POLITYKA BEZPIECZEŃSTWA INFORMACJI

w

Podmiocie leczniczym:

Centrum Rehabilitacji im. Prof. Mieczysława Walczaka w Osiecznej, ul. Zamkowa 2, 64-113 Osieczna, KRS 0000012233, NIP 6971885702, REGON 410386551

Niniejsza Polityka Bezpieczeństwa, zwana dalej Polityką, została sporządzona w celu wykazania, że dane osobowe są przetwarzane i zabezpieczone zgodnie z wymogami prawa, dotyczącymi zasad przetwarzania i zabezpieczania danych w podmiotach leczniczych, w tym Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

Definicje

1. Administrator danych: Centrum Rehabilitacji im. Prof. Mieczysława Walczaka w Osiecznej, ul. Zamkowa 2, 64-113 Osieczna, KRS 0000012233, NIP 6971885702, REGON 410386551
2. Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
3. System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji, narzędzi programowych zastosowanych w celu przetwarzania danych,
4. Użytkownik – osoba upoważniona przez Administratora do przetwarzania danych osobowych,
5. Zbiór danych – każdy uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów,
6. Przetwarzanie danych – jakiekolwiek operacje wykonywane na Danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie w formie tradycyjnej oraz w systemach informatycznych,
7. Identyfikator użytkownika – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym (Użytkownika) w razie Przetwarzania danych osobowych w takim systemie,
8. Hasło – ciąg znaków literowych, cyfrowych lub innych, znanych jedynie osobie uprawnionej do pracy w systemie informatycznym (Użytkownikowi) w razie przetwarzania danych osobowych w takim systemie,
9. Uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu (użytkownika).

I. Postanowienia ogólne

1. Polityka dotyczy wszystkich Danych osobowych przetwarzanych w podmiocie leczniczym, niezależnie od formy ich przetwarzania (przetwarzane tradycyjnie zbiory ewidencyjne w formie papierowej, systemy informatyczne – dane w formie elektronicznej) oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych.
2. Polityka jest przechowywana w siedzibie Administratora w wersji papierowej oraz w wersji elektronicznej.
3. Polityka jest udostępniana do wglądu osobom posiadającym upoważnienie do przetwarzania danych osobowych na ich wniosek, a także osobom, którym ma zostać nadane upoważnienie do przetwarzania danych osobowych, celem zapoznania się z jej treścią.
4. Dane osobowe przetwarzane w podmiocie leczniczym, a uzyskane w związku z udzielaniem świadczeń zdrowotnych, objęte są tajemnicą lekarza/pielęgniarki
5. W zakresie przetwarzania danych pozyskanych w związku z wykonywaniem czynności objętych tajemnicą lekarską, Administrator stosuje się do przepisów dotyczących zachowania tajemnicy zawodowej.
6. Dla skutecznej realizacji Polityki, Administrator Danych zapewnia:
   a) odpowiednie do zagrożeń i kategorii danych objętych ochroną środki techniczne i rozwiązania organizacyjne,
   b) kontrolę i nadzór nad Przetwarzaniem danych osobowych,
   c) monitorowanie zastosowanych środków ochrony.

7. Monitorowanie przez Administratora Danych zastosowanych środków ochrony obejmuje m.in. działania użytkowników, naruszanie zasad dostępu do danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.
8. Administrator danych zapewnia, że czynności wykonywane w związku z przetwarzaniem i zabezpieczeniem danych osobowych są zgodne z niniejszą polityką oraz odpowiednimi przepisami prawa.

II. Dane osobowe przetwarzane u administratora danych

1. Dane osobowe przetwarzane przez Administratora Danych gromadzone są w zbiorach danych.
2. Administrator danych nie podejmuje czynności przetwarzania, które mogłyby się wiązać z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka dla praw i wolności osób. W przypadku planowania takiego działania Administrator wykona czynności określone w art. 35 i nast. RODO.
3. W przypadku planowania nowych czynności przetwarzania, Administrator dokonuje analizy ich skutków dla ochrony danych osobowych oraz uwzględnia kwestie ochrony danych w fazie ich projektowania.
4. Administrator danych prowadzi rejestr czynności przetwarzania. Wzór rejestru czynności przetwarzania stanowi Załącznik nr 1 do niniejszej polityki.

