracowników uczestniczących w przetwarzaniu danych objęto szkoleniami. Obowiązek zapewnienia szkoleń osobom zaangażowanym w proces przetwarzania informacji wynika też z § 20 ust. 2 pkt 6 rozporządzenia KRI, a przeprowadzone 18 i 23 stycznia 2019 r. szkolenie nie uwzględniło wszystkich zagadnień określonych w tym przepisie. Nie obejmowało zagrożeń bezpieczeństwa informacji (§ 20 ust. 2 pkt 6 lit. a rozporządzenia KRI) i stosowania środków zapewniających bezpieczeństwo informacji, w tym urządzeń i oprogramowana minimalizującego ryzyko błędów ludzkich (§ 20 ust. 2 pkt 6 lit. c rozporządzenia KRI).

   IOD wyjaśnił, że: *kontrola NIK zdyscyplinowała nas do podjęcia działań i przeprowadzenia tych szkoleń, które wcześniej trudno było zorganizować z uwagi na zmianowość i konieczność pozostawania części personelu przy łóżkach pacjentów.*

   Dyrektor Szpitala wyjaśniła: *stało się tak z uwagi na to, że nie wiedziałam, że na rynku lokalnym jest firma, która może takie szkolenie przeprowadzić i pomóc we wdrażaniu RODO. Jednocześnie bardzo trudno jest oderwać personel medyczny od obowiązków i zebrać w jednym czasie na szkoleniu.* (akta kontroli str. 335-354, 547-554)

OCENA CZĄSTKOWA Najwyższa Izba kontroli ocenia negatywnie działania Szpitala w zakresie opracowania wymaganej dokumentacji oraz procedur związanych z ochroną przetwarzanych danych osobowych.

OBSZAR

2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych

Opis stanu faktycznego

2.1. Audytor wewnętrzny Szpitala przeprowadził 6 czerwca 2018 r. audyt w zakresie zgodności zapisów PBI z RODO oraz wykonał oględziny Szpitala. Stwierdzonych zostało szereg naruszeń, m.in. takich, jak przywoływanie pacjentów do gabinetów lekarskich po nazwisku, swobodny wgląd do monitorów komputerowych przez osoby rejestrujące się na wizyty, nieodpowiednie zabezpieczenie dokumentacji medycznej pacjentów, m.in. w niezamykanych szafkach, pozostawienie bez nadzoru włączonych komputerów z zalogowanym użytkownikiem do programu przetwarzającego dane osobowe, pozostawianie na tablicy korkowej loginów i haseł do systemów informatycznych, w których przetwarzane były dane osobowe, nieprzeszkolenie pracowników szpitala pod względem ochrony danych osobowych. (akta kontroli str. 356-359)

Dyrektor Szpitala wyjaśniła, że kilka dni po przeprowadzeniu tego audytu, na spotkaniu Komitetu ds. Bezpieczeństwa, *ustaliliśmy że należy usunąć stwierdzone usterki.* IOD wyjaśnił zaś, że po tym spotkaniu podjęto działania aby wyeliminować stwierdzone usterki: *Ukryte zostały tablice z ruchem chorych, usunięte zostały wszelkie karteczki z hasłami. Jeśli chodzi o brak zamykanych szafek na dokumenty – nie wszędzie ukończony zostały montaż zamków do czasu kontroli NIK.* (akta kontroli str. 547-554)

Oględziny wykazały, że pomimo upływu ponad siedmiu miesięcy od dnia audytu wewnętrznego do dnia rozpoczęcia kontroli, nie wszystkie powyższe naruszenia zostały wyeliminowane, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości*. Ustalono m.in., że:

- w dwóch funkcjonujących w ZOZ rejestracjach: do poradni specjalistycznych i lekarza podstawowej opieki zdrowotnej (POZ), nie zagwarantowano pacjentom właściwej anonimowości podczas rejestracji, nie wyznaczono strefy, w której może znajdować się jedna osoba, a pacjenci stali za sobą w bliskiej odległości (linię wyznaczono w trakcie kontroli NIK, już po oględzinach), a w miejscu, w którym w bliskiej odległości sąsiadowały ze sobą dwa okienka rejestracji, nie były one oddzielone (oddzielono je w trakcie kontroli NIK, po oględzinach);
- w rejestracjach nie posługiwano się nazwiskami pacjentów, co było właściwe z punktu widzenia ochrony ich prywatności (identyfikowano ich na podstawie dokumentów tożsamości), a ustawienie monitorów komputerowych nie pozwalało na wgląd do wyświetlanych na nich treści; pacjenci nie mieli również wglądu do dokumentacji medycznej;
- klauzula informacyjna o przetwarzaniu danych osobowych umieszczona była tylko przy jednej z rejestracji (przy drugiej została przyklejona w widocznym miejscu w trakcie oględzin);
- kolejność udzielania porad w gabinetach lekarskich[23] wyznaczana była według terminarza; pacjenci nie byli wywoływani poprzez podanie ich nazwisk, a poprzez werbalne wezwanie przez lekarza lub pielęgniarkę *proszę następną osobę*, co było właściwe z punktu widzenia ochrony prywatności pacjentów;
- dokumentacja w objętych oględzinami poradniach prowadzona była elektronicznie (nie było zatem papierowych dokumentów medycznych i pacjent nie miał możliwości wglądu do historii choroby innych pacjentów leczonych w kontrolowanych gabinetach);
- w dyżurkach pielęgniarek i gabinetach lekarskich trzech objętych oględzinami oddziałów (Chirurgii Urazowo-Ortopedycznej, Ginekologiczno-Położniczy, Chorób Wewnętrznych odcinek męski) niewłaściwie przechowywano dokumentację medyczną (w niezamykanych szafkach lub na półkach), za wyjątkiem jednej szuflady w dyżurce położnych na Oddziale Ginekologiczno-Położniczym i gabinetu lekarskiego na tym oddziale, gdzie część dokumentacji składowano w szufladach zamykanych na klucz;

[23] Oględziny przeprowadzono w poradniach: Ortopedycznej, Chirurgii Ogólnej i Lekarza POZ.

