NAJWYŻSZA IZBA KONTROLI
Delegatura w Krakowie

LKR.410.002.03.2019

Pan Wojciech Szafrański
Prezes Zarządu
Szpital Specjalistyczny
im. L. Rydygiera sp. z o.o.
os. Złotej Jesieni 1
31-826 Kraków

WYSTĄPIENIE POKONTROLNE

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

NAJWYŻSZA IZBA KONTROLI
Delegatura w Krakowie
ul. Łobzowska 67, 30-038 Kraków
T +48 12 342 34 00, F +48 12 342 34 44
lkr@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Szpital Specjalistyczny im. L. Rydygiera sp. z o.o., os. Złotej Jesieni 1, 31-826 Kraków (*Szpital*)
Kierownik jednostki kontrolowanej	Wojciech Szafrański, Prezes Zarządu Szpitala, od 11 marca 2011 r. (akta kontroli str. 3, 7-13)
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; badania kontrolne mogły dotyczyć również 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 Krakowie
Kontrolerzy	1. Paweł Lipowski, specjalista kontroli państwowej, upoważnienie do kontroli nr LKR/38/2019 z 29 stycznia 2019 r. 2. Małgorzata Korusiewicz, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LKR/37/2019 z 29 stycznia 2019 r. (akta kontroli str. 1-2, 778-779)

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

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

W okresie objętym kontrolą w Szpitalu opracowano wymaganą dokumentację oraz procedury związane z ochroną przetwarzanych danych osobowych. Przyjęte rozwiązania techniczne i organizacyjne nie zapewniały jednak pełnej ochrony danych osobowych i nie eliminowały ryzyka nieuzasadnionego dostępu do danych przetwarzanych w systemach informatycznych Szpitala.

W Szpitalu w sposób prawidłowy sporządzono dokumentację związaną z ochroną danych osobowych, uwzględniającą 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 (tzw. ogólne rozporządzenie o ochronie danych)[3], w tym opracowano procedury wewnętrzne oraz dokonywano wymaganych przeglądów i aktualizacji opracowanej dokumentacji. W Szpitalu wyznaczono Inspektora Ochrony Danych (*IOD*) i poprzez przyjęte rozwiązania organizacyjne zagwarantowano mu status niezależności w sprawowaniu tej funkcji. W sposób prawidłowy prowadzono rejestr czynności przetwarzania danych osobowych, przeprowadzano analizy procesów przetwarzania danych osobowych, zawarto wymagane umowy powierzenia przetwarzania danych osobowych oraz udostępniano dokumentację medyczną pacjentów. Szpital dokonał jednego zgłoszenia do Prezesa Urzędu Ochrony Danych Osobowych (*UODO*) stwierdzonego naruszenia ochrony danych osobowych; należycie dokumentowano pozostałe naruszenia ochrony takich danych (niewymagające zgłoszenia). W Szpitalu podejmowano właściwe działania w celu minimalizacji ryzyka utraty danych osobowych w wyniku awarii, błędów lub nieuprawnionej modyfikacji; w trakcie kontroli nie stwierdzono przypadków ujawnienia i przekazywania takich danych podmiotom zewnętrznym w ramach procesu zgłaszania błędu/awarii oprogramowania, a także osobom lub podmiotom nieuprawnionym.

W trakcie kontroli stwierdzono jednak następujące nieprawidłowości:

- Szpital nie przesłał w terminie do Prezesa UODO informacji o powołaniu IOD;
- nie zorganizowano szkoleń związanych z wejściem w życie przepisów RODO w tym dotyczących bezpieczeństwa danych dla całego personelu Szpitala uczestniczącego w procesie przetwarzania danych osobowych;
- umożliwiono personelowi administracyjnemu – nieuzasadniony wykonywanym zakresem obowiązków – dostęp do danych medycznych: dwoje pracowników administracji (z kontrolowanych 30 osób) posiadało pełny dostęp do systemu *„Hospital Information System" („HIS")*[4], tj. do wszystkich informacji z oddziałów, na których komercyjnie leczono pacjentów;
- w systemie „HIS" dwie, z kontrolowanych 39 osób będących personelem medycznym, posiadały uprawnienia do więcej niż jednej poradni i oddziału o różnej specjalizacji medycznej;
- do systemu „HIS", z kontrolowanych 30 osób, uprawnienia dostępu posiadały dwie osoby, które przestały być pracownikami Szpitala po 25 maja 2018 r. (tj. dacie wejścia w życie RODO), a powodów dla utrzymywania praw dostępu w trakcie oględzin nie znali pracownicy odpowiedzialni za funkcjonowanie systemu „HIS", przy czym w Szpitalu w trakcie kontroli wdrażano nową

[2] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej. W niniejszym wystąpieniu zastosowano ocenę opisową.

[3] Dz. Urz. UE L 119 z 4 maja 2016 r., str. 1; dalej: *RODO*.

[4] System informatyczny do obsługi Szpitala, którego głównym zadaniem była obsługa pacjenta w poradniach i na oddziałach (poza podstawową opieką zdrowotną) oraz tworzenie elektronicznej dokumentacji medycznej.

procedurę zmierzającą do poprawy przepływu komunikacji pomiędzy komórkami organizacyjnymi odpowiedzialnymi za ten zakres działalności;
- brak aktualizacji baz sygnatur wirusów stwierdzony na dziewięciu (z kontrolowanych 30) komputerach pracowników oraz stosowanie w Szpitalu oprogramowania antywirusowego, pomimo zapisów rezolucji Nr A8-0189/2018 Parlamentu Europejskiego poświęconej cyberbezpieczeństwu;
- wykorzystywanie w Szpitalu systemu operacyjnego, dla którego wsparcie techniczne ze strony producenta zakończyło się pięć lat temu;
- w 11 z 30 badanych przypadków, do systemów operacyjnych komputerów personel Szpitala logował się przy jednoczesnym użyciu tych samych: loginu i hasła; przy czym stwierdzono także praktykę stosowania tego samego loginu przez personel medyczny na różnych oddziałach, różną złożoność haseł oraz stosowanie loginów w postaci ciągu cyfr.

W ocenie NIK zagrożenia, dla bezpieczeństwa infrastruktury informatycznej Szpitala, które może skutkować nieprawidłowościami w przyszłości (jeżeli Szpital nie podejmie odpowiednich działań) z uwagi na ochronę danych osobowych pacjentów, przewidzianą w przepisach RODO oraz zakres obowiązków personelu medycznego w ramach prowadzenia dokumentacji medycznej, wynikający z opisów ich stanowisk pracy, stanowić mogą:

- braku dostępu do systemu „HIS" dla sześciu z 39 kontrolowanych pielęgniarek oraz braku logowania się do systemu „HIS" przez trzy kontrolowane pielęgniarki w ciągu ponad czterech lat (które przestały być z dniem 25 maja 2018 r. pracownikami Szpitala);
- braku założonego konta w systemie „HIS" dla pięciu kontrolowanych osób wykonujących zawód medyczny, w tym rejestratorek medycznych, które przestały być pracownikami Szpitala po 25 maja 2018 r.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[5] kontrolowanej działalności

OBSZAR

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

Opis stanu faktycznego

1.1. W dniu 11 maja 2018 r. Prezes Zarządu jako Administrator Danych Osobowych (*ADO*) wyznaczył IOD, działając na podstawie przepisów RODO. IOD nie pełnił wcześniej funkcji administratora bezpieczeństwa informacji.

Stanowisko IOD zostało wyodrębnione w Dziale Informatyki (*IT*); jego zadania określono w zakresie czynności IOD[6]. Na podstawie tych regulacji IOD w sprawowaniu swojej funkcji podlegał bezpośrednio Prezesowi Zarządu (*ADO*). Osoba pełniąca funkcje IOD na dzień 11 maja 2018 r. świadczyła usługi na podstawie umowy cywilnoprawnej, a od 20 czerwca 2018 r. pracowała w wymiarze pełnego etatu na stanowisku „administrator aplikacji i systemów bazodanowych". W okresie od marca 2018 r. do stycznia 2019 r. osoba ta – w ramach podnoszenia kompetencji, ukończyła trzy szkolenia związane z ochroną danych osobowych.

Prezes Zarządu wskazał, że IOD *zapewniono możliwość wypełniania obowiązków w sposób niezależny, a powierzenie innych obowiązków nie powodowało konfliktu interesów.*

[5] 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.

[6] Na podstawie zmiany regulaminu organizacyjnego Szpitala z dnia 23 maja 2018 r. (przewidującego odrębne zarządzenie określające obowiązki IOD). Zakres czynności IOD pochodził z 20 czerwca 2018 r.

Na podstawie art. 37 ust. 7 RODO dane IOD oraz sposób i formę kontaktu z nim udostępniono na stronie internetowej Szpitala[7]. Ponadto w zakładce „RODO" na tej stronie umieszczono informacje dla pacjentów o przetwarzaniu ich danych osobowych w celu udzielania świadczeń opieki zdrowotnej (także dla osób upoważnionych do odbioru wyników badań oraz osób korzystających ze szpitalnych pokoi hotelowych – w celu świadczenia takich usług). Informacje takie znajdowały się również na terenie Szpitala.

Teren Szpitala został oznaczony znakami graficznymi informującymi, że obiekt jest monitorowany. Przy każdym z wejść do budynku Szpitala znajdowała się pisemna informacja dotycząca danych monitoringu wizyjnego (dla celów ochrony osób i mienia oraz realizacji nadzoru medycznego), w rozumieniu art. 13 RODO.

(akta kontroli str. 4, 5-6, 14-132, 590-591, 592-600, 717-718, 719-720)

W grudniu 2018 r. Szpital otrzymał zawiadomienie o zakończeniu postępowania administracyjnego w sprawie uznania go za operatora usługi kluczowej (w zakresie udzielania świadczeń opieki zdrowotnej oraz obrotu i dystrybucji produktów leczniczych)[8]. Do dnia zakończenia kontroli Szpital nie otrzymał decyzji w tej sprawie; w związku z powyższym nie powołano wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo (których członkiem powinien być IOD). Prezes Zarządu wyjaśnił, że *Szpital powoła wymagane struktury w wyznaczonym terminie, po otrzymaniu decyzji w sprawie uznania go za operatora usługi kluczowej.*

(akta kontroli str. 508-509, 510-511, 590-591, 592-593, 601-604)

1.2. Szpital na dzień 25 maja 2018 r. posiadał aktualną (uwzględniającą przepisy RODO oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[9]), dokumentację wewnętrzną.

W Szpitalu w październiku 2018 r. opracowano kolejną „Politykę Bezpieczeństwa Informacji" (*PBI*) regulującą ochronę danych osobowych. Dokumentacja ta została zatwierdzona przez Prezesa Zarządu oraz przedstawiona do zapoznania się i stosowania pracownikom poprzez jej zamieszczenie w Intranecie – zakładka „Jakość i zarządzanie". Dokumentacja ta była dostępna dla wszystkich pracowników, jako kolejna aktualizacja dokumentu akredytacyjnego, obowiązującego w obszarze zarządzania informacjami z lat 2010-2014[10].

PBI określała m.in. zadania: koordynatora systemu zarządzania bezpieczeństwem informacji (IOD) oraz administratorów systemów informatycznych (*ASI*)[11], stosowane zabezpieczenia: organizacyjne, ochrony fizycznej danych osobowych oraz sprzętowe: infrastruktury informatycznej, telekomunikacyjnej i oprogramowania oraz postępowanie w przypadku zagrożeń bezpieczeństwa danych osobowych.

W formie załączników do PBI określono m.in. regulaminy: korzystania z komputerów przenośnych oraz z oprogramowania, sprzętu komputerowego i sieciowego, instrukcję zarządzania systemem informatycznym (służącym do przetwarzania danych osobowych), metrykę haseł (określająca sposób tworzenia haseł do systemów informatycznych) oraz rejestr nośników komputerowych zawierających

[7] http://www.szpitalrydygier.pl.

[8] Na podstawie art. 5 ust. 2, art. 41 pkt 5 oraz 42 ust. 1 pkt 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560).

[9] Dz. U. poz. 1000 ze zm.; dalej: ustawa o ochronie danych osobowych.

[10] W ramach działalności medycznej w maju 2009 r. Szpital otrzymał (po raz pierwszy) certyfikat systemu zarządzania jakością według normy ISO 9001:2015 (aktualny jest ważny do marca 2021 r.), natomiast w październiku 2014 r. (po raz pierwszy) certyfikaty systemu zarządzania bezpieczeństwem informacji według norm ISO/IEC 27001:2013 oraz systemu zarządzania środowiskowego według norm ISO 14001:2015 (aktualne są ważne do października 2020 r.). W grudniu 2017 r. Szpital otrzymał certyfikat potwierdzający spełnienie standardów akredytacyjnych Ministra Zdrowia dla lecznictwa szpitalnego (po raz pierwszy w 2010 r.).