III. Obowiązki i odpowiedzialność w zakresie zarządzania bezpieczeństwem

1. Wszystkie osoby zobowiązane są do przetwarzania danych osobowych zgodnie z obowiązującymi przepisami i zgodnie z ustaloną przez Administratora Danych Polityką Bezpieczeństwa Informacji, a także innymi dokumentami wewnętrznymi i procedurami związanymi z Przetwarzaniem danych osobowych w podmiocie leczniczym.
2. Wszystkie dane osobowe w podmiocie leczniczym są przetwarzane z poszanowaniem zasad przetwarzania przewidzianych przez przepisy prawa:
   a) w każdym wypadku występuje chociaż jedna z przewidzianych przepisami prawa podstaw dla przetwarzania danych,
   b) dane są przetwarzane rzetelnie i w sposób przejrzysty,
   c) dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami,
   d) dane osobowe są przetwarzane jedynie w takim zakresie, jaki jest niezbędny dla osiągnięcia celu przetwarzania danych,
   e) dane osobowe są prawidłowe i w razie potrzeby uaktualnione,
   f) czas przechowywania danych jest ograniczony do okresu ich przydatności do celów, do których zostały zebrane, a po tym okresie są one anonimizowane bądź usuwane,
   g) wobec osoby, której dane dotyczą, wykonywany jest obowiązek informacyjny, zgodnie z treścią art. 13 i 14 RODO,
   h) dane są zabezpieczone przed naruszeniami zasad ich ochrony.
3. Administrator danych nie przekazuje osobom, których dane dotyczą, informacji w sytuacji, w której dane te muszą zostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej (art. 14 ust. 5 pkt d RODO)
4. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony Danych osobowych uważa się w szczególności:
   a) naruszenie bezpieczeństwa Systemów informatycznych, w których przetwarzane są dane osobowe, w razie ich przetwarzania w takich systemach,
   b) udostępnianie lub umożliwienie udostępniania danych osobom lub podmiotom do tego nieupoważnionym,
   c) zaniechanie, choćby nieumyślne dopełnienia obowiązku zapewnienia danym osobowym ochrony,
   d) niedopełnienie obowiązku zachowania w tajemnicy Danych osobowych oraz sposobów ich zabezpieczenia,
   e) przetwarzanie danych osobowych niezgodnie z założonym zakresem i celem ich zbierania,
   f) spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nieuprawnione kopiowanie danych osobowych,
   g) naruszanie praw osób, których dane są przetwarzane.
5. W przypadku stwierdzenia okoliczności naruszenia zasady ochrony danych osobowych, użytkownik zobowiązany jest do podjęcia wszystkich niezbędnych kroków, mających na celu ograniczenie skutków naruszenia i do niezwłocznego powiadomienia Administratora Danych.

6. Do obowiązków Administratora Danych w zakresie zatrudniania, zakończenia lub zmiany warunków zatrudnienia pracowników lub współpracowników (osób podejmujących czynności na rzecz Administratora Danych na podstawie innych umów cywilnoprawnych) należy nadzór, by:
   a) pracownicy byli odpowiednio przygotowani do wykonywania swoich obowiązków,
   b) każdy z przetwarzających Dane osobowe był pisemnie upoważniony do przetwarzania zgodnie z „Upoważnieniem do przetwarzania danych osobowych" - wzór Upoważnienia stanowi Załącznik nr 2 do niniejszej Polityki Bezpieczeństwa,
   c) każdy pracownik zobowiązał się do zachowania danych osobowych przetwarzanych w podmiocie leczniczych w tajemnicy. „Oświadczenie i zobowiązanie osoby przetwarzającej dane osobowe do zachowania tajemnicy" stanowi element „Upoważnienia do przetwarzania danych osobowych"
7. Pracownicy zobowiązani są do:
   a) ścisłego przestrzegania zakresu nadanego upoważnienia,
   b) przetwarzania i ochrony danych osobowych zgodnie z przepisami,
   c) zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia,
   d) zgłaszania incydentów związanych z naruszeniem bezpieczeństwa danych oraz niewłaściwym funkcjonowaniem systemu.