- ruch chorych – poza jedną z dyżurek na Oddziale Ginekologiczno-Położniczym – prowadzony był w miejscu, w którym osoby postronne nie miały do niego wglądu;
- w jednej z dyżurek pielęgniarskich na Oddziale Ginekologiczno-Położniczym pracownik pozostawił włączony komputer wraz z uruchomionym systemem HIS[24] i opuścił pomieszczenie;
- pacjenci każdego z kontrolowanych oddziałów (z wyjątkiem dwóch, którzy opuszczali oddziały w dniu oględzin) posiadali na nadgarstkach opaski zawierające imię i nazwisko, numer księgi głównej, kod kreskowy i kod QR (opaski były wydrukowane za pomocą drukarki specjalistycznej);
- na dwóch kontrolowanych oddziałach nie stosowało się kart gorączkowych na łóżkach pacjentów[25], a na kolejnym karty te były zasłonięte;
- stwierdzono pozostawiony klucz w drzwiach do gabinetu położnej jednego z oddziałów, w którym znajdowała się niezabezpieczona dokumentacja kadrowa (grafiki pracy) oraz włączony komputer z uruchomionym systemem HIS – moduł apteka;
- Szpital nie posiadał monitoringu wizyjnego. (akta kontroli str. 361-373, 566)

2.2. Personelowi działów administracyjnych[26] Szpitala ograniczono dostęp do systemu medycznego HIS wyłącznie w zakresie niezbędnym do wykonywanych zadań. Taki personel liczył 24 osoby, z których siedem posiadało dostęp do systemu HIS – jeden informatyk oraz sześciu pracowników Działu Statystyki i Dokumentacji Medycznej. W myśl art. 24 ust. 2 pkt 2 ustawy o prawach pacjenta, osoby wykonujące czynności pomocnicze przy udzielaniu świadczeń zdrowotnych, a także czynności związane z utrzymaniem systemu teleinformatycznego są uprawnione do dostępu do danych medycznych, na podstawie upoważnień administratora danych (pracownicy z dostępem do sytemu HIS posiadali takie upoważnienia). Żadna z osób zatrudnionych w działach administracyjnych nie posiadał dostępu do systemu EDM[27]. (akta kontroli str. 374-378)

2.3. Według stanu na 17 stycznia 2019 r. w Szpitalu zatrudnionych było 167 pielęgniarek lub położnych. Analizą objęto uprawnienia 30 pielęgniarek i położnych w systemie HIS. Wykazała ona, że 22 pielęgniarki i położne posiadały w tym systemie dostęp do pacjentów z innych oddziałów szpitalnych, a nie tylko z oddziału, na którym świadczyły pracę. Kwestię tę opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości.* Przedstawiono tam również wydawanie upoważnień do *odczytu* danych ze zbioru danych pacjentów dla salowych i sanitariuszy. (akta kontroli str. 379-393)

2.4. Od 25 maja 2018 r. do 17 stycznia 2019 r. 17 pracowników Szpitala zakończyło zatrudnienie, po czym trzech powróciło do świadczenia pracy. Pozostałych 14 posiadało nieaktywny dostęp do domeny Windows oraz oprogramowania HIS i EDM. Wprawdzie z uprawnień administratora nie można było (bez czasochłonnej analizy logów) stwierdzić kiedy dostęp do systemów został zablokowany, jednak z analizy dat ostatniego logowania wynika, że nikt nie logował się po dniu zakończenia pracy. W Szpitalu stosowano papierowy *Wniosek o nadanie uprawnień w systemie informatycznym*[28], który wystawiała Kierownik Działu Spraw Personalnych i Socjalnych i przekazywała służbom informatycznym. Potwierdzały one na tym dokumencie fakt odebrania uprawnień, jednak na żadnym z tych 14 wniosków nie wpisywano daty dokonania tej czynności. (akta kontroli str. 429-433)

Informatyk Szpitala wyjaśnił, że uprawnienia odbierał w dacie wskazanej we wniosku[29]. Proces ten nie był czasochłonny i uprawnienia odbierał na bieżąco. (akta kontroli str. 557)

---

[24] Hospital Information System – rodzaj oprogramowania do obsługi ruchu pacjentów wewnątrz podmiotu leczniczego.
[25] Oddział Ginekologiczno-Położniczy i Oddział Chorób Wewnętrznych (oddinek męski).
[26] Dział Organizacji i Kontroli oraz Zamówień Publicznych, Dział Spraw Osobowych i Socjalnych, Dział Finansowo Księgowy, Dział Płac, Dział Techniczno-Gospodarczy i Zaopatrzenia wraz ze stanowiskiem ds. informatyzacji, Dział Statystyki Medycznej, samodzielne stanowiska pracy i dyrektorzy.
[27] EDM – repozytorium elektronicznej dokumentacji medycznej.
[28] Możliwą opcją do zaznaczenia w tym wniosku było nadanie uprawnień nowemu użytkownikowi, modyfikacja posiadanych uprawnień lub odebranie uprawnień w systemie informatycznym.
[29] Wskazywała ją Kierownik Działu Spraw Osobowych i Socjalnych.

2.5. Szpital był uczestnikiem projektu *Podlaski System Informacyjny e-Zdrowie*. Dla posiadanego oprogramowania miał uruchomioną usługę zdalnego zgłaszania dostawcy oprogramowania usterek w działaniu oprogramowania. Usterki były zgłaszane online poprzez dedykowaną stronę internetową. Usługa IZGL służyła do zgłaszania usterek dla oprogramowania używanego w części administracyjnej ZOZ, a NCR do oprogramowania związanego z ruchem chorych. Analiza 50 ze 112 zgłoszeń wykonanych za pomocą NCR między 25 maja 2018 r. a 6 marca 2019 r. wykazała, że w pięciu zgłoszeniach serwisowych (lub w załącznikach do nich) zostały podane personalia, PESEL lub opis procesu leczenia ośmiu pacjentów, co opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości*. W pozostałych przypadkach Szpital zanonimizował dane pacjentów.

(akta kontroli str. 434-463)

2.6. ADO zawarł pięć umów powierzenia przetwarzania danych osobowych w związku z: [1] asystą techniczną oprogramowania, [2] umową serwisową sprzętu IT, [3] usługą administrowania systemami informatycznymi oraz serwerami, [4] świadczeniem usług prawnych i [5] wykonywaniem badań serologicznych. We wszystkich umowach Szpital występował jako podmiot powierzający przetwarzanie danych. Umowy, zgodnie z art. 28 ust. 2 RODO określały przedmiot, czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, a także obowiązki i prawa administratora oraz stanowiły, że podmioty, którym Szpital powierzył przetwarzanie danych w szczególności:

- podejmą wszelkie niezbędne środki bezpieczeństwa dla ochrony przetwarzanych danych;
- zapewnią, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
- pomogą administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO;
- usuną lub zwrócą wszelkie dane osobowe oraz usuną wszelkie ich kopie, po zakończeniu świadczenia usług związanych z przetwarzaniem, zależnie od decyzji ADO, chyba że prawo nakazuje przechowywanie danych osobowych;
- umożliwią przeprowadzanie audytów, w tym inspekcji. (akta kontroli str. 464-465)

2.7. W Szpitalu 12 lutego 2019 r. wprowadzono instrukcję postępowania z incydentami, skróconą instrukcję postępowania w przypadku naruszenia ochrony danych osobowych i wzór rejestru naruszeń ochrony danych osobowych oraz incydentów bezpieczeństwa danych (odpowiednio w ramach Polityki Ochrony Danych Osobowych i Regulaminu Ochrony Danych Osobowych[30]). Zgodnie z uregulowaniami każda osoba upoważniona do przetwarzania danych osobowych była zobowiązana do powiadomienia IOD o stwierdzeniu lub podejrzeniu naruszenia ochrony danych osobowych w przypadku: [1] niewłaściwego zabezpieczenia fizycznego pomieszczeń, urządzeń i dokumentów, [2] niewłaściwego zabezpieczenia sprzętu i oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych, [3] nieprzestrzegania zasad ochrony danych osobowych (czystego biurka/ekranu, ochrony haseł, zamykania pomieszczeń i szaf), [4] zdarzeń losowych zewnętrznych i wewnętrznych, [5] umyślnych incydentów (włamań do systemów informatycznych lub pomieszczeń, kradzieży danych lub sprzętu, wycieku informacji, ujawnienia danych osobom nieupoważnionym, świadomym niszczeniem dokumentów/danych, działania wirusów i innego szkodliwego oprogramowania). Na dzień 20 marca 2019 r. rejestr naruszeń ochrony danych osobowych nie został uzupełniony, pomimo stwierdzenia, w trakcie przeprowadzonych 14 i 15 marca 2019 r. oględzin, sytuacji wymagających powiadomienia, co szerzej opisano w dalszej części wystąpienia pokontrolnego, w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli str. 124, 127-134, 235, 547-554)

[30] Do 11 lutego 2019 r. opis zdarzeń naruszających ochronę danych osobowych oraz zasady postępowania w sytuacji naruszenia systemu ochrony danych osobowych regulowała PBI, na podstawie § 20 pkt 13 KRI.

2.8. Sposób udostępniania dokumentacji medycznej pacjentom oraz osobom i podmiotom upoważnionym przez pacjentów opisywała procedura wewnętrzna Działu Statystyki i Dokumentacji Medycznej[31]. Od 25 maja 2018 r. do 5 marca 2019 r. złożonych było 735 wniosków o udostępnienie dokumentacji medycznej, w tym 139 przez instytucje (z tego 19 przez firmy ubezpieczeniowe) i 596 przez osoby prywatne (dwa wnioski wycofano). Nie było przypadków odmowy udostępnienia dokumentacji medycznej.

Badaniem objęto 49 spraw zakończonych wydaniem dokumentacji medycznej, w tym: 19 (wszystkie), w których o wydanie dokumentacji zwróciły się firmy ubezpieczeniowe oraz 30, w których o wydanie dokumentacji zwróciły się osoby inne niż pacjent. I tak:

- we wszystkich 19 przypadkach, w których dokumentacja była udostępniona firmom ubezpieczeniowym, do wniosków były dołączone upoważnienia pacjentów lub kopie polisy ubezpieczeniowej,
- w 26 przypadkach, w których o udostępnienie dokumentacji medycznej wystąpiły osoby inne niż pacjent, były one upoważnione przez pacjenta do dostępu, zgodnie z art. 26 ust. 1 ustawy o prawach pacjenta,
- w czterech przypadkach Szpital udostępnił dokumentację medyczną trzem osobom nieuprawnionym, a w kolejnym – nieznanej osobie, występującej o kopię dokumentacji medycznej poprzez e-mail, bez osobistego stawiennictwa, jednocześnie nie prowadzono wykazu zawierającego informacje dotyczące udostępnianej dokumentacji medycznej (dla pacjentów lub osób upoważnionych przez pacjentów), o którym mowa w art. 27 ust. 4 powołanej ustawy, co szerzej opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości.* (akta kontroli str. 527-530)

2.9. Zarządzenie siecią komputerową odbywało się centralne za pomocą usługi Active Directory. Autoryzacja w systemie HIS wymagała podania indywidulanego loginu i hasła użytkownika, stwierdzono natomiast, że uwierzytelnianie w systemach operacyjnych komputerów nie zawsze wymagało podania tych danych, co opisano w dalszej części wystąpienia, w sekcji *Stwierdzone nieprawidłowości.* Hasła podlegały okresowej zmianie, ustawionej automatycznie przez administratora systemów informatycznych.

Szpital dysponował 100 komputerami, w tym dziewięcioma laptopami, które – jak podał informatyk Szpitala – służyły do pracy, jako urządzenia stacjonarnie. Dyski laptopów nie były szyfrowane, nie korzystano również z pseudonimizacji danych, gdyż – jak wyjaśnił informatyk – nie było takiej potrzeby. Oględzinami NIK objęto 30 komputerów (w tym jeden laptop), po 10 użytkowanych przez lekarzy, pielęgniarki lub położne i pracowników administracyjnych. Stwierdzono, że:

- 29 komputerów pracowało na systemie Windows 7 lub wyższym[32], a jeden na systemie Windows XP, chociaż ten system operacyjny od 8 kwietnia 2014 r. nie jest objęty wsparciem producenta, co oznacza, że nie będą udostępniane nowe poprawki zabezpieczeń, poprawki niedotyczące zabezpieczeń, bezpłatne lub płatne wsparcie techniczne i aktualizacje zawartości technicznej online,
- dostęp do 26 komputerów ze zbadanej próby ograniczony był poprzez konieczność podania loginu i hasła, a z czterech komputerów można było korzystać bez podania takich danych (liczba znaków haseł w komputerach, do których dostęp wymagał ich podania, odpowiadała wymaganiom co do ich odpowiedniej złożoności),
- w 26 komputerach zainstalowany był program antywirusowy z zaimplementowaną aktualną bazą wirusów, trzy kolejne nie posiadały takiej ochrony, a w czwartym baza wirusów była nieaktualna od 502 dni,
- 19 użytkowników posiadało uprawnienia standardowe, co wykluczało m.in. możliwość instalacji dowolnego oprogramowania, kolejnych zaś 11 nadano uprawnienia administratora,

---

[31] *Procedura udostępniania dokumentacji medycznej*, opracowana przez Kierownika Działu Statystyki i Dokumentacji Medycznej (nie posiadała daty wdrożenia) umieszczona była na stronie internetowej Szpitala pod adresem http://www.spzoz.augustow.pl/dokumedyczna – dostęp z 25 marca 2019 r.

[32] 22 Windows 7, sześć Windows 8, jeden Windows 10.

– we wszystkich komputerach objętych oględzinami porty USB umożliwiały odczytywanie danych z podłączonego nośnika.

Niewłaściwe zabezpieczenie komputerów przed utratą danych elektronicznych szerzej opisano poniżej, w sekcji *Stwierdzone nieprawidłowości.*

Serwerownia została zabezpieczona przed dostępem osób postronnych. Prowadziły do niej drzwi przeciwpożarowe zamykane na dwa zamki oraz zainstalowany był system alarmowy, dezaktywowany kartą magnetyczną. Wewnątrz, na podłodze technicznej, umieszczone były dwie szafy typu rack z macierzami na których zainstalowane zostały systemy użytkowane w Szpitalu. Na wyposażeniu znajdował się system klimatyzacji oraz czujnik pożarowy i gaśnica. W trakcie oględzin stwierdzono jednak pozostawienie łatwopalnych materiałów, co opisano także poniżej, w sekcji *Stwierdzone nieprawidłowości.* (akta kontroli str. 541-546)

Kopie bezpieczeństwa od 23 lutego 2019 r. (po zakupie serwera do kopii zapasowych) przechowywane były w innej lokalizacji niż serwerownia. W trakcie kontroli P/16/059 Podlaski System Informacyjny e-Zdrowie stwierdzono, że kopie zapasowe przechowywane były krzyżowo na dyskach serwerów Szpitala, znajdujących się w pomieszczeniu serwerowni. Stwierdzono również wówczas, że pełna kopia – pomimo zapisów w Instrukcji Zarządzania Systemem Informatycznym – nie była z przyczyn technicznych przesyłana raz w tygodniu na serwer znajdujący się w Urzędzie Marszałkowskim Województwa Podlaskiego. Serwer ten miał m.in. służyć partnerom projektu do składowania kopii zapasowych. Niewłaściwe przechowywanie kopii zapasowych do 23 lutego 2019 r. szerzej opisano poniżej, w sekcji *Stwierdzone nieprawidłowości.* Informatyk Szpitala wyjaśnił, że kopie różnicowe wykonywane były codziennie, a co tydzień kopie pełne.

(akta kontroli str. 557-561)

Stwierdzone nieprawidłowości

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

1. Podjęte przez Szpital działania nie we wszystkich obszarach zapewniały adekwatną ochronę prywatności pacjentów oraz danych zawartych w dokumentacji medycznej. W trakcie oględzin NIK stwierdzono, że:
   - W dyżurkach pielęgniarskich i pokojach lekarskich objętych oględzinami oddziałów szpitalnych[33] dokumentacja medyczna przechowywana była w niezamykanych szufladach lub na półkach (wyjątkiem było jedno z biurek w gabinecie lekarskim na Oddziale Ginekologiczno-Położniczym i jedna z szuflad w dyżurce pielęgniarskiej na tym samym oddziale, które były zamykane na klucz).
   - W każdym z trzech objętych oględzinami gabinetów poradni monitory[34] ustawione były prostopadle do kierunku ruchu pacjenta, który mógł widzieć wyświetlane treści.
   - Do jednego z pomieszczeń na Oddziale Ginekologiczno-Położniczym został pozostawiony klucz w drzwiach. Wewnątrz znajdowała się dokumentacja kadrowa pracowników i uruchomiony system HIS – moduł apteka. Na tym samym oddziale w dyżurce położnych pracownik, zalogowany w systemie HIS, opuścił stanowisko pracy i nie wylogował się uprzednio z systemu ani nie zablokował stacji roboczej.
   - Przy rejestracji do poradni specjalistycznych nie wyznaczono strefy przebywania jednego pacjenta, a w trakcie oględzin stwierdzono, że kolejni pacjenci stali w bliskiej odległości od pacjenta aktualnie obsługiwanego przez pracowników rejestracji. Obszar przebywania jednego pacjenta wyznaczono w trakcie kontroli NIK. Wyznaczenie takiej strefy rekomendowane było w *Przewodniku po RODO w służbie zdrowia.*
   - Dwa okienka rejestracji do poradni specjalistycznych były zlokalizowane w bliskiej odległości od siebie i nie były przedzielone, co również rekomendowane było w wymienionym przewodniku. Płytą oddzielono je w trakcie kontroli NIK.

[33] Oddziały: Chirurgii Urazowo-Ortopedycznej, Ginekologiczno-Położniczy, Chorób Wewnętrznych odcinek męski.
[34] Poradnie: Ortopedyczna, Chirurgii Ogólnej i Lekarza Podstawowej Opieki Zdrowotnej.

- Ruch chorych w jednej z trzech dyżurek Oddziału Ginekologiczno-Położniczego prowadzony był na tablicy zawieszonej na ścianie, na której znajdowało się imię i nazwisko pacjenta oraz numer zajmowanej sali. (akta kontroli str. 361-372)

Powyższe działania stwarzały ryzyko ujawnienia danych osobowych i/lub danych medycznych pacjentów. Zgodnie z art. 24 ust. 1 RODO administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z tym rozporządzeniem. Jednocześnie, w myśl motywu 39 preambuły oraz art. 5 ust. 1 lit. f. RODO, dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich, niedozwolonym lub niezgodnym z prawem przetwarzaniem. W myśl art. 13 ustawy o prawach pacjenta, pacjent ma prawo do zachowania w tajemnicy przez osoby wykonujące zawód medyczny informacji z nim związanych, uzyskanych w związku wykonywaniem tego zawodu.

Dyrektor Szpitala wyjaśniła, że nie wiedziała, że takie sytuacje mają miejsce. Dyrektor sporadycznie przebywa w obszarze medycznym szpitala i według niej na pewno wymaga to poprawy, *(...) podjęliśmy już pewne działania i nadal będziemy je realizować. Jeśli chodzi o rejestrację i brak przepierzenia między okienkami oraz brak linii oddzielającej kolejnych pacjentów – jest to nowa rejestracja uruchomiona w IV kwartale 2018 r. i nie zdążyliśmy zainstalować wszystkich elementów.* IOD wyjaśnił zaś, że: *(...) kwestie te wymagają wzmocnienia nadzoru, częstszych audytów wewnętrznych. Jeśli chodzi zaś o zamknięcia szafek z dokumentacją medyczną – zostało już zlecone pracownikowi gospodarczemu szpitala wykonanie takich zamknięć.* Pracownicy, którzy pozostawili niezablokowane komputery wyjaśnili, że musieli opuścić miejsce pracy w pośpiechu. Wynikało to z nawału ich obowiązków, ale są świadomi zaniedbania, jakie popełnili. (akta kontroli str. 547-554, 569-572)

NIK wskazuje, że podobne ustalenia poczynił audytor wewnętrzny ponad osiem miesięcy przed rozpoczęciem kontroli NIK i Szpital miał wystarczająco dużo czasu na podjęcie skutecznych działań.

2. Opaski na nadgarstkach pacjentów trzech oddziałów[35] zawierały – poza numerem księgi głównej, kodem kreskowym i kodem QR – imię i nazwisko pacjenta. Zgodnie zaś z art. 36 ust. 5 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej[36] – opaska zawierać powinna informacje zapisane w sposób uniemożliwiający identyfikację pacjenta przez osoby nieuprawnione. (akta kontroli str. 361-373)

   Dyrektor Szpitala wyjaśniła, że nie wiedziała, że te opaski drukowane są w taki sposób. *Polecę poprawienie tekstu na opaskach zgodnie z ustawą o lecznictwie.* IOD również nie miał świadomości takiej praktyki. Informatyk Szpital wyjaśnił zaś, że w rozmowie z konsultantem dostawcy oprogramowania ustalił, że takie ustawienia poczynił dostawcza oprogramowania w chwili wdrażania całego systemu w 2015 roku, gdy informatyk nie byłem jeszcze pracownikiem Szpitala i że na prośbę Szpitala dostawca oprogramowania może zmienić dowolnie te ustawienia, bo Szpital sam nie ma możliwości dokonania takiej zmiany. (akta kontroli str. 547-554, 556-557)

3. Dwadzieścia dwie z 30 (73,3%) objętych analizą pielęgniarek i położnych miało dostęp w systemie HIS do oddziałów lub poradni szpitalnych, na których nigdy nie świadczyły pracy lub pracowały w tych komórkach organizacyjnych – według danych z Działu Spraw Osobowych i Socjalnych – jeszcze w latach 90. W zależności od pracownika był im przyznany dostęp od jednego do siedmiu dodatkowych oddziałów lub poradni. (akta kontroli str. 379-393)

   Analizowane pielęgniarki i położne posiadały wprawdzie upoważnienia do przetwarzania danych osobowych ze zbioru dotyczącego pacjentów, niemniej w art. 5 pkt 1 lit. c RODO wskazano zasadę adekwatności i minimalizacji danych, tj. wymóg ustalenia kto i w jakim zakresie jest uprawniony do przetwarzania danych. Z kolei w § 20 ust. 2 pkt 4

[35] Oględzinami objęto oddziały: Chirurgii Urazowo-Ortopedycznej, Ginekologiczno-Położniczy i Chorób Wewnętrznych odcinek męski.
[36] Dz. U. z 2018 r. poz. 2190, ze zm.

rozporządzenia KRI zawarto zobowiązanie dla kierownictwa podmiotu publicznego do podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji mają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań. Zdaniem NIK nie ma potrzeby nadawać większych uprawnień personelowi pielęgniarskiemu lub położniczemu niż oddział (lub oddziały i poradnie), w których faktycznie świadczyły pracę.

Uprawnienia w systemie HIS zostały nadane pracownikom podczas wdrażania *Podlaskiego Systemu Informacyjnego e-Zdrowie* i nie wykonał tego obecny informatyk Szpitala. Dyrektor wyjaśniła, że nie wiedziała, że pielęgniarki mają nadane takie uprawnienia w systemie typu HIS i że prawdopodobnie takie uprawnienia nadano im w trakcie realizacji projektu e-Zdrowie i od tamtej pory nikt tego nie weryfikował. IOD wyjaśnił, że również nie wiedział, że takie uprawnienia nadano pielęgniarkom i podjęte zostaną działania aby to zmienić. (akta kontroli str. 547-554)

4. W pięciu (z 50 analizowanych) zgłoszeniach za pośrednictwem systemu help desk NCR (lub w załącznikach do nich) zamieszczono niezanonimizowane dane personalne ośmiu pacjentów: imię i nazwisko, PESEL, w tym dane medyczne czterech. Nie było to niezbędne do rozwiązania zgłaszanego problemu. Nawet dostawca oprogramowania w jednym z komunikatów prosił o podawanie numeru ID pacjenta, zamiast jego danych osobowych[37]. (akta kontroli str. 434-463)

   W art. 5 pkt 1 lit. c RODO wskazano zasadę adekwatności i minimalizacji danych. Podanie imienia, nazwiska, PESEL-u i danych medycznych było zaś zbędne do usunięcia usterki. IOD wyjaśnił, że dowiedział się o tym w trakcie kontroli NIK. *Elementarnym obowiązkiem zgłaszających jest zachować odpowiednią anonimizację danych*. Dyrektor Szpitala wyjaśniła, że nie wiedziała o takich praktykach. Pracownicy wysyłający zgłoszenia zawierające dane osobowe lub dane medyczne pacjentów wyjaśnili, że nie są w stanie sobie przypomnieć co mogło być przyczyną takich sytuacji – być może załączony został niewłaściwy plik (zrzut z ekranu), na którym nie były zanonimizowane dane pacjentów, a może nie nadpisał się on w procesie anonimizacji danych, ale były to ich zdaniem sytuacje sporadyczne. Wyjaśniali to również pośpiechem i przeoczeniem. (akta kontroli str. 547-557)

5. Trzynastu, z analizowanej grupy 15 pracowników obsługi[38], upoważniono do dostępu (siedem osób) lub przetwarzania (sześć osób) danych ze zbioru danych pacjentów. W rejestrze upoważnień każdorazowo wskazano że poziom dostępu dotyczy *odczytu* danych z tego zbioru[39]. W treści upoważnień dziesięciu osób wskazano, że związane jest to z odbiorem wyników badań z pracowni diagnostycznych, a w przypadku trzech osób wskazano ogólnie, że dotyczy to danych, *do których ma dostęp podczas wykonywania swoich obowiązków w czasie udzielania świadczeń zdrowotnych pacjentom*. Zadaniami tych osób (salowe, sanitariusz, sterylizator z bloku operacyjnego) była m.in. pomoc w obsłudze chorego, utrzymanie należytej czystości sal chorych, pomoc w zmianie bielizny, czuwanie nad bezpieczeństwem chorych, wykonywanie wszelkich zleceń lekarzy i pielęgniarek w zakresie obsługi chorych, sterylizacja materiałów opatrunkowych i bielizny, testowanie wsadów i prowadzenie dokumentacji skuteczności sterylizacji, transport chorych do pracowni diagnostycznych, transport odpadów i śmieci. W indywidualnych zakresach obowiązków powyższej grupy osób nie stwierdzono zapisów o wykonywaniu obowiązków wymagających dostępu lub przetwarzania przez nich danych medycznych ze zbioru danych pacjentów. Wystarczające byłoby zatem odbieranie od tych pracowników deklaracji lub zobowiązania o zachowaniu w tajemnicy informacji, z którymi mogli mieć kontakt w trakcie wykonywania obowiązków służbowych. Dostęp do danych osobowych przez te osoby nie jest niezbędny (konieczny) do realizacji ich obowiązków służbowych, nawet tych związanych z transportem chorych, a sam

---

[37] Komunikat w zgłoszeniu 2018/9621.

[38] Ogółem takich pracowników było w Szpitalu 58, z których 46 miało wydane upoważnienia do odczytu danych ze zbioru danych pacjenta. Upoważnień nie wydano sprzątaczkom, krawcowej, konserwatorowi c.o., konserwatorowi urządzeń elektrycznych, stolarzowi.

[39] Pozostałe możliwe poziomy dostępu to tworzenie, modyfikacja, usuwanie, archiwizacja, administracja systemami informatycznymi.

transport chorego i odbiór wyników badań może być zorganizowany w sposób zapewniający właściwą ochronę danych, bez konieczności dostępu do nich i ich przetwarzania. (akta kontroli str. 246-333, 394-428)

Dyrektor Szpitala, wyjaśniając powody wydania upoważnień tej grupie pracowników podała, że jest to pomocne w bieżącej pracy oddziałów. Salowe i sanitariusze przewożą pacjentów na diagnostykę, odbierają wyniki badań. Dodała też, że: *(...) dokonamy wewnętrznej oceny, czy można odebrać te upoważnienia i nie odbędzie się z uszczerbkiem dla właściwej pracy Szpitala.* IOD wyjaśnił, że działanie to służyło usprawnieniu pracy szpitala, *(...) inna organizacja będzie wymagała dodatkowych działań i będzie zabierać czas personelowi. W systemie typu HIS nie ma wyników badań, bo nie została przeprowadzona integracja w ramach e-Zdrowia, a jest ona bardzo kosztowna.* (akta kontroli str. 547-554)

W ramach kontroli P/16/059 Podlaski System Informacyjny e-Zdrowie ustalono, że zakupiony w ramach tego projektu system HIS nie posiadał funkcjonalności pozwalających na wymianę danych z system pracowni RTG i systemem laboratorium. Przewidywany koszt integracji tych systemów z HIS to koło 1.000 tys. zł.

Podgląd już utrwalonych danych stanowi ich przetwarzanie. Pracownicy obsługi nie powinni mieć wglądu do dokumentacji medycznej, ze względu na przepisy art. 9 ust. 1 i 2 RODO, uzależniające dostęp do tzw. szczególnych kategorii danych, w tym danych dotyczących zdrowia, od spełnienia określonych, szczególnych warunków (np. zapewnienia opieki zdrowotnej lub leczenia). Jednocześnie, zgodnie z art. 24 ust. 2 i art. 26 ust. 1 ustawy o prawach pacjenta, dokumentację medyczną można ujawnić tylko określonym podmiotom, w tym podmiotom leczniczym, osobom wykonującym zawód medyczny uczestniczącym w udzielaniu świadczeń medycznych lub właściwym organom. Podobne zasady określają art. 40 i art. 41 ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty[40]. Nie mają też zastosowania przepisy art. 24 ust. 2 pkt 2 ustawy o prawach pacjenta, dotyczące osób wykonujących czynności pomocnicze przy udzielaniu świadczeń zdrowotnych, które są uprawnione do dostępu do danych medycznych, na podstawie upoważnień administratora danych. Zadania związane z dostępem do danych medycznych nie wynikają z zakresów obowiązków analizowanych osób. Ponadto, zgodnie z art. 5 ust. 1 i art. 6 ust. 1 RODO, przetwarzanie danych powinno być ograniczone i zminimalizowane do tego, co jest niezbędne do celów przetwarzania. Sprzątanie pomieszczeń, dbanie o czystość pacjentów, transport chorych i kierowanie pojazdem, nie stanowi celu przetwarzania, uzasadniającego dostęp do danych. Przewóz pacjentów i odbieranie wyników zleconych badań powinny być zorganizowane w sposób uniemożliwiający personelowi dostęp do danych medycznych.

6. Do rejestru naruszeń ochrony danych osobowych oraz incydentów zagrażających bezpieczeństwu danych nie wpisano incydentów stwierdzonych podczas oględzin NIK, przeprowadzonych 14 i 15 marca 2019 r. Obowiązek przekazania IOD takich informacji wynikał z treści punktu 1 w rozdziale 7 Polityki Ochrony Danych Osobowych oraz z treści pkt 1 rozdziału 9 Regulaminu Ochrony Danych Osobowych. Stwierdzone naruszenia dotyczyły niewłaściwego zabezpieczenia sprzętu i oprogramowania m.in.: uruchomienie czterech komputerów nie wiązało się z koniecznością podania loginu i hasła, jedenastu użytkowników posiadało uprawnienia administratora w systemie operacyjnym, na trzech komputerach nie było zainstalowanego programu antywirusowego, a na jednym nie był on aktualny.

   Pracownik uczestniczący wraz z kontrolerem NIK w oględzinach wyjaśnił, że mówił IOD o stwierdzonych w trakcie oględzin ustawieniach komputerów, jednak nie podał przykładów. *(...) po uzyskaniu kopii protokołu z tych oględzin rozpocząłem wraz z informatykiem naprawę stwierdzonych usterek i z pośpiechu nie przedstawiłem szczegółów IOD.*

   Dyrektor Szpitala wyjaśniła, że nie była świadoma, że takie informacje nie zostały przekazywane IOD.

[40] Dz. U. z 2018 r. poz. 617, ze zm.

IOD wyjaśnił, że nie otrzymał informacji o takich incydentach, stąd nie zostały one zaewidencjonowane w rejestrze. (akta kontroli str. 124, 228-235, 541-545, 547-555)

Świadczy to o niewłaściwym zapoznaniu pracowników Szpitala z przyjętymi uregulowaniami z zakresu ochrony danych osobowych, w szczególności dotyczącymi sposobu postępowania w przypadku naruszenia ochrony danych osobowych.

7. Szpital, w czterech z 49 zbadanych (8,2%) sprawach nieprawidłowo udostępnił dokumentację medyczną, czym wbrew wymogom określonym w art. 24 ustawy o prawach pacjenta, nie zapewnił ochrony danych zawartych w dokumentacji medycznej:
   - w trzech przypadkach dokumentacja medyczna była udostępniona osobom nieupoważnionym przez pacjentów, wbrew art. 26 ust. 1 ustawy o prawach pacjenta, zgodnie z którym podmiot udzielający świadczeń zdrowotnych udostępnia dokumentację medyczną pacjentowi lub jego przedstawicielowi ustawowemu bądź osobie upoważnionej przez pacjenta;
   - w jednym przypadku nie zweryfikowano tożsamości osoby, której udostępniono dokumentację medyczną. Dokumentacja została udostępniona pocztą elektroniczną (e-mail) na wniosek złożony tą samą drogą, podczas gdy – zgodnie z obowiązującą w Szpitalu procedurą udostępniania dokumentacji medycznej – powinna być ona udostępniana za okazaniem dokumentu potwierdzającego tożsamość.

   Jednocześnie w Szpitalu nie był prowadzony wykaz zawierający informacje dotyczące udostępnianej dokumentacji medycznej dla pacjentów lub osób upoważnionych przez pacjentów, wymagany art. 27 ust. 4 ustawy o prawach pacjenta, a na złożonych wnioskach nie było danych (imienia i nazwiska) oraz podpisu pracownika, który udostępnił dokumentację medyczną.

   Kierownik Statystyki wyjaśniła, że: *udostępnianiem dokumentacji medycznej zajmuje się jeden pracownik, a w przypadku jego nieobecności zastępują go pozostałe osoby z działu. Nie pamiętam, który z pracowników udostępnił dokumentację medyczną oraz jakie były przyczyny udostępnienia dokumentacji osobom nieupoważnionym. W przypadku udostępnienia dokumentacji e-mailem, prawdopodobnie pacjentka kontaktowała się wcześniej w innej sprawie, w związku z tym była nam znana, dlatego dokumentacja został udostępniona tą drogą. Uznałam, że wykazem są wnioski zebrane w kolejności chronologicznej, ponieważ zawierają wymagane elementy, poza imieniem i nazwiskiem oraz podpisem osoby, która udostępniła dokumentację medyczną.*
   (akta kontroli str. 527-540)

   Dyrektor Szpitala wyjaśniła, że nie ma kontroli nad wszystkimi działaniami pracowników. Pracownicy są uczuleni na właściwe postępowanie z udostępnianiem dokumentacji pacjentów. IOD wyjaśnił zaś, że nie miał wiedzy o takich praktykach. Jego zdaniem przepisy prawa w tym zakresie powinny być ściśle przestrzegane przez pracowników wydających dokumentację medyczną. (akta kontroli str. 547-554)

   Brak danych pracownika, który udostępnił dokumentację medyczną uniemożliwia jego identyfikację oraz możliwość wyciągnięcia wobec tego pracownika konsekwencji służbowych. Jednocześnie NIK wskazuje, że procedura udostępniania dokumentacji medycznej została opracowana przez kierownika Działu Statystyki i Dokumentacji Medycznej – nie był to zatem dokument wprowadzony zarządzeniem Dyrektor Szpitala.

8. Podczas oględzin 30 komputerów[41] (po 10 obsługiwanych przez lekarzy, pielęgniarki i pracowników administracyjnych) stwierdzono następujące naruszenia bezpieczeństwa danych przechowywanych w postaci elektronicznej:
   - Jedenastu (36,7%) użytkowników komputerów posiadało uprawnienia administratora, chociaż nie wykonywali czynności związanych z zapewnieniem prawidłowego działania sieci komputerowej Szpitala. Posiadanie takich uprawnień było niezgodne z § 20 ust. 2 pkt 4 rozporządzenia KRI, według którego zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji

[41] Łącznie Szpital posiadał 100 komputerów.

posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków, mających na celu zapewnienie bezpieczeństwa informacji. Było to również niezgodne z punktem 6 rozdziału 3 Instrukcji Zarządzania – RODO – Wykaz Zabezpieczeń RODO, który stanowił, że obowiązuje zasada minimalizacji uprawnień.

- Dostęp do czterech (13,3%) komputerów nie wymagał podania loginu i hasła. Trzy z tych komputerów (75%) miały dla ich użytkownika nadane uprawnienia administratora. Dodatkowo na jednym z tych komputerów (Oddział Pediatryczny) w podręcznych folderach zamieszczone były dokumenty zawierające dane osobowe pacjentów wraz z historią leczenia. Możliwość uruchomienia komputera bez podania loginu i hasła była niezgodna z punktem 1 rozdziału 3 Instrukcji Zarządzania – RODO – Wykaz Zabezpieczeń RODO, który mówił o tym, że dostęp do systemu informatycznego nadawany jest każdemu użytkownikowi w formie indywidualnego identyfikatora (loginu). Działanie to było również niezgodne z § 20 ust. 2 pkt 7 lit. a i § 21 ust. 2 pkt 3, w związku z § 20 ust. 1 rozporządzenia KRI, gdyż bez przyznania indywidualnych loginów użytkownikom, nie była możliwa prawidłowa rozliczalność systemów. Przy takich rozwiązaniach nie jest możliwe do ustalenia, która z osób fizycznych używających tego samego (jednego) loginu, przetwarzała w systemach (w tym przypadku w systemie operacyjnym) dane podlegające prawnej ochronie. Jednocześnie – zgodnie z motywem 39 preambuły RODO – dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu.
- Na trzech (10%) komputerach nie zainstalowano programu antywirusowego, a na kolejnym jego ostatnia aktualizacja miała miejsce ponad 16 miesięcy wcześniej. Działanie to było niezgodne z punktem 5 rozdziału 7.2 Instrukcji Zarządzania – RODO – Wykaz Zabezpieczeń RODO, który stanowił, że zastosowano system antywirusowy na serwerze i na stacjach roboczych. Jednocześnie było to niezgodne z § 20 ust. 2 pkt 7 i 9 rozporządzenia KRI, zgodnie z którymi kierownictwo podmiotu publicznego jest obowiązane do podejmowania działań zapewniających ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także zabezpieczenia przetwarzanych informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie. Dodatkowo, zgodnie z przepisem § 20 ust. 2 pkt 12 tego rozporządzenia, zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych polega w szczególności na dbałości o aktualizację oprogramowania, minimalizowaniu ryzyka utraty informacji w wyniku awarii oraz ochronie przed błędami, utratą, nieuprawnioną modyfikacją.
- W systemach operacyjnych dwóch (6,7%) komputerów znajdujących się w dyżurkach pielęgniarskich zalogowani byli użytkownicy, którzy w chwili oględzin byli już nieobecni w pracy (zakończyli swój dyżur). Działanie to było niezgodne z punktem 12 rozdziału 2 Regulaminu Ochrony Danych Osobowych, zgodnie z którym po zakończeniu pracy użytkownik zobowiązany jest wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy. Pracownicy wyjaśnili, że zapomnieli wylogować się wychodząc do domu.