[11] W okresie objętym kontrolą funkcję ASI pełniło siedem osób.

dane osobowe. Wprowadzono również wzór oświadczenia pracowników o zapoznaniu się z treścią PBI.

Za nadzór nad przestrzeganiem przez personel obowiązku zapoznania się z ww. procedurami oraz złożenia podpisu na oświadczeniach to potwierdzających, odpowiedzialność ponosili kierownicy komórek organizacyjnych Szpitala (w tym ordynatorzy i pielęgniarki oddziałowe). Podpisane oświadczenia przechowywane były w komórkach organizacyjnych.

Prezes Zarządu wskazał, że pracownicy nie mieli dostępu do dokumentów tworzących politykę ochrony danych osobowych, których ujawnienie mogłoby stanowić zagrożenie przetwarzania danych i/lub ich ujawnienie (pracownicy mieli dostęp jedynie do pustych, tj. nieuzupełnionych szablonów). Dodał, że do takich dokumentów należały, np. polityka tworzenia kopii zapasowych oraz baza danych haseł.

Postanowienia PBI obejmowały ochronę danych osobowych pracowników oraz pacjentów. Akty prawne przywołane w opracowanej dokumentacji odnosiły się do stanu prawnego z okresu jej przygotowania.

Prezes Zarządu wskazał, że w latach 2018-2019 dokonano aktualizacji procedur systemowych wynikających z wypełniania norm ISO: 27001 i 9001 oraz akredytacji Ministra Zdrowia (procedury systemu zarządzania bezpieczeństwem informacji). Dotyczyło to (aktualizowanych w czerwcu 2018 r.), m.in. analizy ryzyka bezpieczeństwa informacji, przeprowadzania testów akceptacyjnych „*HIS*", a także zarządzania: incydentami bezpieczeństwa informacji, uprawnieniami, kluczami do pomieszczeń, zmianami w systemach informatycznych oraz ogólnych zasad bezpieczeństwa informacji.

Ponadto w maju 2018 r. Szpital wprowadził procedurę zarządzania wnioskami osób, których dane przetwarzano w Szpitalu. W styczniu 2019 r. wprowadzono nową procedurę zarządzania monitoringiem wizyjnym oraz zaktualizowano zasady zakładania kont użytkowników w dwóch programach komputerowych (do obsługi: badań laboratoryjnych oraz finansowo-księgowej) oraz w Intranecie, zasady zakładania kont pocztowych oraz przyznawania dostępu do zasobów internetowych.

(akta kontroli str. 133-296, 312-316, 590-593, 605-606, 717-720, 770-773)

W Szpitalu opracowano procedury i dokumentację wynikającą z regulacji wewnętrznych dotyczących ochrony danych osobowych, tj.: procedury dotyczące: nadawania i wycofywania uprawnień do przetwarzania danych osobowych[12]; nadawania uprawnień w systemach informatycznych[13]; zarządzania dostępem zdalnym oraz zarządzania dostępem fizycznym do pomieszczeń[14].

Ponadto wdrożono plany awaryjne („plany ciągłości działania"), obejmujące siedem obszarów, w tym m.in. ryzyko braku dostępu do sieci komputerowej, oprogramowania i danych oraz braku nadzoru nad osobami trzecimi. Plany te podlegały testowaniu (w 2018 r. odbyło się osiem testów, dotyczących m.in. sprzętu komputerowego).

Odnosząc się do dokonania przeglądów i aktualizacji tej dokumentacji Prezes Zarządu wskazał, że:

– dostosowano do wymogów RODO formularze upoważnienia do przetwarzania danych;

[12] Procedura zarządzania zasobami ludzkimi, zakładająca ewidencjonowanie wydawanych upoważnień.

[13] Procedura zarządzania uprawnieniami.

[14] Procedura zarządzania kluczami do pomieszczeń

– podpisano nowe lub zaktualizowano umowy dotyczące powierzenia przetwarzania danych (w których Szpital występował jako administrator danych lub jako podmiot przetwarzający);
– przygotowano i opublikowano informacje dla osób, od których zbierane są dane osobowe oraz formularze dla osób zgłaszających żądania związane z przetwarzaniem swoich danych osobowych;
– przeprowadzono okresową analizę ryzyka i sporządzono plan postępowania z ryzykiem;
– na dzień wejścia w życie RODO przeprowadzono audyt wewnętrzny stanu przygotowania do spełnienia wymagań („*analizę stanu zgodności PBI, środków i rozwiązań organizacyjnych stosowanych w Szpitalu z wymaganiami określonymi w RODO*"). Audyt ten odnosił się do 21 obszarów funkcjonowania Szpitala. W 20 z nich stwierdzono stopień zgodności na „spełnianie wymagań", a niespełnianie wymagań dotyczyło powierzenia przetwarzania danych osobowych. Stwierdzono konieczność podpisania nowych umów powierzenia przetwarzania danych osobowych (zidentyfikowano 104 przypadki wymagające zawarcia umowy powierzenia danych, w tym sześć nieprzygotowanych umów, 81 umów w trakcie zatwierdzania, podpisywania lub negocjacji oraz 17 podpisanych umów).

(akta kontroli str. 133-137, 590-593, 607-614, 615-637, 770-771, 772, 774-775)

1.3. W Szpitalu od 25 maja 2018 r. prowadzono rejestr czynności przetwarzania danych osobowych zawierający elementy określone w art. 30 RODO. Rejestr ten prowadzono w formie elektronicznej oraz pisemnej.

Rejestr ten określał 12 kategorii przetwarzania danych, w tym m.in. dane osobowe pacjentów, osób upoważnionych i opiekunów prawnych oraz dane medyczne; dane kontaktowe osób fizycznych wykonujących badania naukowe; dane personalne osób upoważnionych lub opiekunów prawnych i dane medyczne oraz dane osobowe osób rejestrujących się w „e-rejestracji".

Rejestr czynności przetwarzania zawierał wszystkie informacje wymagane art. 30 RODO, tj. określał: cel przetwarzania danych (np. wykonywanie świadczeń opieki zdrowotnej); podstawę prawną przetwarzania danych[15]; opis kategorii osób, których dane dotyczą (np. pacjenci); kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione (np. Narodowy Fundusz Zdrowia; *NFZ*) oraz planowane terminy usunięcia poszczególnych kategorii danych[16].

Rejestr ten nie przewidywał sytuacji przekazania jakiejkolwiek kategorii danych osobowych do państwa trzeciego lub organizacji międzynarodowej. W zakresie opisu technicznych i organizacyjnych środków bezpieczeństwa odsyłał do PBI (w tym do regulaminu korzystania z komputerów, instrukcji zarządzania systemem informatycznym oraz ogólnych zasad bezpieczeństwa informacji, procedur zarządzania: kluczami do pomieszczeń, dostępem zdalnym oraz uprawnieniami).

W ramach opisu ogólnych środków bezpieczeństwa rejestr wskazywał m.in. na ochronę dostępu do pomieszczeń (np. szafy zamykane, sejfy), systemy alarmowe, systemy *backupu* (tworzenia kopii zapasowych), zapasowe (nadmiarowe) łącza sieciowe, *firewalle* (zabezpieczenia styku sieci LAN/WAN), wygaszacze ekranów

[15] M.in. rozporządzenie Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz. U. poz. 2069) oraz ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2017 r. poz. 1318 ze zm.); dalej: *ustawa o prawach pacjenta*.

[16] Np. 10 lat dla danych kontaktowych właścicieli samochodów od czasu zakończenia korzystania z abonamentu parkingowego, pięć lat dla danych kontaktowych pracowników od daty rozwiązania z nimi stosunku pracy, rok od daty nagrania rozmowy telefonicznej z osobą zgłaszającą zdarzenie medyczne, 10 lat od zakończenia pobytu w szpitalnym pokoju hotelowym oraz 30 dni od daty zapisu obrazu (w tym dla realizacji nadzoru medycznego).

komputerowych zabezpieczone hasłem, zablokowane porty USB (przez program antywirusowy) oraz szkolenia personelu.

Rejestr zawierał imię i nazwisko ADO oraz IOD oraz ich dane kontaktowe. Osobą odpowiedzialną za prowadzanie rejestru był IOD.

(akta kontroli str. 297-311, 321-322, 590-591, 592-593, 770-771, 777)

1.4. Przed wejściem w życie przepisów RODO w Szpitalu, w marcu 2018 r., powołano zespół ds. wdrożenia RODO (systemu ochrony danych osobowych zgodnego z RODO), który w tym samym miesiącu dokonał audytu procesów przetwarzania we wszystkich komórkach organizacyjnych i tym samym wywiązał się z obowiązku wskazanego w art. 32 RODO. Prezes Zarządu wskazał, że na podstawie zebranych danych, zespół analizował istotność i ryzyka związane z każdą kategorią przetwarzania danych. Dodał, że *Zespół uwzględnił wszystkie zgłoszone przez komórki organizacyjne kategorie procesów przetwarzań danych. W wyniku analizy przygotowano zestawienie, które następnie stanowiło podstawę do stworzenia rejestru czynności przetwarzania.*

Prezes Zarządu wskazał, że w Szpitalu od 2014 r. prowadzono sformalizowaną, systematyczną analizę procesów (przetwarzania danych), monitorując stopień skuteczności stosowanych zabezpieczeń, zgodnie z zasadami określonymi we wdrożonym systemie bezpieczeństwa informacji, zgodnym z wymaganiami normy ISO 27001. Dodał, że *wszystkie dotychczasowe audyty kończyły się uzyskaniem pozytywnych decyzji certyfikacyjnych (potwierdzających zgodność funkcjonowania systemu z wymaganiami norm i przepisów prawa).* Wyjaśnił również, że w Szpitalu prowadzono analizę ryzyka obejmującą procesy przetwarzania danych osobowych, zgodnie z wymaganiami normy ISO 27001. Ostatnią taką analizę przeprowadzono w październiku 2018 r. zgodnie z procedurą analizy ryzyka bezpieczeństwa informacji. Dla istotnych zidentyfikowanych ryzyk opracowywano plan postępowania z ryzykiem.

(akta kontroli str. 133-137, 508-521, 590-593, 638-648, 651)

Arkusz szacowania ryzyka bezpieczeństwa informacji (stanowiący analizę ryzyka przetwarzania danych osobowych) z października 2018 r. wskazywał na 98 rozpoznanych zagrożeń. Dla 13 z nich określono nieakceptowalny poziom ryzyka (m.in. dla braku właściwego nadzoru nad czasem przetwarzania dokumentacji w formie papierowej, możliwości celowego lub przypadkowego zabrania dokumentacji innej osoby oraz ryzyka ujawnienia haseł i kodów dostępów z powodu ich częstej zmiany). Na tej podstawie opracowano plan postępowania z ryzykiem bezpieczeństwa informacji. W planie tym założono dla ww. ryzyk realizację działań korygujących (np. stopniowe przechodzenie na dokumentację elektroniczną, szkolenia z bezpieczeństwa informacji), w okresie od kwietnia 2019 r. do czerwca 2020 r. lub sukcesywnie w ramach prowadzonych inwestycji[17].

Prowadzone działania naprawcze były dokumentowane. Określono wykaz zasobów podlegających ocenie skuteczności zabezpieczeń, osoby odpowiedzialne oraz częstotliwość prowadzenia oceny.

(akta kontroli str. 133-134, 135-137, 317-320, 323-331, 332-333)

1.5. W Szpitalu nie wykonano (fakultatywnej) oceny skutków dla ochrony danych, o której mowa w art. 35 RODO. Prezes Zarządu wskazał, że w okresie od 25 maja 2018 r., *nie wystąpiły zdarzenia wymagające dokonania oceny skutków dla ochrony danych (zgodnie z art. 35 RODO), ponieważ zakres i rodzaj przetwarzania danych nie uległy zmianie, a ponadto Szpital przetwarza dane szczególne (dokumentację medyczną) na podstawie wymagań prawnych, co stanowi*

[17] Dotyczyło to czterech działań dotyczących wymiany zamków kodowych i mechanicznych oraz instalacji nowych kamer.

wyłączenie zgodnie z art. 35 ust. 10 RODO. Dodał, że *zakres przetwarzanych w Szpitalu danych osobowych (danych medycznych związanych z udzielaniem świadczeń medycznych) nie jest wymieniony w wykazie rodzajów operacji przetwarzania wymagających oceny skutków przetwarzania, opublikowanym przez Prezesa UODO*[18].

Przy czym Prezes Zarządu wyjaśnił, że jednym z zadań powołanego zespołu ds. wdrożenia RODO była analiza wszystkich występujących w Szpitalu procesów przetwarzania danych. Na podstawie zebranych danych, zespół analizował istotność i ryzyka związane z każdą kategorią przetwarzania danych, podczas prowadzonych cyklicznie zebrań.

Dodał także, że w *Szpitalu prowadzi się regularnie analizę ryzyka obejmującą procesy przetwarzania danych osobowych zgodnie z wymaganiami normy ISO 27001*. *Szacowanie to pozwala na określenie listy procesów zachodzących w Szpitalu a związanych z przetwarzaniem danych osobowych oraz ich skutków.* Wskazał także na szacowanie ryzyka, które miało miejsce w maju 2018 r., ww. identyfikację (w październiku 2018 r.) obszarów ryzyka bezpieczeństwa informacji, oraz opracowany plan postępowania z ryzykiem.

(akta kontroli str. 334-335, 336-338)

1.6. W Szpitalu według stanu na 25 maja 2018 r. zatrudnionych (ogółem) było 1 384 osoby, dodatkowo 139 osób wykonywało pracę na podstawie umów cywilnoprawnych. W związku z wejściem przepisów RODO w Szpitalu zorganizowano szkolenia wewnętrzne prowadzone przez IOD. Szkolenia te odbyły się w okresie od marca do lipca 2018 r., w tym – przed wejściem w życie RODO – w maju 2018 r. przeprowadzono tygodniowy cykl (codziennych) szkoleń adresowanych dla personelu Szpitala (także pracowników Zakładu Opieki Długoterminowej w Makowie Podhalańskim, znajdującego się w strukturach Szpitala). Ogółem przeszkolono 751 osób (49%)[19].

Tematyka szkoleń dotyczyła m.in. ochrony danych osobowych, w tym przepisów prawnych oraz zmian w PBI wynikających z RODO. Dodatkowo w lipcu 2018 r. dla wybranych (2-3) osób z każdej komórki organizacyjnej (łącznie 64 osoby) zorganizowano szkolenie przeprowadzone przez firmę zewnętrzną z zakresu bezpieczeństwa informacji, w tym ochrony danych osobowych. Tym samym, według stanu na koniec lipca 2018 r., szkoleniami objęto łącznie 815 osób (59%).

Poza ww. szkoleniami w Szpitalu przyjęto plany szkoleń wewnętrznych na 2018 r. i 2019 r. Plan szkoleń wewnętrznych na 2019 r. zakładał m.in. szkolenie z zakresu cyberbezpieczeństwa oraz szkolenie uzupełniające z bezpieczeństwa informacji.

(akta kontroli str. 334-395, 590-593, 638-648, 649-654, 657-658, 717-720)

1.7. Odnosząc się do stosowania w Szpitalu kodeksu dobrych praktyk lub medycznego kodeksu branżowego Prezes Zarządu wyjaśnił, że działania ww. zespołu ds. wdrożenia RODO oparte były na wytycznych RODO oraz projekcie „Kodeksu postępowania dla sektora ochrony zdrowia" (wersji nr 12 z 13 marca 2018 r.). Pomimo złożonego projektu ostatecznie Kodeks ten nie został zatwierdzony przez UODO i nie został oficjalnie wdrożony w Szpitalu.

Dodał, że *w zakresie ochrony danych osobowych Szpital w swojej działalności kieruje się wytycznymi wdrożonego systemu zarządzania bezpieczeństwem informacji ISO 27001, ustawą o ochronie danych osobowych oraz systemem*

[18] 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).

[19] Szkoleniami – według list obecności (stanowiącymi przyjęty sposób potwierdzenia udziału pracownika w szkoleniu wewnętrznym) objęto: kadrę zarządzającą, lekarzy, pielęgniarki i położne, rejestratorki oraz inny personel medyczny, a także pracowników działów administracyjnych (w tym informatyków).

akredytacji szpitali MZ. Wytyczne przyjęte w Szpitalu w momencie wdrożenia ww. systemów jakości (ISO, akredytacja) były zgodne z zasadami określonymi w „Przewodniku po RODO w służbie zdrowia" z 24 września 2018 r.[20]. Jedynie w zakresie wzywania pacjentów do gabinetów lekarskich zwiększono anonimowość pacjenta (ustalono zasadę wzywania pacjenta posługując się jego imieniem, a w przypadku, gdy w kolejce oczekujących jest więcej niż jedna osoba o danym imieniu, dodatkowo wskazując godzinę wizyty – zmiany wprowadzono z dniem 25 maja 2018 r.).

Wyjaśnił przy tym, że *Szpital przygotowując się do procesu wdrożenia RODO opierał swoje działania również na innych materiałach opracowanych i zatwierdzonych przez kompetentne organy („Wskazówki Prezesa UODO dotyczące wykorzystywania monitoringu wizyjnego*" z lipca 2018 r., inne dokumenty i informacje publikowane na portalach: uodo.gov.pl oraz csioz.gov.pl). Dodał, że *stosowanie zatwierdzonych i opublikowanych Kodeksów postępowania wynika z przepisów RODO i Szpital zastosuje się do wymagań Kodeksu postępowania dla podmiotów medycznych niezwłocznie, gdy tylko zostanie on zatwierdzony i opublikowany (…) Szpital stosował ww. dokumenty jako istotną pomoc w procesie wdrożenia i będzie stosował wszelkie kodeksy i poradniki przygotowane przez kompetentne organy.*

(akta kontroli str. 334-335, 336-338, 396-405)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w zakresie opracowania wymaganej dokumentacji oraz procedur związanych z ochroną przetwarzanych danych osobowych stwierdzono następujące nieprawidłowości:

1. Szpital nieterminowo zgłosił fakt powołania IOD do UODO.

   IOD w Szpitalu został powołany 11 maja 2018 r. Informację o jego powołaniu przekazano do UODO w postaci papierowej 26 czerwca 2018 r., tj. po 32 dniach po terminie określonym w art. 10 ustawy o ochronie danych osobowych.

   W dniu 8 października 2018 r. do Szpitala wpłynęło pismo Prezesa UODO, w którym zwrócił się o dokonanie zgłoszenia w wymaganej, elektronicznej formie. Zgłoszenia takiego Szpital dokonał 15 października 2018 r., tj. po upływie prawie pięciu miesięcy od daty wejścia w życie ustawy o ochronie danych osobowych.

   IOD wyjaśnił, że opóźnienie związane z powiadomieniem Prezesa UODO spowodowane było problemem technicznym związanym z niemożliwością dokonania prawidłowego zgłoszenia.

   (akta kontroli str. 590-591, 592-600)

2. Nieobjęcie 41% zatrudnionych pracowników Szpitala zajmujących się przetwarzaniem danych osobowych pacjentów szkoleniami z zakresu bezpieczeństwa danych w związku z wejściem w życie RODO.

   Według stanu na koniec lipca 2018 r. szkoleniami w zorganizowanej formie objęto 815 wszystkich osób zatrudnionych w Szpitalu (59%).
   Dyrektor ds. Infrastruktury i Techniki Medycznej wyjaśniła, że dodatkowo pracownicy uczestniczą *przynajmniej raz w roku w szkoleniu prowadzonym przez firmę zewnętrzną dotyczącym szeroko rozumianego bezpieczeństwa informacji, w tym z zakresu bezpieczeństwa danych osobowych*. Średnio w szkoleniu uczestniczy ok. 60 osób, co najmniej dwie osoby z każdej komórki organizacyjnej (szkolenie na 2019 r. zaplanowano na drugą połowę roku). Dodała, że *każdy pracownik przy odbieraniu upoważnienia do przetwarzania danych osobowych przechodzi stosowne szkolenie prowadzone przez IOD.*

[20] W ramach kontroli przedłożono „Przewodnik po RODO dla służby zdrowia", który został opublikowany 24 września 2018 r. na stronie Ministerstwa Cyfryzacji.

(akta kontroli str. 334-395, 590-593, 638-648, 649-654, 657-658, 717-720)

Nieobjęcie szkoleniami wszystkich pracowników przed wejściem w życie przepisów RODO, tj. przed 25 maja 2018 r., NIK traktuje jako nieprawidłowość z uwagi na 25. miesięczne *vacatio legis* dla tego rozporządzenia. Tak długi okres czasu umożliwiał przeszkolenie wszystkich pracowników uczestniczących w procesach przetwarzania danych odpowiednio wcześniej.

(akta kontroli str. 334-395, 590-593, 638-648, 649-654, 657-658, 717-720)

OCENA CZĄSTKOWA

Szpital wywiązał się z obowiązku opracowania dokumentacji oraz procedur uwzględniających przepisy RODO. Wyznaczono IOD, właściwie i terminowo opracowano i prowadzono rejestr czynności przetwarzania danych osobowych, który zawierał wszystkie wymagane elementy, przeprowadzono analizę procesów przetwarzania danych osobowych oraz rzetelnie dokonano oceny stopnia ich bezpieczeństwa w stwierdzonych ryzykach. Stwierdzono jednak nieprawidłowości polegające na:

- niezgłoszeniu w terminie faktu powołania IOD do Prezesa UODO;
- nieprzeszkoleniu 41% pracowników uczestniczących w przetwarzaniu danych osobowych szkoleniami związanymi z wejściem w życie RODO oraz zagadnieniami dotyczącymi bezpieczeństwa danych.

Zdaniem NIK za ryzyko dla bezpieczeństwa w zakresie ochrony danych, które może skutkować nieprawidłowościami w przyszłości (jeżeli Szpital nie podejmie odpowiednich działań) należy uznać objęcie 59% pracowników Szpitala szkoleniami związanymi z obowiązywaniem przepisów z zakresu ochrony danych osobowych, w tym RODO w dacie wejścia w życie tych przepisów. Osiągnięty wskaźnik przeszkolonych pracowników, zdaniem NIK, należy uznać za niesatysfakcjonujący z punktu widzenia zadań IOD określonych w art. 39 ust. 1 lit. b) RODO. Cykliczny system szkoleń z zakresu ochrony danych osobowych, w tym RODO dla personelu medycznego Szpitala, w szczególności tzw. szkoleń przypominających, sprzyjać będzie minimalizacji ryzyk dla bezpiecznego przetwarzania ww. danych.

OBSZAR

2. Zapewnienie prawidłowego przetwarzania i ochrony danych osobowych

Opis stanu faktycznego

2.1. W wyniku oględzin wybranych w sposób losowy trzech oddziałów Szpitala[21], stwierdzono, że:

- na żadnym z łóżek w salach chorych nie było kart pacjentów z ich danymi osobowymi i/lub medycznymi;
- wszyscy pacjenci (przyjęci na oddział) posiadali opaski na nadgarstkach jedynie z wydrukowanymi kodami kreskowymi oraz numerem księgi głównej;
- nie stwierdzono pozostawiania kluczy w drzwiach pomieszczeń oddziałów;
- na kontrolowanych oddziałach w różnym zakresie stosowano monitoring wizyjny, który nie naruszał praw pacjentów (np. poprzez takie jego umiejscowienie, że kamery mogłyby rejestrować dokumentację medyczną);
- przed wejściem na oddziały oraz na teren dyżurek lekarskich (i pielęgniarskich – poza oddziałem internistycznym) zastosowano system kontroli dostępu (konieczny kod do zamka szyfrowego);
- w przypadku dyżurek pielęgniarskich:
  - były one zamykane na zwykły klucz (jedna dyżurka) lub na zamek elektroniczny (z kodami dostępu; dwie dyżurki);

[21] Oddział (Kliniczny) Chirurgii Szczękowo-Twarzowej, Oddział Chirurgii Ogólnej i Onkologicznej oraz Oddział Chorób Wewnętrznych.

- ruch chorych prowadzony był za pomocą list z nazwiskiem (imieniem) pacjenta i wskazaniem sali, na której przebywał (oraz danymi lekarza prowadzącego) – w sposób niewidoczny dla pacjentów oddziałów;
- dane osobowe i medyczne przechowywane były w zamykanych szafach;

– w dyżurkach lekarskich:
  - dane osobowe i medyczne przechowywane były w zamykanych skrzyniach/szafach na dokumenty lub w biurkach;
  - lekarze w trakcie oględzin korzystali z systemu „HIS".

W trakcie oględzin nie stwierdzono przypadków nie blokowania komputera po zakończeniu na nim pracy przez personel medyczny oraz ustawienia monitorów w sposób umożliwiający wgląd w ekran pacjentom.

(akta kontroli str. 579-584, 780)

W wyniku oględzin sposobu rejestrowania pacjentów do poradni szpitalnych ustalono, co następuje:

– rejestracja nr 1 (budynek główny Szpitala)[22]:
  - rejestracja prowadzona była przy ośmiu stanowiskach (jedno przeznaczone było dla osoby stojącej);
  - stanowiska były odpowiednio od siebie oddzielone uniemożliwiając usłyszenie danych osobowych lub wgląd w dokumenty, w tym w dokumentację medyczną osoby obsługiwanej na sąsiednim stanowisku (zastosowano w tym zakresie szyby mleczne);
  - nie wprowadzono oznaczeń, które sprzyjałyby zapewnieniu odstępu pomiędzy osobą obsługiwaną przy stanowisku a pacjentami oczekującymi w kolejce do rejestracji;
  - kolejność obsługi (podejścia) pacjenta do rejestracji ustalana była na podstawie bloczków pobieranych z automatu;

– rejestracja nr 2 (budynek poradni szpitalnych)[23]:
  - rejestracja prowadzona była przy pięciu okienkach, wszystkie dla osób stojących (wyodrębniono osobne okienko dla tzw. szybkiej terapii onkologicznej);
  - okienka nie były od siebie technicznie oddzielone, co mogło umożliwiać usłyszenie danych osobowych lub wgląd w dokumenty, w tym w dokumentację medyczną osoby obsługiwanej na sąsiednim stanowisku;
  - nie wprowadzono oznaczeń, które sprzyjałyby zapewnieniu odstępu pomiędzy osobą obsługiwaną przy stanowisku a pacjentami oczekującymi w kolejce do rejestracji;
  - kolejność obsługi (podejścia) pacjenta do okienka rejestracji ustalana była na podstawie kolejności przyjścia pacjentów do rejestracji.

W trakcie kontroli w przypadku obu rejestracji naklejono linie na podłodze mające na celu zachowanie odstępu pomiędzy osobą obsługiwaną a osobami oczekującymi. Prezes Zarządu wskazał ponadto, że w przypadku rejestracji nr 2, Szpital *planuje przebudowę rejestracji w budynku poradni, co zmieni całkowicie sposób rejestrowania się pacjentów i umożliwi w pełni spełnienie wymagań.*

W przypadku obu rejestracji:

[22] Do poradni: ginekologiczno-położniczej, onkologii klinicznej, rehabilitacyjnej, zdrowia psychicznego, urologicznej, chirurgii ogólnej, proktologicznej, ortopedii i traumatologii narządu ruchu, ortopedii i neuroortopedii, kardiologicznej i chorób wewnętrznych oraz okulistycznej. Rejestracja po remoncie przeprowadzonym w 2017 r.

[23] Do poradni: dermatologicznej, neurologicznej, stwardnienia rozsianego, leczenia oparzeń i ran przewlekłych, chirurgii plastycznej, otolaryngologii, hematologicznej oraz chirurgii szczękowo-twarzowej.

– na tablicach ogłoszeń umieszczono klauzule informacyjne o przetwarzaniu danych osobowych. Wskazano na nich także m.in. na konieczność okazania dowodu tożsamości przez pacjentów przy rejestrowaniu się do poradni;
– w części, do której dostęp miał wyłącznie personel (odpowiednio: za stanowiskami lub wewnątrz pomieszczenia) znajdowały się metalowe, zamykane szafy na dokumentację medyczną, uszeregowane według rodzajów poradni;
– wizyty do poszczególnych poradni (data i godzina) ustalane były na podstawie systemu „HIS". Na tej podstawie pacjentom wręczano kartki zawierające m.in. nazwę poradni, datę i godzinę wizyty;
– podczas obsługi pacjentów (w trakcie oględzin) nie posługiwano się nazwiskami pacjentów i innymi danymi wrażliwymi (jednostkami chorobowymi), a pacjentów identyfikowano na podstawie dowodów osobistych;
– nie stwierdzono sytuacji (w trakcie oględzin), w których w zasięgu wzroku osoby rejestrującej się byłyby dane osobowe lub dokumentacja medyczna innych pacjentów.

(akta kontroli str. 585-587, 717-718, 719-720, 780)

W wyniku oględzin trzech losowo wybranych miejsc przyjęć pacjentów[24], ustalono, co następuje:
– sposób wzywania pacjenta do poradni gwarantował anonimowość: pacjenci wywoływani byli (werbalnie) przez podanie imienia przez osobę wzywającą (lekarz/pielęgniarka);
– po wejściu do gabinetów stwierdzono, że karty pacjentów przechowane były w sposób niewidoczny dla innych pacjentów[25];
– dokumentacja medyczna (karty pacjentów) prowadzona była w systemie „HIS" oraz w formie papierowej (przez lekarza);
– gabinetów nie pozostawiono bez nadzoru – w poradni chirurgii ogólnej stosowano klucz elektroniczny (zamek szyfrowy), w pozostałych poradniach stosowano drzwi zamykane na klucz (w żadnym z zamków nie stwierdzono kluczy).

Dodatkowo, według oświadczeń pracowników Szpitala pacjenci wywoływani byli przez lekarzy lub pielęgniarki według ustalonej godziny przyjęcia (wywołanie odbywało się po imieniu pacjenta, względnie po godzinie przyjęcia w przypadku tożsamości imion kolejnych pacjentów).

(akta kontroli str. 588-589)

W Szpitalu zamontowano monitoring wizyjny, który rejestrował wyłącznie obraz (w tym na oddziałach szpitalnych, rejestracjach do poradni, windach). Prowadzono rejestr, który zawierał wykaz rejestratorów oraz wykaz kamer. Według danych udostępnionych w trakcie kontroli na terenie Szpitala zainstalowano według odrębnych (dwóch) źródeł: 219 i 215 kamer (sprawnych: 201, w większości analogowych, nieposiadających dostępu zdalnego) o orientacyjnym czasie nagrania wynoszącym od 5 do 450 dni.

Po przeprowadzonej w trakcie kontroli weryfikacji przedstawiono wykaz obejmujący łącznie 220 kamer, wśród, których część nie posiadała: adresów „IP", dostępu zdalnego oraz serwisu (interfejsu) web.

[24] Poradnia chirurgii ogólnej (gabinet lekarski; budynek główny, działająca w tej lokalizacji od 2011 r.), poradnia chirurgii szczękowo-twarzowej (gabinet lekarski i zabiegowy, budynek poradni szpitalnych, uruchomiony w 2005 r.) oraz poradnia kardiologiczna (gabinet lekarski, budynek główny, przy Oddziale Kardiologicznym).

[25] W gabinetach w miejscu ogólnie widocznym nie było kart pacjentów; w przypadku poradni kardiologicznej w gabinecie w miejscu ogólnie widocznym były karty pacjentów w kopertach odwróconych, tj. z niewidoczną częścią przednią z danymi pacjenta.

Prezes Zarządu wyjaśnił, że Szpital instalował monitoring wizyjny we wszystkich pomieszczeniach, *w których wymagany jest taki nadzór na podstawie odrębnych przepisów*. Zapisane na rejestratorach dane monitoringu wizyjnego były kasowane automatycznie za pomocą wewnętrznych mechanizmów rejestratorów. Rejestratory nadpisywały najstarsze zapisy bieżącym obrazem z kamer. Zapisy były usuwane w sposób trwały i nie było możliwości ich odzyskania po ich nadpisaniu nowym zapisem. Dodał, że istniała możliwość wykonania kopii nagrań *na wniosek upoważnionych osób lub organów* (…), a w*szelkie wykonane kopie nagrań monitoringu przechowuje się 10 lat, po których upływie są trwale usuwane*.

Dostęp do zasobów sieciowych z kopiami zapisów, na podstawie upoważnienia ADO posiadało (w styczniu 2019 r.) pięciu pracowników Działu IT.

Odnosząc się do udostępnienia pracownikom informacji o wprowadzaniu kamer monitoringu, Prezes Zarządu wyjaśnił, że *monitoring wizyjny jest stosowany od początku działania Szpitala*. Dodał, że *montaż nowych kamer/rejestratorów wymusza konieczność odpowiedniego oznakowania tego miejsca*. Poza ww. oznaczeniem terenu Szpitala, że obiekt jest monitorowany (znakami graficznymi i klauzulami informacyjnymi), w Szpitalu opracowano i wdrożono (w styczniu 2019 r.) ww. procedurę zarządzania monitoringiem wizyjnym, zamieszczoną w Intranecie.

(akta kontroli str. 334-335, 336-338, 406-480, 590-591, 592-593, 655-656)

2.2. W okresie objętym kontrolą zarządzanie siecią w Szpitalu nie odbywało się za pomocą scentralizowanego systemu zarządzania usługą katalogową.

Prezes Zarządu wyjaśnił, że zarządzanie kontami użytkowników komputerów odbywało się zgodnie z procedurą „ogólne zasady bezpieczeństwa informacji". *Dział IT konfigurując nowe komputery przygotowywał standardowe instalacje zawierające zdefiniowanego użytkownika „u.", założonego na ograniczonych prawach użytkownika systemu W. (bez praw administratora komputera).* Dodał, że komputery przygotowywane do pracy posiadały zainstalowany komplet oprogramowania niezbędnego do pracy (w tym system „HIS" i oprogramowanie antywirusowe). *Użytkownicy nie instalowali samodzielnie oprogramowania, nie konfigurowali komputerów i nie mogli samodzielnie tworzyć nowych użytkowników komputera.* Zasady tworzenia haseł do udostępnionego użytkownikom konta były opisane w ww. procedurze.

Dodał, że na wybranych komputerach testowane było w ograniczonym zakresie zarządzanie domenowe. Objęcie takim zarządzaniem wszystkich komputerów szpitalnych było zaplanowane w ramach realizowanego przez Urząd Marszałkowski Województwa Małopolskiego projektu „Małopolski System Informacji Medycznej 2".

(akta kontroli str. 481-482, 483-484)

W Szpitalu w systemie „HIS" wykorzystywano moduły: „oddział"[26], „poradnia"[27], „zakażenia szpitalne"[28], „apteka"[29], „blok operacyjny"[30] oraz „pracownie"[31].

Personelowi niemedycznemu Szpitala umożliwiono dostęp do danych medycznych w zakresie niezbędnym do wykonywanych zadań (na podstawie kontrolowanej,

[26] Realizacja czynności związanych z leczeniem szpitalnym pacjenta – przyjęcie, wypis, skierowania na badania, zapotrzebowania do apteki szpitalnej, monitorowanie czynników zakaźnych.

[27] Realizacja czynności związanych z leczeniem ambulatoryjnym pacjenta – przyjęcie, wypis, skierowania na badania i do pracowni diagnostycznych, prowadzenie terminarzy wizyt.

[28] Monitorowanie zaistniałych zakażeń szpitalnych, ich przyczyn i czynników mogących na nie wpływać.

[29] Prowadzenie magazynów leków i ewidencji obrotu lekami dla oddziałów i pacjentów.

[30] Wprowadzanie danych związanych z zabiegami operacyjnymi wykonywanymi na bloku operacyjnym a zlecanymi z oddziałów szpitalnych, ewidencja zużytych materiałów i czasu pracy poszczególnych sal.

[31] Wprowadzanie danych związanych z badaniami i zabiegami wykonywanymi przez pracownie.

losowo dobranej próby 30 osób), przy czym nadanie pełnych upoważnień dwóm osobom będzie opisane w dalszej części niniejszego wystąpienia.

(akta kontroli str. 770-771, 772, 776)

Prezes Zarządu wskazał, że zarządzanie przydzielaniem i odbieraniem praw dostępu do systemu „HIS", w tym służącego do prowadzenia Elektronicznej Dokumentacji Medycznej (*EDM*), odbywało się zgodnie z ww. procedurą „zarządzanie uprawnieniami". O nadanie lub cofnięcie praw dostępu do systemu „HIS" wnioskował w stosunku do swoich podwładnych, kierownik komórki organizacyjnej (na obowiązującym formularzu). Dostęp nadawany był przez administratora właściwego systemu, który zakładał konto użytkownika i przypisywał zestaw praw do danego konta.

Prezes Zarządu wyjaśnił, że *adekwatność przyznanych praw dostępu była systematycznie nadzorowana przez kierowników komórek organizacyjnych.* Kryterium oceny adekwatności stosowanych praw była niezbędność posiadania dostępu do określonych danych względem możliwości pełnienia sprawowanej funkcji i wykonywania powierzonych zadań. Dodał, że *dostępu do danych, które były zbędne, nie przydzielano, stosując zasadę minimalizacji praw dostępu.*

(akta kontroli str. 481-482, 483-484)

2.3. Według stanu na 11 lutego 2019 r. w Szpitalu zatrudnionych było 562 pielęgniarek i położnych. Na zbadanej, losowej próbie 39 z nich stwierdzono, że 31 z nich posiadało dostęp w systemie „HIS" ograniczony do miejsca świadczenia pracy, zaś dwie pielęgniarki również do innych oddziałów i poradni (o różnej specjalności medycznej), a kolejne sześć pielęgniarek (w tym „specjalistka" i „starsza" pielęgniarka), nie miało dostępu do systemu „HIS" (brak konta użytkownika)[32].

W opisach tych stanowisk pracy kluczowy obowiązek sformułowano jako dokumentowanie świadczeń zdrowotnych, przewidując jako „kwalifikacje niezbędne (minimalne)" pracę w systemie „M.O." (obsługę sprzętu komputerowego i monitora ekranowego).

Prezes Zarządu wyjaśnił, że użytkownicy otrzymują dostęp do systemu „HIS" wyłącznie na podstawie pisemnego wniosku swojego bezpośredniego przełożonego.

(akta kontroli str. 485-486, 487, 492-502, 659-663, 664-666, 667-680, 809-821)

Rejestr upoważnień pracowników Szpitala do przetwarzania danych osobowych (od 25 maja 2018 r.) obejmował 2 046 osoby[33]. Zakres upoważnień obejmował dane osobowe pacjentów, osób upoważnionych i opiekunów prawnych oraz dane medyczne. Przewidziany w rejestrze zakres czynności odnosił się do art. 4 pkt 2 RODO; jako fakt powodujący ustanie upoważnienia przyjmowano rozwiązanie umowy lub stosunku pracy.

(akta kontroli str. 770-771, 772, 777)

Prezes Zarządu wyjaśnił, że *w Szpitalu prowadzona jest jedynie dokumentacja medyczna w postaci papierowej. Posiadany „HIS" umożliwia generowanie dokumentów elektronicznych, jednak po wydrukowaniu, zgodnie z obowiązującym prawem dokumentacja ta wymaga autoryzacji i jest klasyfikowana, jako dokumentacja papierowa.*

---

[32] Próba 30 osób wybrana losowo; dla zapewnienia, aby w wybranej do badania próbie znajdowała się przynajmniej jedna osoba z każdego oddziału/poradni dodatkowo dobrano dziewięć osób (według kolejności na liście), tj. łącznie skontrolowano 39 osób. W Szpitalu wykorzystywano oprogramowanie „O.", autorstwa „C.H.", Wersja „6.50.6.0". Oprogramowanie to zapewniało obsługę części medycznej (związanej z udzielaniem świadczeń zdrowotnych i prowadzeniem dokumentacji medycznej).

[33] Z uwagi na zastosowany outsourcing usług sprzątania, nie obejmował salowych/personelu sprzątającego.

Dodał, że wszystkie zlecenia badań wewnątrz Szpitala były przesyłane w formie elektronicznej, *pomiędzy zintegrowanymi systemami wchodzącymi w skład „HIS"* (umożliwiającymi wymianę danych). *Ponadto każde zlecenie wykonania badań jest również drukowane, a następnie z pacjentem lub z pobranym materiałem przekazywane do badań. Forma papierowa zleconych elektronicznie badań jest niezbędna ze względu na obowiązek złożenia podpisu pod zleceniem i wynikiem badań.*

W ramach wewnętrznego transportu chorych wraz z pacjentem sanitariusze (posiadający upoważnienia do przetwarzania danych osobowych*)* przewozili papierowe zlecenia na wykonanie badań (zabezpieczone w kopercie/teczce, uniemożliwiającej dostęp do danych osobowych postronnym osobom).

(akta kontroli str. 717-718, 719-720)

2.4. Po 25 maja 2018 r. w Szpitalu zatrudnienie zakończyło 120 osób (według stanu na 11 lutego 2019 r.). W wyniku oględzin systemu „HIS"/„EDM" w zakresie dostępu dla pracowników (posiadane konto użytkownika), z którymi rozwiązano stosunek pracy (w tym również tzw. lekarzy kontraktowych i personelu zatrudnionego na podstawie umów cywilnoprawnych), ustalono, że trzy osoby zatrudnione na stanowiskach pielęgniarek, którym utworzono konto w systemie „HIS", a które przestały być pracownikami, posiadały aktywne konto i nie logowały się do tego systemu przez ponad cztery lata[34].

Prezes Zarządu wyjaśnił, że wynikało to *ze sposobu, w jakim od strony technicznej zarządza się prawami dostępu użytkowników w systemie „HIS".* Dodał, że *taka sytuacja nie świadczy o błędzie w zarządzaniu kontem danego użytkownika, a jedynie o technicznych ograniczeniach (zastosowanych przez producenta rozwiązaniach) systemu „HIS".*

W trakcie ww. oględzin stwierdzono również, że w pięciu przypadkach osoby wykonujące zawód medyczny i zajmujące stanowiska rejestratorek medycznych, które przestały być pracownikami Szpitala (po 25 maja 2018 r.), nie miały założonego konta w systemie „HIS".

W opisach stanowisk pracy rejestratorek medycznych jako „kluczowy obowiązek" sformułowano m.in. „zakładanie i dokonywanie wydruków „historii choroby", „ewidencjonowanie pacjenta w systemie „O." z wszystkimi wymaganymi opcjami uzupełnienia", codzienne prowadzenie i wydruk księgi głównej Szpitala z systemu „O.". W ramach „kwalifikacji niezbędnych (minimalnych)" dla umiejętności informatycznych wskazywano m.in. „podstawową umiejętność obsługi oprogramowania „O." i „podstawowe umiejętności posługiwania się programami obowiązującymi w Szpitalu w zakresie obsługi pacjenta i sprawozdawczości".

Dla personelu medycznego (m.in. opiekun medyczny, lekarz starszy asystent) jako „kwalifikacje niezbędne (minimalne)" wymagano „znajomości szpitalnego systemu informatycznego".

Prezes Zarządu wyjaśnił, że możliwe jest, że osoby, które były zatrudnione na stanowisku rejestratorki medycznej nie posiadały konta i nadanych praw dostępu w systemie „HIS", *jeżeli zakres obowiązków tych osób nie wymagał takiego dostępu.*

(akta kontroli str. 485-486, 487, 492-502, 503-507, 664-666, 667-680, 685-689)

2.5. W okresie objętym kontrolą Szpital posiadał osiem umów z dostawcami oprogramowania w zakresie świadczenia przez dostawców serwisu oprogramowania danego producenta (tzw. *help desk*)[35].

---

[34] Próba 30 osób wybrana losowo, z grupy 120 pracowników.

[35] Poza wskazanymi poniżej: z „M." (system „C." do obsługi laboratorium), „M." (serwis do systemu „I." służącego do obsługi finansowo-księgowej), „A. P." (producent systemu „I."), „H.pl" (obsługa poczty elektronicznej i strony internetowej) oraz „P.P." (system do obsługi diagnostyki obrazowej).

Oględzinami objęto trzy wybrane elementy systemu „HIS", w zakresie świadczenia przez ich dostawców pomocy technicznej, w okresie od 25 maja 2018 r., tj.:

– system „HIS":
  - wyznaczony pracownik Działu IT zdalnie zgłaszał usterki dostawcy oprogramowania („*C.H.C."* z siedzibą w Katowicach) przez stronę internetową dostawcy, wypełniając formularz z opisem błędu;
  - w zgłoszeniu do dostawcy wskazywano ID pacjenta, które było generowane dla pacjenta przez program;
  - w przypadku przesyłania danych wraz z załączoną dokumentacją medyczną, ww. pracownik Szpitala zamazywał dane osobowe pacjenta (w dokumentacji medycznej);
  - do dnia oględzin ww. pracownik dokonał 181 zgłoszeń serwisowych, które zweryfikowano[36];
– system „PACS"[37] do obsługi świadczeń zdrowotnych z zakresu radiologii:
  - wyznaczonych dwóch pracowników Działu IT (w tym Kierownik) emailowo zgłaszało usterki dostawcy oprogramowania („S." z siedzibą w Warszawie) poprzez opis (w treści emaila) błędu/usterki;
  - zgłoszenie mogło również następować drogą telefoniczną (na podstawie tego typu zgłoszeń, dostawca oprogramowania rejestrował zgłoszenie, a jego potwierdzenie przesyłał emailem);
  - w zgłoszeniu do dostawcy oprogramowania wskazywano ID pacjenta, które było generowane dla pacjenta przez program „O.", które jednocześnie wraz ze zleceniem przesyłane było do ww. programu;
  - do dnia oględzin dokonano 11 zgłoszeń serwisowych (przez ww. pracownika), które zweryfikowano;
– system do obsługi świadczeń zdrowotnych z zakresu podstawowej opieki zdrowotnej:
  - Kierownik Działu IT emailowo zgłaszał usterki dostawcy oprogramowania („drE." z siedzibą w Krakowie) z opisem błędu/usterki;
  - zgłoszenie mogło również następować drogą telefoniczną; na podstawie tego typu zgłoszeń, dostawca ww. oprogramowania rejestrował zgłoszenie i przystępował do jego zrealizowania, a w przypadku, gdy błędu nie można było usunąć bezzwłocznie, przysłał potwierdzenie przyjęcia zgłoszenia (z jego numerem) emailem;
  - w zgłoszeniu do dostawcy oprogramowania wskazywano ID zleceń/wyników badań (pacjenta), które było generowane dla pacjenta przez ww. program;
  - do dnia oględzin dokonano 58 zgłoszeń serwisowych (przez ww. pracownika), które zweryfikowano.

We wszystkich ww. programach:

– zgłoszenia serwisowe z komórek organizacyjnych Szpitala do Działu IT odbywały się telefonicznie, na ich podstawie pracownicy Działu formułowali zgłoszenia do dostawcy oprogramowania;
– w opisie wszystkich kontrolowanych zgłoszeń, nie stwierdzono wpisanych danych pacjenta (dane osobowe, w tym medyczne); podawano dane ogólne zgłaszanego przypadku, w tym ID pacjenta/wyników badań i/lub zleceń.

(akta kontroli str. 696-702, 703-704)

[36] W dniu 23 maja 2018 r. dostawca ww. oprogramowania poinformował Szpital o konieczności zawarcia umowy powierzenia danych (umowę taką zawarto), a w dniu 29 maja 2018 r. dostawca oprogramowania poinformował Szpital o konieczności pomijania danych osobowych w dokonywanych zgłoszeniach serwisowych.

[37] „Picture Archiving and Communication System".

Prezes Zarządu wskazał, że kwestia kontaktu z dostawcą oprogramowania, w szczególności zgłaszanie ewentualnych problemów była uregulowana w umowach z danym dostawcą, nie w dokumentacji wewnętrznej Szpitala. Ponadto użytkownicy systemów nie byli upoważnieni do bezpośredniego kontaktu z dostawcami oprogramowania. W przypadku wystąpienia problemów, użytkownicy zgłaszali je do administratora danego systemu w Szpitalu.

Odnosząc się do posiadania przez Szpital informacji dotyczących wywiązania się przez dostawcę nowo wdrożonego oprogramowania z obowiązku przeprowadzania testów adaptacyjnych[38], Prezes Zarządu wyjaśnił, że *producent oprogramowania był zobowiązany do przestrzegania prawa, a dostawcy oprogramowania w zawartych umowach deklarowali zgodność swoich systemów z obowiązującym prawem.*

(akta kontroli str. 481-482, 483-484)

2.6. W okresie objętym kontrolą Szpital posiadał 72 umowy powierzenia przetwarzania danych osobowych pacjentów. W umowach tych Szpital występował 48 razy, jako administrator danych, powierzający przetwarzanie danych innemu podmiotowi, a 24 razy jako podmiot przetwarzający dane.

Szczegółowym badaniem pod kątem wymagań określonych w art. 28 RODO objęto pięć umów zawartych przez Szpital, w których był podmiotem powierzającym przetwarzanie danych objętych systemem „HIS", tj. na prowadzenie systemu „O.", „drE.", „ARPACS", „L.": i „I.". Umowy te zawierały wszystkie postanowienia wymagane przez art. 28 RODO. Wskazany w tych umów zakres danych osobowych powierzonych przez Szpital podmiotom zewnętrznym wynikał z rodzaju usług, które zgodnie z umową mieli na rzecz Szpitala realizować.

(akta kontroli str. 721-734, 735-742, 743-747, 748-750, 751-769, 770-772, 777)

Prezes Zarządu wskazał, że przyczyny zawierania umów powierzenia przetwarzania danych były następujące:

- wynikająca z prowadzonego leczenia konieczność zlecania świadczeń medycznych, badań lub opisów badań na rzecz pacjentów Szpitala innym podmiotom wykonującym działalność leczniczą, na podstawie umów pomiędzy podmiotami;
- konieczność wykonywania przez Szpital świadczeń medycznych na rzecz pacjentów innych podmiotów wykonujących działalność leczniczą, na podstawie umów pomiędzy podmiotami;
- konieczność udostępnienia dostawcom sprzętu i oprogramowania, posiadanej przez Szpital infrastruktury i danych w systemie „HIS", w celu realizacji zawartej umowy serwisu i wykonania wynikających z tej umowy prac;
- konieczność zawarcia umowy ubezpieczenia i wynikającego z zawartej umowy procesu likwidacji szkód.

(akta kontroli str. 481-482, 483-484)

2.7. W okresie objętym kontrolą w Szpitalu nie prowadzono odrębnej dokumentacji dotyczącej naruszeń ochrony danych osobowych. Prezes Zarządu wskazał na dokumentację wynikającą z PBI oraz procedur systemu zarządzania bezpieczeństwem informacji (norma ISO 27001) oraz programu akredytacji szpitali MZ (wskazano m.in. na procedurę zarządzania incydentami bezpieczeństwa informacji).

W Szpitalu rejestrowane były stwierdzone lub zgłaszane tzw. incydenty bezpieczeństwa. Rejestr incydentów jako załącznik do procedury zarządzania incydentami bezpieczeństwa informacji, był prowadzony elektronicznie. W rejestrze tym znajdowały się stwierdzone naruszenia bezpieczeństwa danych osobowych

[38] Określonego w art. 21 ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570 ze zm.).

(nie każdy rejestrowany incydent był uważany za naruszenie bezpieczeństwa danych osobowych w rozumieniu RODO).

Rejestr stwierdzonych przypadków naruszenia bezpieczeństwa danych osobowych („rejestr incydentów") obejmował w 2018 r. 28 incydenty (m.in. 13 dotyczyło przetwarzania danych osobowych bez wydanego upoważnienia i przeszkolenia, a trzy dotyczyły działania „HIS"). W żadnym z nich nie stwierdzono naruszenia prawa. W sześciu przypadkach stwierdzono konieczność wprowadzenia działań korygujących, a w 10 – konieczność ponownego szacowania ryzyka.

Zarejestrowano jeden incydent (w sierpniu 2018 r.) dotyczący naruszenia poufności i dostępności danych (ujawnienia danych niewłaściwej osoby). Polegał on na nieumyślnym zabraniu dokumentacji medycznej pacjenta przez innego pacjenta jednej z poradni, który zgłoszono (elektronicznie) do Prezesa UODO. Przyczyną zdarzenia było naruszenie „zasady czystego biurka" przez personel medyczny. Szpital poinformował zainteresowane osoby i ustalił sposób odebrania dokumentacji od osoby, która ją zabrała oraz sposób przekazania dokumentacji pacjentowi, którego ta dokumentacja dotyczyła. Odpowiedzi z UODO Szpital nie uzyskał. Po tym incydencie IOD przeprowadził szkolenie dla pracowników oddziału, którego działalności ten incydent dotyczył z bezpieczeństwa dokumentacji medycznej.

W 2019 r. (15 marca) w rejestrze incydentów odnotowano cztery incydenty. Podczas oględzin na losowo wybranej próbie stwierdzono, że w Szpitalu logowano się jednym kontem przez kilka osób oraz, że hasła miały niewłaściwą złożoność. Na dzień zakończenia kontroli sytuacji te nie wpisano do rejestru incydentów (nie uznano je za przypadki naruszenia bezpieczeństwa danych).

W analizowanym okresie do IOD Szpitala nie wpłynęły skargi dotyczące ujawnienia danych osobowych.

(akta kontroli str. 133-137, 508-521, 590-593, 638-648, 651, 770-771, 772, 777)

2.8. Regulacje wewnętrzne dotyczące sposobu udostępniania dokumentacji medycznej: określono w załączniku nr 5 do regulaminu organizacyjnego Szpitala z dnia 8 lutego 2019 r. (wcześniej: z dnia 7 sierpnia 2017 r.). Przyjęta procedura określała sposób udostępniania dokumentacji medycznej, wymogi formalne związane ze złożeniem wniosku o jej udostępnienie i wysokość opłaty z tym związanej.

Określono wzór wniosku o udostępnienie dokumentacji medycznej (i potwierdzenia jej odbioru) wraz z potwierdzeniem złożenia wniosku wydawanym pacjentowi, a także wzór rejestru wniosków dotyczących udostępnienia dokumentacji oraz wzór karty udostępnienia dokumentacji medycznej z archiwum.

(akta kontroli str. 508-509, 510-511, 522-524, 525-530, 711-716)

Od 25 maja do 31 grudnia 2018 r. do Szpitala wpłynęło łącznie 4 595 wniosków od pacjentów lub osób fizycznych przez pacjentów upoważnionych o udostępnienie dokumentacji medycznej. W 2018 r. takich zapytań było: 6 702 (w 6 485 przypadkach udostępniono dokumentację, a w 29 przypadkach odmówiono jej udostępnienia; 217 osób pomimo złożonego wniosku nie odebrało dokumentacji).

Analiza 30 wniosków złożonych przez pacjentów, w przypadku, których udostępniono dokumentację medyczną innej osobie, niż pacjent, którego ta dokumentacja dotyczyła, wykazała, że wnioski te składane były na przyjętym wzorze; na wnioskach pacjenci zobowiązywali się do pokrycia kosztów udostępnienia dokumentacji medycznej na podstawie ustawy o prawach pacjenta.

Na wnioskach pacjenci wskazywali dane osoby upoważnionej do odbioru dokumentacji medycznej, potwierdzając to własnoręcznym podpisem lub do wniosku dołączano odręczne upoważnienie do odbioru (stwierdzono przy tym przypadki nieczytelnych podpisów pacjentów, tj. bez wskazania ich imienia i nazwiska).

Na wnioskach znajdowały się potwierdzenia odbioru dokumentacji. Nie stwierdzono przypadków udostępnienia danych medycznych osobom nieuprawnionym.

Od 25 maja do 31 grudnia 2018 r. do Szpitala wpłynęło łącznie 572 zapytań od podmiotów innych niż pacjenci lub osoby przez pacjentów upoważnione o udostępnienie dokumentacji medycznej[39], w tym 69 zapytań od ubezpieczycieli. Ogółem w 2018 r. takich wniosków było – odpowiednio: 899 oraz 118.

Analiza 30 zapytań od 16 firm ubezpieczeniowych, wykazała, że zapytania te zawierały jako załączniki m.in. kopie upoważnień (pełnomocnictw) pacjentów do wystąpienia o taką dokumentację.

Szpital odmawiał ubezpieczycielom udostępnienia dokumentacji medycznej pacjenta (ubezpieczonego) ze względu na braki formalne m.in. przedłożenie kopii podpisów i pełnomocnictwa pacjenta (brak oryginalnego pełnomocnictwa/podpisu); brak oryginalnego podpisu lekarza oraz brak upoważnienia dla lekarza. W poddanych kontroli zbiorach dokumentacji znajdowały się również przypadki pisemnej informacji kierowanej do ubezpieczyciela, że dana osoba nie była pacjentem Szpitala.

Szpital przesyłał dokumentację medyczną powołując się na art. 28 ustawy o prawach pacjenta oraz zarządzenie Prezesa Zarządu, tj. po wniesieniu opłaty obejmującej koszty przygotowania kserokopii i opłaty pocztowej za jej przesłanie (na podstawie faktury), w tym po uzyskaniu opinii radcy prawnego Szpitala. Na tej podstawie weryfikowano podstawę prawną każdego żądania/zapytania/prośby o udostępnienie dokumentacji lub danych w niej zawartych.

(akta kontroli str. 705, 706-710)

2.9. Według przedstawionego wykazu na 729 stacjach roboczych w Szpitalu użytkowano system „HIS" (na wszystkich komputerach zainstalowano system antywirusowy „K.L."). Szpital nie posiadał pełnych danych o systemach operacyjnych zainstalowanych na stacjach roboczych w infrastrukturze IT.

(akta kontroli str. 770-771, 772, 777)

Szpital stosował regulacje wewnętrzne dotyczące zabezpieczeń, tj.:

- zasady stosowania zabezpieczeń fizycznych opisane były w procedurze „zarządzania kluczami do pomieszczeń"; zasady zabezpieczenia danych, serwerów i wykonywania kopii zapasowych opisane były w procedurze „zasady zabezpieczenia systemów informatycznych", szczegóły dotyczące tworzenia i przechowywania kopii zapasowych zawarto w załączniku (niepodlegającym publikacji); ponadto stosowanie fizycznych zabezpieczeń zasilania opisane było w planach awaryjnych przygotowanych przez Dział Infrastruktury Szpitalnej[40];
- regulacje dotyczące ochrony kryptograficznej komputerów zawarte były w załączniku do PBI („regulamin korzystania z komputerów przenośnych"), zasady ochrony kryptograficznej w sieci zawarte były w procedurze „zarządzanie dostępem zdalnym";
- sposób nadawania loginów był opisany w procedurze „zasady zakładania kont użytkowników".

[39] Pozostałe zapytania od podmiotów/instytucji wpływały m.in. od Miejskiego Ośrodka Pomocy Społecznej w Krakowie, Zakładu Ubezpieczeń Społecznych, Kasy Rolniczego Ubezpieczenia Społecznego, Biura Rzecznika Praw Pacjenta, sądów, prokuratur, Policji, NFZ, Wojewódzkiej Komisji ds. Orzekania o Zdarzeniach Medycznych w Krakowie oraz firm odszkodowawczych.

[40] Obejmowały one instrukcje postępowania: na wypadek awarii hydrauliczno-ciepłowniczej, postępowania dyspozytora na wypadek powstania awarii wentylacji mechanicznej i klimatyzacji oraz awarii elektroenergetycznej, awarii w instalacji gazów medycznych, awarii sprzętu komputerowego, awarii urządzeń telekomunikacyjnych, postępowania dyspozytora na wypadek rozlania rtęci, powstania kradzieży lub dewastacji mienia Szpitala, awarii lodówek w Aptece Szpitalnej, wycieku oleju napędowego oraz wszelkich substancji ropopochodnych oraz kasowania alarmu przeciw pożarowego.

Wyjaśniając przyjętą politykę dotyczącą zmiany haseł dostępu w systemie „HIS" Prezes Zarządu wskazał, że *system „HIS" wymusza zmianę hasła, co 30 dni i pamięta ostatnio używane hasła, uniemożliwiając ich ponowne użycie. Ponadto weryfikowana jest długość i złożoność hasła w celu blokowania haseł prostych.*

(akta kontroli str. 508-509, 510-511, 574, 664-666, 667-680)

W wyniku przeprowadzonych oględzin dwóch serwerowni Szpitala, ustalono, że jedna z serwerowni (w części administracyjnej budynku[41]) nie posiadała drzwi antywłamaniowych (prowadziły do niej drzwi standardowe, wzmocnione metalem, bez atestu dla drzwi antywłamaniowych i/lub przeciwpożarowych, zamykane na dwa zwykłe zamki mechaniczne) oraz systemu antywłamaniowego. W trakcie kontroli Szpital rozpoczął procedurę zakupu drzwi antywłamaniowych.

W pomieszczeniu tej serwerowni zamontowano kamerę, rejestrującą obraz (wejście do serwerowni). Przed wejściem do serwerowni znajdowała się jedna wolnostojąca gaśnica (przeznaczona do gaszenia urządzeń pod napięciem). Urządzenia serwerowni (ok. 10 serwerów w dwóch szafach „RACK") podłączone były do układu podtrzymywania napięcia „UPS" (pięć urządzeń, w tym cztery w szafach i jeden wolnostojący); dodatkowo nad pomieszczeniem znajdował się dodatkowy „UPS" (urządzenia te podtrzymywały zasilanie do ok. 20 min.).

(akta kontroli str. 575-576, 577-578, 780)

Druga z serwerowni znajdowała się w części budynku Szpitala przeznaczonej do udzielania świadczeń zdrowotnych (ok. 30m^2). Pomieszczenie, w którym znajdowały się serwery posiadało dwa „zespoły okien" (z kratami antywłamaniowymi i roletami zabezpieczającymi). Zamontowano drzwi podwójne: standardowe oraz antywłamaniowe i przeciwpożarowe (z atestami), zamykane na dwa zwykłe zamki mechaniczne. Serwerownia wyposażona była w alarm przeciwwłamaniowy (z powiadomieniem dźwiękowym). Monitoring pomieszczenia był prowadzony poprzez rejestrację obrazu (trzy kamery).

Przed wejściem do serwerowni znajdowała się jedna gaśnica (w skrzynce, przeznaczona do gaszenia urządzeń pod napięciem). Druga taka gaśnica (wolnostojąca) znajdowała się wewnątrz serwerowni. Urządzenia serwerowni (ok. 15 serwerów w trzech szafach „RACK") podłączone były do układu podtrzymywania napięcia „UPS" (cztery urządzenia); urządzenia te podtrzymywały zasilanie do ok. 20 min. W serwerowni znajdowały się kaloryfery, które były odłączone na zaworze zasilającym (w trakcie kontroli kaloryfery te zdemontowano).

(akta kontroli str. 575-576, 577-578, 780)

Pomieszczenia obu serwerowni nie były oznakowane, nie odróżniały się od wejść do innych, sąsiednich pomieszczeń. Ewidencjonowano przebywanie osób w serwerowniach (zeszyty wejść/wyjść). Zamontowane wewnątrz centralki klimatyzacji powiadamiały (automatycznie emailowo) Dział IT o zmianach temperatury (poniżej/powyżej 18°C). W przypadku zaniku napięcia następowało także powiadomienie (automatycznie emailowo) Działu IT. Klucze do serwerowni znajdowały się w pomieszczeniach Działu IT.

Wewnątrz serwerowni znajdowały się czujki systemu przeciwpożarowego (sygnalizatory znajdowały się przed wejściami), które podłączone były do systemu Państwowej Straży Pożarnej. Wewnątrz serwerowni działały systemy klimatyzacji nadmiarowej, tj. po dwa klimatyzatory odrębne z centralkami (działające zamiennie w trybie całodobowym). Serwerownie zasilane były z dwóch niezależnych źródeł (po zaniku napięcia, tj. po ok. 1 min. przez automatycznie włączające się agregaty). Stan okablowania nie wskazywał uszkodzeń. Przez pomieszczenia serwerowni nie

[41] Pomieszczenie bez okien (ok. 10 m^2), sąsiadujące z innymi pomieszczeniami biurowymi.

przebiegały rury, nie znajdowały się w nich także urządzenia komputerowe wycofane z użytku lub materiały łatwopalne.

(akta kontroli str. 575-576, 577-578, 780)

W ramach kontroli dokonano oględzin wybranej losowo próby 30 komputerów (po 10 użytkowanych przez: lekarzy, pielęgniarki lub położne oraz pracowników administracji), służących do przetwarzania danych osobowych[42].

W wyniku oględzin nie stwierdzono, aby kontrolowani użytkownicy posiadali uprawnienia administratorów w systemach operacyjnych komputerów.

(akta kontroli str. 664-666, 667-680, 690-695)

Polityka wykonywania kopii bezpieczeństwa w Szpitalu zdefiniowana była w procedurze „zasady zabezpieczenia systemów informatycznych". Prezes Zarządu wyjaśnił, że wykonywanie kopii bezpieczeństwa obejmowało całe bazy danych oraz wybrane woluminy. Dokładny wykaz wykonywanych kopii bezpieczeństwa znajdował się w Dziale IT w dokumencie „polityka kopii zapasowych".

Zgodnie z tym dokumentem w Szpitalu wykorzystywano 13 rodzajów oprogramowania, w dwóch serwerowniach; kopie w 11 przypadkach wykonywano automatycznie, w dziewięciu przypadkach, co 24 godziny (w sześciu przypadkach były to kopie pełne).

Ze względów bezpieczeństwa kopie zasobów używanych w jednej serwerowni przechowywano w drugiej z nich. *Poprawność wykonywania kopii bezpieczeństwa weryfikowano na bieżąco (…) administrator okresowo weryfikował statusy wykonanych kopii bezpieczeństwa oraz wykonywał ręczne testy odzyskiwania danych z kopii bezpieczeństwa* (…) Dodatkowo skuteczność wykonywania kopii bezpieczeństwa podlegała regularnej, planowej ocenie, zgodnie z „wykazem zasobów podlegających regularnej ocenie skuteczności zabezpieczeń".

(akta kontroli str. 664-666, 667-680)

W Szpitalu wykorzystywano dziewięć laptopów jako komputery przenośne. Prezes Zarządu wskazał, że w celu zagwarantowania bezpieczeństwa lokalnie przechowywanych danych na tych komputerach stosowano szyfrowanie danych na dyskach twardych (pliki lub dyski). Ponadto w Szpitalu używano komputerów typu laptop jako komputery stacjonarne bez ich wynoszenia z pomieszczenia, w którym były używane. W celu zabezpieczenia przed kradzieżą tego typu komputerów zakupiono linki zabezpieczające. Do sprzętu tego typu stosowano te same zasady, co do innych komputerów stacjonarnych.

(akta kontroli str. 664-666, 667-670)

Prezes Zarządu wskazał, że w Szpitalu stosowano anonimizację danych w przypadkach udostępniania danych medycznych w celu wykonywania badań naukowych lub umożliwienia kształcenia kadry medycznej. Dane udostępniano na podstawie zawartych uprzednio umów, a anonimizację danych wykonywano przed udostępnieniem danych.

(akta kontroli str. 664-666, 667-670)

W Szpitalu w sierpniu i w październiku 2018 r. przeprowadzono audyt wewnętrzny dotyczący bezpieczeństwa informacji i systemów informacyjnych. Kryteria audytu obejmowały normę ISO 27001:2013, standardy akredytacyjne (Centrum Monitorowania Jakości w Ochronie Zdrowia 2009), RODO oraz przepisy ustawy ochronie danych osobowych. Audytem objęto 14 komórek organizacyjnych. W jego wynikach zidentyfikowano tzw. potencjały do doskonalenia, tj. zwiększenie nadzoru nad: aktualnością tablic informacyjnych (na jednym z oddziałów); indywidualną dokumentacją medyczną pacjenta pozostawioną i dostępną dla osób postronnych

[42] Osoby wybrane losowo wśród pracowników medycznych, tj. dostępne na punkcie pielęgniarskim danego oddziału lub w pokoju lekarzy danego oddziału lub pracownicy administracji na swoich stanowiskach.

na dwóch oddziałach; przeprowadzenie szkolenia wewnętrznego statystek medycznych w zakresie ochrony danych osobowych (na jednym z oddziałów); zwiększenie nadzoru (Kierownika Działu Kontraktowania, Rozliczeń i Statystyki Medycznej) nad terminowym kompletowaniem i „zamknięciem" dokumentacji medycznej oddziału i jej przekazywania do archiwum szpitalnego.

(akta kontroli str. 508-509, 510-511, 531-573)

Stwierdzone nieprawidłowości

W działalności Szpitala w zakresie zapewnienia prawidłowego przetwarzania i ochrony danych osobowych stwierdzono następujące nieprawidłowości:

1. W wyniku oględzin systemu „HIS"/„EDM" ustalono, że dwoje (z 30 losowo kontrolowanych) pracowników administracji Szpitala (ds. planowania i analiz oraz ds. komercji i marketingu) posiadało pełny dostęp do tego systemu (do wszystkich informacji z tzw. oddziałów płatnych)[43].

   Prezes Zarządu wyjaśnił, powołując się na art. 24 ust. 2 pkt 1 ustawy o prawach pacjenta, że dostęp do danych medycznych mogą posiadać inne osoby niż personel medyczny („inne osoby wykonujące czynności pomocnicze przy udzielaniu świadczeń zdrowotnych"). Dodał, że w szczególności dostęp do dokumentacji medycznej pacjentów, którym wykonywane są odpłatne świadczenia medyczne *mają wybrani pracownicy Szpitala, np. Kierownik Działu Komercji, Marketingu i Komunikacji Korporacyjnej. Uprawnienia dostępu do systemu „HIS" są przyznawane zgodnie z zasadami minimalizacji praw. Jeżeli będzie możliwe ograniczenie zakresu nadawanych uprawnień bez ograniczenia możliwości wykonywania obowiązków, a zarazem będzie to technicznie możliwe do zrealizowania, to takie ograniczenie dostępu będzie zastosowane.*

   Zdaniem NIK, mając na uwadze art. 5 pkt 1 lit. c) RODO oraz § 20 ust. 2 pkt 4 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[44], zasadne jest ograniczenie dostępu dla personelu niemedycznego do zakresu niezbędnego do wykonywanych zadań, tj. tylko do zrealizowanych procedur medycznych u danego pacjenta z wyłączeniem dostępu do jego dokumentacji medycznej. Ponadto w ocenie NIK osoby zatrudnione w Dziale Komercji, Marketingu i Komunikacji Korporacyjnej oraz Dziale Planowania i Analiz nie wykonują czynności pomocniczych przy udzielaniu świadczeń zdrowotnych, w rozumieniu art. 24 ust. 2 pkt 1 ustawy o prawach pacjenta.

   (akta kontroli str. 485-486, 487, 488-491, 664-666, 667-680, 681-684)

2. W wyniku oględzin systemu „HIS"/„EDM" w zakresie nadanych w nim uprawnień 39 kontrolowanym pielęgniarkom i położnym pracującym w Szpitalu ustalono, że dwie osoby posiadały uprawnienia dostępu do więcej niż jednej poradni i oddziału o różnej specjalizacji medycznej[45].

   Prezes Zarządu wyjaśnił, że *niektóre osoby zatrudnione na danym oddziale, posiadają dostęp do więcej niż jednej komórki organizacyjnej zdefiniowanej w systemie „HIS" (…) Taka sytuacja wynika ze sposobu, w jakim od strony technicznej zarządza się prawami dostępu użytkowników w systemie „HIS" i nie świadczy o nadaniu zwykłych praw dostępu do różnych oddziałów Szpitala.*

---

[43] Oględziny prowadzono w zakresie dostępu do danych dla grupy 30 z 106 osób personelu niemedycznego, celem ustalenia uprawnień tych osób, jako użytkowników, w ramach wykonywanych obowiązków służbowych. Uprawnienia w okresie objętym kontrolą nadawane były przez pracownika Działu IT działającego w imieniu ASO.

[44] Dz. U. z 2017 r. poz. 2247; dalej: *rozporządzenie KRI.*

[45] Starsza pielęgniarka mająca dostęp do: Oddziału Dermatologii, Poradni Dermatologicznej i Poradni Leczenia Oparzeń oraz starsza pielęgniarka mająca dostęp do: Oddziału Kardiologii i Chorób Wewnętrznych, Poradni Kardiologicznej, „SOR – Hospitalizacja" oraz Oddziału Płatnego Kardiologii.

Zdaniem NIK, mając na uwadze art. 5 pkt 1 lit. c) RODO oraz § 20 ust. 2 pkt 4 rozporządzenia KRI, zasadne jest ograniczenie dostępu dla pielęgniarek wyłącznie do realizowanych zadań i obowiązków na danym oddziale i/lub poradni Szpitala i zapewnienie bieżącego monitoringu posiadanych uprawnień użytkowników systemu „HIS" w zakresie miejsca pracy personelu medycznego.

(akta kontroli str. 485-486, 487, 492-502, 659-663, 664-666, 667-680)

3. W wyniku oględzin systemu „HIS"/„EDM" w zakresie dostępu dla osób, które przestały być pracownikami Szpitala (po 25 maja 2018 r.), stwierdzono, że w systemie znajdowały się nadal aktywne konta dwóch pracowników, z którymi rozwiązano stosunek pracy po tej dacie (kontrolowana grupa 30 osób). Wiedzy o podstawie dostępu dla tych osób nie posiadali obecni w trakcie oględzin pracownicy Działu IT, przy czym w trakcie kontroli wdrażano nową procedurę zmierzającą do poprawy przepływu komunikacji pomiędzy komórkami organizacyjnymi odpowiedzialnymi za ten zakres działalności Szpitala.

   Prezes Zarządu wyjaśnił, że osoba, która przestaje być pracownikiem Szpitala, może zostać zatrudniona przez jedną z (sześciu) firm zewnętrznych, pracujących na rzecz Szpitala. Dodał, że w przypadku niektórych pracowników, świadczą oni pracę z tytułu zatrudnienia przez te firmy. *Dlatego całkowicie normalną sytuacją jest, że niektórzy obecni lub byli pracownicy mogą posiadać w systemach „HIS" odpowiednie prawa dostępu i odpowiada to faktycznie wypełnianym przez te osoby obowiązkom.*

   Zdaniem NIK, mając na uwadze § 20 ust. 2 pkt 4 i 5 rozporządzenia KRI, zasadne jest zapewnienie prawidłowego obiegu informacji pomiędzy pracownikami Działu IT, nadającymi w imieniu ADO uprawnienia do systemów „HIS" (zawierających dane osobowe pacjentów), a właściwymi ws. zawierania umów o świadczenie pracy i/lub usług medycznych, komórkami organizacyjnymi, w sytuacji kontynowania współpracy ze Szpitalem przez byłych jego pracowników.

   (akta kontroli str. 485-486, 487, 492-502, 503-507, 664-666, 667-680, 685-689)

4. W trakcie oględzin wybranej losowo próby 30 komputerów stwierdzono w dziewięciu przypadkach brak aktualizacji baz sygnatur wirusów w stosowanym oprogramowaniu antywirusowym („K. L.").

   Prezes Zarządu wyjaśnił, że *komputery w Szpitalu są chronione przez zainstalowane oprogramowanie antywirusowe „K. L.", niezależnie od tego, która aktualizacja baz sygnatur wirusów została zainstalowana na danej stacji. Na komputerach stosowanych w Szpitalu bazy sygnatur wirusów są domyślnie aktualizowane, co najmniej raz dziennie. System raportuje problem aktualności baz sygnatur w celu informowania użytkownika* (jak i administratora), *co jednak nie oznacza wyłączenia funkcji ochrony. System antywirusowy jest zarządzany centralnie z serwera administracyjnego i administrator ma pełną kontrolę zarówno nad harmonogramem wykonywania aktualizacji na komputerach użytkowników jak i posiada pełną informację o stanie ochrony antywirusowej na komputerach użytkowników.* Ponadto *d*odał, że *w kwestii sygnalizowania nieaktualności bazy sygnatur* ww. *oprogramowanie antywirusowe jest aktywne, pomimo tego, że kwestie ewentualnych problemów z aktualizacją nie wymagają interwencji użytkownika (ale należą do zadań administratora) oraz nie mają decydującego wpływu na ogólne działanie systemu ochrony antywirusowej. Ponadto cały ruch sieciowy z zewnątrz i na zewnątrz Szpitala jest filtrowany, skanowany i zabezpieczany przez sprzętowy firewall oraz odrębne oprogramowanie antywirusowe „F." działające niezależnie od oprogramowania „K.". Dlatego występowanie na komputerach ostrzeżeń o konieczności aktualizacji bazy sygnatur wirusów nie świadczy o braku ochrony antywirusowej,*

a stosowana w Szpitalu podwójna ochrona antywirusowa jest bardzo skuteczna, czego dowodem jest brak od dawna skutecznych ataków na komputery i dane na nich się znajdujące.