IV. Obszar przetwarzania danych osobowych

1. Obszar, w którym przetwarzane są dane osobowe w formie papierowej i elektronicznej w systemach informatycznych na terenie podmiotu leczniczego obejmuje:
   1) Szpital Rehabilitacyjny, w ramach którego działają:
      a) Oddział Rehabilitacyjny,
      b) Dział Farmacji,
   2) Ambulatorium:
      a) Oddział dzienny rehabilitacji ogólnoustrojowej,
      b) Poradnia rehabilitacyjna,
   1) pion kierowniczy, na który składają się:
      a) dyrektor,
      b) zastępca dyrektora ds. medycznych,
      c) zastępca dyrektora ds. pielęgniarstwa i administracji,
      d) główny księgowy,
      e) kierownik rehabilitacji,
      f) przełożona pielęgniarek
   2) komórki organizacyjne prowadzące obsługę administracyjną:
      a) sekcja administracyjno-gospodarcza,
      b) sekcja ekonomiczno-finansowa
   3) samodzielne stanowiska pracy:
      a) statystyk medyczny,
      b) sekretariat i sprawy pracownicze,
      c) dietetyk,

Obszary przetwarzania danych osobowych zlokalizowane są przy ul. Zamkowej 2, 64-113 Osieczna.

V. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Administrator Danych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.
2. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych.
3. Środki obejmują:

a) ograniczenie dostępu do pomieszczeń i obszarów, w których przetwarzane są dane osobowe, jedynie do osób odpowiednio upoważnionych. Inne osoby mogą przebywać w pomieszczeniach i obszarach wykorzystywanych do przetwarzania danych jedynie w towarzystwie osoby upoważnionej,

b) zamykanie pomieszczeń tworzących obszar Przetwarzania danych osobowych określony w pkt. IV powyżej na czas nieobecności pracowników, w sposób uniemożliwiający dostęp do nich osób trzecich,
c) wykorzystanie niszczarki do skutecznego usuwania dokumentów zawierających dane osobowe,
d) ochronę sieci lokalnej przed działaniami inicjowanymi z zewnątrz przy użyciu sieci firewall,
e) wykonywanie kopii awaryjnych danych,
f) ochronę sprzętu komputerowego wykorzystywanego u administratora przed złośliwym oprogramowaniem,
g) zabezpieczenie dostępu do urządzeń przy pomocy haseł dostępu,
h) wykorzystanie szyfrowania danych przy ich transmisji.

VI. Naruszenia zasad ochrony danych osobowych

1. W przypadku stwierdzenia naruszenia ochrony danych osobowych Administrator dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.
2. W każdej sytuacji, gdy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator zgłasza fakt naruszenia zasad ochrony danych organowi nadzorczemu bez zbędnej zwłoki – jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Wzór zgłoszenia określa załącznik Nr 3 do niniejszej polityki.
3. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator zawiadamia o incydencie także osobę, której dane dotyczą.

VII. Powierzenie przetwarzania danych osobowych

Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO i tylko jeżeli są to dane, które może ujawnić bez naruszenia lekarskiej/pielęgniarskiej tajemnicy zawodowej.

VIII. Przekazywanie danych do państwa trzeciego

Administrator Danych Osobowych nie będzie przekazywał danych osobowych do państwa trzeciego, poza sytuacjami w których następuje to na wniosek osoby, której dane te dotyczą.

IX. Postanowienia końcowe

1. Za niedopełnienie obowiązków wynikających z niniejszego dokumentu pracownik ponosi odpowiedzialność na podstawie kodeksu pracy, Przepisów o ochronie danych osobowych oraz Kodeksu karnego w odniesieniu do danych osobowych objętych tajemnicą zawodową.
2. Odpowiedzialność Zleceniobiorcy w tym zakresie wynika z kodeksu cywilnego, Przepisów o ochronie danych osobowych oraz Kodeksu karnego w odniesieniu do danych osobowych objętych tajemnicą zawodową.
3. Integralną część niniejszej Polityki bezpieczeństwa stanowią następujące Załączniki: