POLITYKA

bezpieczeństwa przetwarzania danych osobowych
w Samodzielnym Publicznym Zespole Zakładów
Opieki Zdrowotnej w Pionkach

SPIS TREŚCI

Rozdział I
Postanowienia ogólne.

§ 1
Niniejsza „Polityka bezpieczeństwa przetwarzania danych osobowych w Samodzielnym Publicznym Zespole Zakładów Opieki Zdrowotnej w Pionkach**,** zwana dalej Polityką, została opracowana zgodnie z wymogami § 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).

§ 2
Określenia i skróty użyte w Polityce oznaczają:
1. Administrator Danych Osobowych – Samodzielny Publiczny Zespół Zakładów Opieki Zdrowotnej w Pionkach a reprezentuje szpital dyrektor .
2. Inspektor Ochrony Danych – oznacza osobę nadzorującą z upoważnienia Administratora przestrzeganie stosowania środków technicznych i organizacyjnych zapewniających ochronę danych osobowych w sposób odpowiedni do zagrożeń oraz kategorii danych objętych ochroną.
3. Administrator Systemów Informatycznych, zwany dalej ASI – pracownik wyznaczony przez Dyrektora, odpowiedzialny za wdrożenie i stosowanie zasad bezpieczeństwa danych osobowych w zakresie technicznych zabezpieczeń systemu informatycznego,
4. Osoba upoważniona lub użytkownik systemu, zwany dalej użytkownikiem – osoba posiadająca upoważnienie wydane przez Administratora i uprawniona do przetwarzania danych osobowych, w zakresie wskazanym w upoważnieniu.
5. System informatyczny, zwany dalej systemem, w rozumieniu art. 7 pkt 2a) Ustawy.
6. Zabezpieczenie danych w systemie, zwane dalej zabezpieczeniem – czynności wykonywane w rozumieniu art. 7 pkt 2b) Ustawy.
7. Wewnętrzna sieć teleinformatyczna – sieć Administratora, łącząca co najmniej dwa indywidualne stanowiska komputerowe, umożliwiająca użytkownikom określony dostęp do przetwarzania danych.

Rozdział II

Deklaracja intencji, cele i zakres polityki bezpieczeństwa.

§ 3

Administrator wyraża pełne zaangażowanie dla zapewnienia bezpieczeństwa przetwarzanych danych osobowych oraz wsparcie dla przedsięwzięć technicznych i organizacyjnych związanych z ochroną danych osobowych.

§ 4
1. Polityka określa podstawowe zasady bezpieczeństwa i zarządzania bezpieczeństwem systemów.
2. Polityka dotyczy wszystkich danych osobowych, przetwarzanych w szpitalu, niezależnie od formy ich przetwarzania (zbiory ewidencyjne, systemy informatyczne) oraz od tego czy dane są lub mogą być przetwarzane w zbiorach danych.
3. Polityka ma zastosowanie wobec wszystkich komórek organizacyjnych szpitala.

§ 5

Celem Polityki jest ochrona danych osobowych, przetwarzanych w szpitalu, przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów określających zasady postępowania przy przetwarzaniu danych osobowych oraz przed zmianą, uszkodzeniem lub zniszczeniem.

§ 6

1. Cele Polityki realizowane są poprzez zapewnienie danym osobowym następujących cech:

a. poufności — właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom;
b. integralności — właściwości zapewniającej, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
c. rozliczalności — właściwości zapewniającej, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

2. Za osobę nieupoważnioną uważa się osobę, która nie otrzymała zgody administratora na udostępnienie mu danych osobowych w trybie i na zasadach określonych w RODO oraz osobę nieposiadającą upoważnienia do przetwarzania danych osobowych, nadanego przez administratora w trybie wynikającym z RODO.

§ 7

Dla skutecznej realizacji Polityki Administrator zapewnia:

1. odpowiednie do zagrożeń i kategorii danych objętych ochroną, środki techniczne i rozwiązania organizacyjne;
2. szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony;
3. okresowe szacowanie ryzyka zagrożeń dla zbiorów danych;
4. monitorowanie zastosowanych środków ochrony.

§8

Administrator zapewnia zgodność niniejszej Polityki z przepisami określającymi zasady przetwarzania danych osobowych, tj:

- Rozporządzeniem Parlamentu Europejskiego i Rady Europy (RODO)
- ustawą z 10 maja 2018 r. o ochronie danych osobowych
- rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024);

Rozdział III
Obowiązki i odpowiedzialność w zakresie zarządzania bezpieczeństwem.

§ 9

1. Zarządzanie bezpieczeństwem systemów jest procesem ciągłym, realizowanym przy współdziałaniu osób upoważnionych do przetwarzania danych z IOD i ASI.

2. Wszystkie osoby upoważnione do przetwarzania danych zobowiązane są do:
    a. przetwarzania danych osobowych zgodnie z obowiązującymi przepisami;
    b. postępowania zgodnie z ustaloną przez Administratora Polityką oraz z:

- „Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w szpitalu";
- „Instrukcją organizacji i przetwarzania danych osobowych w szpitalu".

3. W przypadku naruszenia przepisów lub zasad postępowania, osoba upoważniona do przetwarzania danych osobowych podlega odpowiedzialności służbowej i karnej.

§ 10

1. Do obowiązków IOD należy nadzorowanie przestrzegania zasad ochrony, określonych w dokumentacji opisującej sposób przetwarzania danych oraz zastosowane środki ochrony.
2. Osoby upoważnione przez Administratora do przetwarzania danych osobowych, zobowiązane są do:

    a. ścisłego przestrzegania zakresu udzielonego upoważnienia;
    b. zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
    c. zgłaszania IOD incydentów związanych z naruszeniem bezpieczeństwa danych oraz niewłaściwego funkcjonowania systemu, a także informowania IOD o przypadkach naruszenia bezpieczeństwa danych.

Rozdział IV
Obszary przetwarzania danych.

§ 11

1. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe w komórkach organizacyjnych szpitala jest prowadzony przez IOD.
2. Za obszar przetwarzania danych należy rozumieć obszar, w którym wykonywana jest choćby jedna z czynności wchodzących w zakres pojęcia „przetwarzanie danych osobowych „

Rozdział V

Wykaz zbiorów danych oraz programów zastosowanych do przetwarzania danych osobowych.

§ 12

Wykaz zbiorów danych oraz programów zastosowanych do przetwarzania danych osobowych w komórkach organizacyjnych szpitala jest prowadzony przez IOD a w zakresie elektronicznego przetwarzania również przez ASI.

Rozdział VI

Struktury zbiorów danych oraz przepływ danych pomiędzy systemami.

§ 13

W szpitalu dane osobowe mogą być przetwarzane w zbiorach danych, przy zastosowaniu systemów informatycznych oraz zbiorów ewidencyjnych w postaci kartotek, skorowidzów, ksiąg i wykazów.

§ 14

1. Zawartość pól informacyjnych, występujących w systemach zastosowanych w celu przetwarzania danych osobowych, musi być zgodna z przepisami prawa, które uprawniają lub zobowiązują Administratora do przetwarzania danych osobowych.
2. Na żądanie Administratora lub IOD, kierownik komórki organizacyjnej szpitala lub inna osoba wskazana przez Administratora, zobowiązany jest wskazać podstawy prawne określające zakres przetwarzanych danych osobowych.

§ 15

Na żądanie Administratora lub IOD, ASI zobowiązany jest do wskazania powiązań między polami informacyjnymi, które zawierają dane osobowe w systemie.

§ 16

1. Przepływ danych, pomiędzy systemami zastosowanymi w celu przetwarzania danych osobowych, może odbywać się w postaci przepływu jednokierunkowego lub przepływu dwukierunkowego.
2. Przepływ jednokierunkowy oznacza, że system informatyczny udostępnia dane ze zbioru (bazy) danych tylko w trybie „do odczytu”.
3. Przepływ dwukierunkowy umożliwia upoważnionemu użytkownikowi korzystanie z danych w trybach „do odczytu” i „do zapisu”, tj. umożliwia wprowadzanie nowych danych i modyfikację istniejących.

§ 17

Przesyłanie danych pomiędzy systemami może odbywać się sposób manualny, przy wykorzystaniu nośników zewnętrznych (np. dyskietka, CD, DVD, taśma streamera, dysk wymienny, Pen Drive itp.) lub w sposób półautomatyczny, przy wykorzystaniu funkcji eksportu/ importu danych za pomocą teletransmisji (np. poprzez wewnętrzną sieć teleinformatyczną).

Rozdział VII
Środki ochrony.

§ 18

1. Administrator zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.
2. Kierownicy komórek organizacyjnych szpitala lub inne osoby wskazane przez Administratora, przeprowadzają okresową analizę ryzyka dla poszczególnych systemów i na tej podstawie przedstawiają Administratorowi propozycje w zakresie zastosowania środków technicznych i organizacyjnych (środków ochrony), celem zapewnienia ochrony przetwarzanych danych.
3. Analiza ryzyka obejmuje:

a. identyfikację występujących zagrożeń dla systemów i zbiorów danych;
b. określenie wielkości ryzyka, tj. prawdopodobieństwa, że określone zagrożenie wykorzysta podatność (słabość) zasobu;
c. identyfikację obszarów wymagających zabezpieczeń.

4. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów i zbiorów danych osobowych.

§ 19

1. Środki ochrony, zastosowane przez Administratora dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych, obejmują:

a. środki fizyczne;
b. środki osobowe;
c. środki techniczne.

2. Środki ochrony fizycznej obejmują:

a. lokalizację miejsc przetwarzania danych osobowych w pomieszczeniach o ograniczonym i kontrolowanym dostępie;
b. ustalenie zasad pobierania kluczy do pomieszczeń i szaf;
c. wyposażenie pomieszczeń, w których przetwarzane są dane osobowe, we wzmocnione drzwi i okna;
d. składowanie zbiorów danych osobowych (w tym nośników wymiennych i nośników kopii zapasowych) w odpowiednio zabezpieczonych szafach.
e. zabezpieczenie pomieszczeń systemem alarmowym, umowa z firmą ochrony mienia.

3. Środki ochrony osobowej obejmują:

a. dopuszczenie do przetwarzania danych osobowych wyłącznie osób posiadających upoważnienie wydane przez Administratora;
b. zapoznanie tych osób z zasadami przetwarzania danych osobowych oraz obsługą systemu służącego do przetwarzania danych;
c. odebranie stosownych zobowiązań i oświadczeń; tj.: zobowiązania do zachowania w tajemnicy danych i sposobów ich zabezpieczenia oraz oświadczenia o zapoznaniu z treścią przepisów określających zasady postępowania przy przetwarzaniu danych osobowych, a także z dokumentacją opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ich ochronę.

4. Środki ochrony technicznej obejmują:

a. mechanizmy kontroli dostępu do systemów i zasobów;
b. zastosowanie odpowiednich i regularnie aktualizowanych narzędzi ochronnych (programy antywirusowe, „ściany ogniowe”, itp.);
c. regularne tworzenie kopii zapasowych zbiorów danych przetwarzanych w systemach informatycznych;
d. zastosowanie ochrony zasilania -UPS.

§ 20

Uwzględniając kategorie przetwarzanych danych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka dla poszczególnych systemów, ustala się podstawowy poziom bezpieczeństwa.

§ 21

System informatyczny, któremu przypisano poziom bezpieczeństwa wymieniony w § 20 ust. 1, spełniać musi wymagania wymienione w załączniku do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).