(akta kontroli str. 1355-142, 228-234, 541-545, 573-576)

W trakcie kontroli dokonano stosownych zmian, eliminując nieprawidłowości dotyczące bezpieczeństwa danych gromadzonych w formie elektronicznej. (akta kontroli str. 566)

Dyrektor Szpitala wyjaśniła, że nie wiedziała o takich sytuacjach. IOD wyjaśnił, że sądził, że wszystkie komputery są właściwie zabezpieczone. Informatyk Szpitala wyjaśnił zaś, że: *(...) taki stan zastałem wraz z rozpoczęciem pracy w grudniu 2018 r. i nie wiedziałem, że niektóre z sytuacji stwierdzonych w trakcie kontroli miały miejsce. Spraw, które wymagają mojej interwencji w Szpitalu jest bardzo dużo, większość czasu zajmuje*

mi naprawianie bieżących usterek. Na pozostałe sprawy często nie wystarcza mi czasu. Stwierdzone w trakcie kontroli usterki usunąłem na bieżąco.

(akta kontroli str. 547-554, 556-557)

9. Pięciu z 24 pracowników administracyjnych korzystało z poczty elektronicznej w ogólnodostępnych serwisach internetowych, a nie w domenie wykupionej przez Szpital na profesjonalnym portalu świadczącym usługi tego typu. Nie zapewniono tym samym odpowiedniego bezpieczeństwa dla danych elektronicznych, o którym mowa w § 20 ust. 2 pkt 7 rozporządzenia KRI. Za pomocą adresów e-mailowych tych pracowników wysyłano m.in. sprawozdanie z działalności Szpitala do Starostwa Powiatowego, faktury do Działu Statystyki i Dokumentacji Medycznej, informowano oferentów o wyborze najkorzystniejszej oferty wybranej w przetargu, kontaktowano się w sprawach stażu i szkoleń. Nie stwierdzono wiadomości wysyłanych prywatnie. Pozostali pracownicy administracyjni posiadali właściwe adresy poczty elektronicznej. Informatyk Szpitala wyjaśnił, że taka sytuacja miała miejsce zanim rozpoczął pracę w Szpitalu. Informatyk zdawał sobie sprawę, że wymagało to zmiany, pozostawała kwestia historii korespondencji i bazy e-mailowej na tych zewnętrznych serwerach oraz posiadania przez kontrahentów Szpitala *starych* adresów e-mailowych. IOD wyjaśnił zaś, że w 2005 roku, zaczynając pracę w Szpitalu, założył adres e-mailowy dla siebie. Nie było wówczas informatyka w szpitalu, który zrobiłby to na jakimś oficjalnym serwerze pocztowym. Dodał: *(...) już zwróciłem się do informatyka o założenie oficjalnych adresów e-mailowych dla pracowników, którzy dzisiaj ich nie mają.*

(akta kontroli str. 375-376, 551-554, 556-557, 577)

10. Kopie zapasowe nie były właściwie przechowywane. Do 23 lutego 2019 r. Szpital nie posiadał oddzielnego serwera, zlokalizowanego w innym miejscu niż serwerownia główna – który miałby służyć do przechowania kopii zapasowych. Działanie to było niezgodne z § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI, zgodnie z którym zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych polega w szczególności na minimalizowaniu ryzyka utraty informacji w wyniku awarii. Kopie baz danych systemów informatycznych Szpitala były przechowywane w jednym pomieszczeniu z danymi produkcyjnymi i – jak stwierdzono w trakcie kontroli projektu *Podlaski System Informacyjny e-Zdrowie* – z przyczyn technicznych nie były przesyłane na macierze dyskowe Urzędu Marszałkowskiego Województwa Podlaskiego w Białymstoku. Pożar lub awaria macierzy dyskowych wiązać się mogły w tym przypadku z utratą również kopii zapasowych. Informatyk Szpitala wyjaśnił, że taki stan zastał wraz z rozpoczęciem pracy w grudniu 2018 r. (akta kontroli str. 556-561)

11. W pomieszczeniu serwerowni znajdowały się kartonowe opakowania po sprzęcie informatycznym. Były to materiały łatwopalne i serwerownia, z uwagi na prawdopodobieństwo wystąpienia przegrzania macierzy dyskowych lub przepięcia elektrycznego, nie powinna być miejscem do ich składowania. Informatyk Szpitala wyjaśnił, że nie wie, kto pozostawił te kartony w serwerowni. Dodał: *(...) dostęp do niej – oprócz mnie, mają też inni upoważnieni pracownicy. Gdy otrzymałem informację sugerującą ich uprzątnięcie, to zostały zutylizowane.* (akta kontroli str. 544, 556-557)

OCENA CZĄSTKOWA

Najwyższa Izba Kontroli ocenia negatywnie podjęte przez Szpital działania w celu zapewnienia prawidłowego przetwarzania i ochrony danych osobowych.

IV. Wnioski

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

Wnioski

1. Dokonywanie przeglądów i aktualizacji PBI oraz uregulowań dotyczących ochrony danych osobowych.
2. Przeprowadzanie szkoleń dotyczących ochrony danych osobowych oraz szkoleń uwzględniających zagadnienia z zakresu bezpieczeństwa informacji określone w § 20 ust. 2 pkt 6 rozporządzenia KRI dla wszystkich pracowników zaangażowanych w proces przetwarzania informacji.

3. Zwrócenie uwagi personelowi medycznemu na konieczność właściwej organizacji pracy w zakresie przechowywania dokumentacji medycznej, rozpoczynania i zawieszania pracy z systemami informatycznymi.
4. Zaopatrywanie opasek identyfikacyjnych pacjentów w znaki nieujawniające imion i nazwisk pacjentów osobom postronnym.
5. Zapewnienie dostępu pielęgniarkom i położnym do systemu typu HIS, w zakresie wynikającym z realizowanych przez nie zadań i obowiązków.
6. Niepodawanie w zgłoszeniach serwisowych danych osobowych i medycznych pacjentów.
7. Odebranie upoważnień do dostępu lub przetwarzania danych ze zbioru danych pacjenta dla salowych i sanitariuszy.
8. Regularne uzupełnianie rejestru naruszeń ochrony danych osobowych oraz incydentów zagrażających bezpieczeństwu danych.
9. Udostępnianie dokumentacji medycznej wyłącznie osobom upoważnionym przez pacjentów oraz weryfikowanie tożsamości osób, którym jest ona udostępniana.
10. Prowadzenie wykazu dotyczącego udostępnianej dokumentacji medycznej pacjentom, wymaganego art. 27 ust. 4 ustawy o prawach pacjenta
11. Utworzenie adresów e-mailowych, w domenie użytkowanej przez Szpital, osobom nieposiadającym takich adresów i zobowiązanie ich do zaprzestania użytkowania kont na serwisach komercyjnych.

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 Białymstoku. 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.

Białystok, 1 kwietnia 2019 r.

Kontroler:

Wojciech Zambrzycki
starszy inspektor kontroli państwowej

podpis

p.o. DYREKTORA DELEGATURY
Najwyższej Izby Kontroli w Białymstoku
z up. WICEDYREKTOR
Robert Skwarko

podpis