Odnosząc się do wykorzystania w Szpitalu programu antywirusowego („K. L."), pomimo zapisów rezolucji Nr A8-0189/2018 Parlamentu Europejskiego poświęconej cyberbezpieczeństwu, Prezes Zarządu wyjaśnił, że *Szpital oczekuje na wykonanie audytu w Polsce i na zobowiązujące decyzje w tej sprawie. Szpital zastosuje się do wymagań prawnych, jeżeli takie zostaną opublikowane i będą odnosić się do legalności ww. oprogramowania.*

Zdaniem NIK, mając na uwadze § 20 ust. 2 pkt 7 i pkt 9 oraz pkt 12 lit. a) oraz lit. e)-g) rozporządzenia KRI, konieczne jest zapewnienie bieżącej aktualizacji baz sygnatur wirusów, gdyż samo zainstalowanie programu antywirusowego nie stanowi skutecznego zabezpieczenia przy tak szybko zmieniającej się liczbie i rodzaju zagrożeń.

(akta kontroli str. 664-666, 667-680, 690-695)

5. W ramach ww. oględzin stwierdzono, w dziewięciu przypadkach, stosowanie w Szpitalu systemu operacyjnego, dla którego wsparcie techniczne ze strony producenta zakończyło się ponad pięć lat temu. Powyższe oznacza, że producent nie udostępnia: nowych poprawek zabezpieczeń, poprawek niedotyczących zabezpieczeń, bezpłatnego lub płatnego wsparcia technicznego i aktualizacji zawartości technicznej *online*.

   Prezes Zarządu wyjaśnił, że *w Szpitalu jest nadal wykorzystywany system operacyjny (…) z powodów ekonomicznych. Szpital systematycznie wymienia używane komputery na nowe, niemniej jednorazowa wymiana wszystkich starych komputerów jedynie z powodu zaprzestania wsparcia technicznego ze strony producenta danej wersji oprogramowania systemowego nie jest ekonomicznie uzasadniona ani też możliwa. Stare komputery są, więc stopniowo wycofywane z użycia.*

   Zdaniem NIK, mając na uwadze § 20 ust. 2 pkt 12 lit. a)-c) oraz e)-g) rozporządzenia KRI, sytuacja wykorzystywania w Szpitalu systemu operacyjnego, dla którego wsparcie techniczne ze strony producenta zakończyło się ponad pięć lat temu, może stwarzać ryzyko dla bezpieczeństwa infrastruktury IT Szpitala.

   (akta kontroli str. 664-666, 667-680, 690-695)

6. W trakcie ww. oględzin stwierdzono również niestosowanie schematu tworzenia kont użytkowników i sposobów logowania się określonego w PBI skutkującego tym, że:

   1) w 11 przypadkach osoby zatrudnione w Szpitalu logowały się do systemu operacyjnego użytkowanych komputerów przy jednoczesnym użyciu tych samych: loginu i hasła. Stwierdzono także praktykę stosowania tego samego loginu przez personel medyczny na różnych oddziałach.

      Odnosząc się do tych ustaleń Prezes Zarządu wyjaśnił, że *Szpital posiada kilkaset komputerów używanych przez ponad tysiąc użytkowników, dlatego nie jest możliwe w praktyce ręczne zakładanie indywidualnych kont dla każdego użytkownika, tym bardziej, że niektóre komputery są użytkowane przez wiele osób (różnych lekarzy w różnych godzinach). Ten problem zostanie rozwiązany przez wdrożenie zarządzania domenowego (rozwiązanie to jest obecnie w fazie testowania).* Dodał, że *przyjęto w Szpitalu rozwiązanie przejściowe – na komputerach, na których nie przechowuje się lokalnych danych medycznych (np. komputerach w dyżurkach lekarskich) zakładane jest zwykle jedno konto użytkownika („u.") używane przez wszystkich*

użytkowników tego komputera. Zabezpieczenie dostępu do danych zostało przeniesione na poziom logowania do systemu „HIS", gdzie każdy użytkownik posiada własny login i hasło. Nie powoduje to ryzyka ujawnienia danych, ponieważ system „HIS" przechowuje wszystkie dane w bazie danych, a nie lokalnie w komputerze. Natomiast na komputerach użytkowanych indywidualnie, gdzie możliwe jest zapisywanie dokumentów (np. na komputerach w sekretariatach oddziałów) użytkownicy posiadają indywidualne hasło.

Zdaniem NIK taka sytuacja, niezgodna z przyjętą w Szpitalu polityką bezpieczeństwa informacji (część 9.3 pkt 2)-5) Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, stanowiącej załącznik nr 3 do PBI), narusza również § 20 ust. 2 pkt 7 lit. a) i § 21 ust. 2 pkt 3 rozporządzenia w sprawie KRI.

2) hasła użytkowników posiadały różną złożoność (np. cztery litery w jednym przypadku, dwie cyfry w innym przypadku), tj. niezgodnie z przyjętą w Szpitalu polityką bezpieczeństwa informacji (część 9.3 pkt 2)-4) Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych).

   Prezes Zarządu wyjaśnił, że *stwierdzone przypadki używania haseł nie spełniających wymagań, co do złożoności były spowodowane trudnością zarządzania dużą ilością komputerów i niską skutecznością nadzoru przy ręcznym zarządzaniu loginami i hasłami, co opisano powyżej. Szpital zdaje sobie sprawę z konieczności usprawnienia zarządzania loginami i hasłami i dlatego obecnie jest testowane wdrożenie zarządzania domenowego w celu definitywnego rozwiązania tego problemu.*

   Zdaniem NIK taka sytuacja niezgodna z przyjętą w Szpitalu polityką bezpieczeństwa informacji, narusza również § 20 ust. 2 pkt 7 lit. a) i § 21 ust. 2 pkt 3 rozporządzenia w sprawie KRI.

3) dwóch użytkowników (pracowników administracji) miało loginy (różne) w postaci sześciu cyfr, tj. niezgodnie z przyjętą w Szpitalu polityką bezpieczeństwa informacji (część 9.3 pkt 2)-4) Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych).

   Prezes Zarządu wyjaśnił, że *polityka tworzenia kont i nadawania uprawnień nie ogranicza możliwości stosowanych różnych nazw użytkowników (loginów). W przeciwieństwie do polityki haseł, nie ma powodów do wykluczania nazwy użytkownika składającej się z cyfr.*

   PBI przyjęta w Szpitalu (w tym Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych) zobowiązywała osoby, które przetwarzają dane osobowe do posługiwania się własnym identyfikatorem (loginem) i hasłem w celu uzyskania dostępu, tworzenia haseł trudnych do odgadnięcia dla innych oraz zakazywała ujawniania identyfikatora lub hasła współpracownikom. Pouczenie w tym zakresie dla pracowników znajdowało się dodatkowo na stosowanym w Szpitalu upoważnieniu do przetwarzania danych osobowych.

   Zdaniem NIK taka sytuacja niezgodna z przyjętą w Szpitalu polityką bezpieczeństwa informacji, narusza również § 20 ust. 2 pkt 7 lit. a) i § 21 ust. 2 pkt 3 rozporządzenia w sprawie KRI.

   (akta kontroli str. 664-666, 667-680, 690-695, 770-771, 772, 774, 775)

OCENA CZĄSTKOWA W ocenie NIK wdrożone w Szpitalu rozwiązania techniczne i organizacyjne nie zapewniają w pełni prawidłowego przetwarzania i ochrony danych osobowych.

Wprawdzie w okresie objętym kontrolą Szpital w sposób prawidłowy zawarł umowy powierzenia przetwarzania danych, które zawierały wymagane przez RODO postanowienia. Szpital właściwie dokumentował naruszenia ochrony danych osobowych oraz dokonał odpowiedniego zgłoszenia stwierdzonego naruszenia ochrony danych osobowych. W sposób właściwy udostępniano dokumentację medyczną pacjentów oraz podejmowano właściwe działania w celu minimalizacji ryzyka utraty danych osobowych w wyniku awarii, błędów lub nieuprawnionej modyfikacji (w tym podjęto działania celem poprawy infrastruktury technicznej jednej z serwerowni).

Jednak kluczowe ryzyka w tym zakresie wynikają ze stwierdzonych w trakcie kontroli nieprawidłowości:

- dostępu personelu administracyjnego do danych medycznych (dwa przypadki w kontrolowanej próbie 30 osób);
- nieodpowiednich uprawnień personelu medycznego w wykorzystywanych systemach informatycznych (dwa przypadki w kontrolowanej próbie 39 osób);
- aktywnych kont dwóch pracowników, z którymi rozwiązano stosunek pracy w kontrolowanej próbie 30 osób;
- braku aktualizacji baz sygnatur wirusów w stosowanym oprogramowaniu antywirusowym (w dziewięciu przypadkach w kontrolowanej próbie 30) oraz stosowaniu tego oprogramowania, mimo zapisów rezolucji Nr A8-0189/2018 Parlamentu Europejskiego poświęconej cyberbezpieczeństwu;
- stosowania w Szpitalu systemu operacyjnego (w dziewięciu przypadkach w kontrolowanej próbie 30), dla którego zakończyło się ponad pięć lat temu wsparcie techniczne[46];
- niestosowania we wszystkich przypadkach przyjętego w PBI schematu tworzenia kont i sposobów logowania się dla użytkowników.

Za potencjalne ryzyka dla bezpieczeństwa infrastruktury informatycznej Szpitala należy uznać:

- brak dostępu dla osób zatrudnionych na stanowiskach pielęgniarek (sześć przypadków w kontrolowanej próbie) do systemu „HIS" (brak konta użytkownika), co zdaniem NIK wydaje się wątpliwe mając na uwadze zakres obowiązków pielęgniarek w ramach prowadzenia dokumentacji medycznej, przewidziany w opisach stanowisk pracy oraz stosowanie w Szpitalu systemu „HIS";
- nielogowanie się do systemu „HIS" przez pielęgniarki przez ponad cztery lata (trzy przypadki w kontrolowanej próbie) oraz brak konta w tym systemie dla osób wykonujących zawód medyczny i rejestratorek medycznych (pięć przypadków), co zdaniem NIK wydaje się wątpliwe mając na uwadze zakres obowiązków odpowiednio: w ramach prowadzenia dokumentacji medycznej i obsługi systemu „HIS".

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) zapewnienie przeprowadzania szkoleń dla personelu Szpitala uczestniczącego w przetwarzaniu danych osobowych z zakresu bezpieczeństwa danych, w tym RODO;
2) podjęcie działań w celu ograniczenia do niezbędnego zakresu nadawanych uprawnień w systemie „HIS" dla pracowników administracyjnych;

[46] M.in. nie dostarczanie aktualizacji zabezpieczeń, bezpłatnych lub płatnych opcji asystowanej pomocy technicznej i aktualizacji zawartości technicznej online.

3) zapewnienie adekwatności uprawnień użytkowników systemu „HIS” dla pielęgniarek i położnych zaangażowanych w proces przetwarzania danych osobowych pacjentów do realizowanych przez nie zadań i obowiązków;
4) bieżące odbieranie uprawnień do systemu „HIS” dla osób, które przestały być pracownikami Szpitala;
5) zapewnienie bieżącej aktualizacji baz sygnatur wirusów na komputerach użytkowników końcowych;
6) intensyfikację działań zmierzających do wykorzystywania w Szpitalu wyłącznie systemów operacyjnych posiadających wsparcie ze strony producenta;
7) wyeliminowanie możliwości logowania się wbrew zasadom przyjętym w PBI, w szczególności poprzez zintensyfikowanie działań zmierzających do wprowadzenia scentralizowanego i ujednoliconego systemu logowania się do systemów operacyjnych.

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 Krakowie. 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 dni 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.

Kraków, dnia kwietnia 2019 r.

Najwyższa Izba Kontroli

Kontrolerzy:
Paweł Lipowski
specjalista kontroli państwowej

.....
podpis

Małgorzata Korusiewicz
główny specjalista kontroli państwowej

.....

podpis