ŁÓDZKIE CENTRUM FIZJOTERAPII

POLITYKA OCHRONY DANYCH OSOBOWYCH

dla Podmiotu Leczniczego

Numer dokumentu: RODO-01/2026 | Wersja 1.0

Data wejścia w życie: 01.09.2026

Administrator: Łódzkie Centrum Fizjoterapii spółka z ograniczoną odpowiedzialnością

Zakład leczniczy: Łódzkie Centrum Fizjoterapii

Adres / miejsca przetwarzania: Zielona 29, 90-602 Łódź

Numer księgi rejestrowej RPWDL: 000000307184

Zatwierdził: Kierownik Podmiotu Leczniczego.

Rozdział I. Postanowienia ogólne

§1. Cel i charakter Polityki

1. Polityka określa system zarządzania ochroną danych osobowych przez Administratora prowadzącego działalność leczniczą, w tym zasady legalności, rozliczalności, bezpieczeństwa, realizacji praw osób, zarządzania dostępem, podmiotami zewnętrznymi, ryzykiem i naruszeniami.

2. Politykę stosuje się łącznie z Regulaminem Organizacyjnym RO-01/2026, Standardami Ochrony Małoletnich oraz procedurami PO-01/2026–PO-14/2026. Dokumenty wykonawcze nie mogą rozszerzać dostępu do danych ani uprawnień zawodowych ponad przepisy prawa i rzeczywistą rolę danej osoby.

3. Polityka nie zastępuje przepisów o prawach pacjenta, tajemnicy zawodowej, dokumentacji medycznej ani systemie informacji w ochronie zdrowia. W razie rozbieżności stosuje się przepisy bezwzględnie obowiązujące i rozwiązanie zapewniające wyższy poziom ochrony praw pacjenta.

§2. Podstawy prawne

Politykę opracowano w szczególności z uwzględnieniem:

- rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO);
- ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych;
- ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej;
- ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta;
- ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia – tekst jednolity ogłoszony w 2026 r.;
- rozporządzenia Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie dokumentacji medycznej, z uwzględnieniem zmian obowiązujących od 1 lipca 2026 r.;
- przepisów regulujących zawody medyczne, tajemnice zawodowe, monitoring, rachunkowość, zatrudnienie, cyberbezpieczeństwo i świadczenie usług drogą elektroniczną – w zakresie mającym zastosowanie.

§3. Zakres podmiotowy

1. Polityka obowiązuje wszystkie osoby działające z upoważnienia Administratora albo mające dostęp do danych, niezależnie od podstawy zatrudnienia lub współpracy, w tym pracowników, osoby wykonujące zawody medyczne, rejestrację, administrację, osoby rozliczające, praktykantów, studentów, stażystów, wolontariuszy i podwykonawców – w zakresie ich rzeczywistej roli.

2. Osoba prowadząca zajęcia rekreacyjne, trening funkcjonalny, usługi organizacyjne albo inne usługi niemedyczne nie uzyskuje z tego tytułu dostępu do dokumentacji medycznej ani pełnych danych o zdrowiu. Dostęp może obejmować wyłącznie informacje niezbędne do bezpiecznego wykonania konkretnej czynności i wymaga udokumentowanej podstawy oraz zakresu.

§4. Definicje

Ilekroć w Polityce mowa o:

- Administratorze – rozumie się pełną firmę albo nazwę podmiotu wskazanego w metryce, który ustala cele i sposoby przetwarzania danych;
- Podmiocie – rozumie się podmiot leczniczy i zakład leczniczy opisane w Regulaminie Organizacyjnym, odpowiednio do kontekstu;
- danych o zdrowiu – rozumie się dane dotyczące zdrowia fizycznego lub psychicznego, w tym dane ujawniające informacje o stanie zdrowia i korzystaniu ze świadczeń;
- dokumentacji medycznej – rozumie się dokumentację prowadzoną i udostępnianą na zasadach prawa medycznego; nie każdy dokument elektroniczny jest EDM w znaczeniu ustawowym;
- IOD – rozumie się inspektora ochrony danych, jeżeli został wyznaczony;
- naruszeniu – rozumie się naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utraty, zmodyfikowania, nieuprawnionego ujawnienia lub dostępu do danych;
- odbiorcy – rozumie się osobę lub podmiot, któremu ujawnia się dane, z wyłączeniami wynikającymi z RODO;
- podmiocie przetwarzającym – rozumie się podmiot przetwarzający dane w imieniu Administratora na podstawie art. 28 RODO.

Rozdział II. Administrator, odpowiedzialność i rozliczalność

§5. Administrator i Kierownik

1. Administratorem jest podmiot posiadający podmiotowość prawną i ustalający cele oraz sposoby przetwarzania; Kierownik wykonuje w jego imieniu obowiązki organizacyjne w granicach umocowania. Nie utożsamia się automatycznie Administratora z nazwą placówki, komórką organizacyjną ani dostawcą systemu.

2. Kierownik zapewnia zasoby, podział odpowiedzialności, dokumentowanie decyzji, przeglądy uprawnień, szkolenia, obsługę naruszeń, realizację praw, ocenę dostawców, ciągłość działania i okresową weryfikację zgodności z Regulaminem Organizacyjnym.

3. Właściciele procesów odpowiadają za prawidłowe opisanie celu, zakresu danych, odbiorców, okresu retencji, systemów, zagrożeń i zabezpieczeń w rejestrze czynności przetwarzania.

§6. Inspektor ochrony danych

1. Kierownik dokumentuje ocenę, czy zachodzą przesłanki obowiązkowego wyznaczenia IOD, w szczególności ze względu na główną działalność polegającą na przetwarzaniu na dużą skalę danych o zdrowiu. Ocena uwzględnia liczbę pacjentów, wolumen i różnorodność danych, czas, zasięg geograficzny, charakter monitorowania oraz profil ryzyka.

2. Jeżeli IOD zostanie wyznaczony, Administrator zapewnia jego niezależność, bezpośrednie raportowanie najwyższemu kierownictwu, brak konfliktu interesów, dostęp do informacji i zasobów oraz publikuje i zgłasza jego dane zgodnie z prawem.

3. IOD doradza i monitoruje zgodność, lecz nie przejmuje od Administratora odpowiedzialności za decyzje dotyczące celów, podstaw, środków bezpieczeństwa, zgłoszeń naruszeń ani akceptacji ryzyka.

§7. Rejestry i dokumentacja rozliczalności

Administrator prowadzi i aktualizuje co najmniej:

- rejestr czynności przetwarzania, a gdy działa jako podmiot przetwarzający – także rejestr kategorii czynności;
- ewidencję upoważnień i dostępów, wykaz systemów i zasobów informacyjnych;
- rejestr podmiotów przetwarzających, odbiorców i – jeżeli występują – współadministratorów;
- rejestr naruszeń, żądań osób, udostępnień dokumentacji medycznej i skarg dotyczących prywatności;
- rejestr ryzyk, ocen skutków dla ochrony danych, testów równowagi i ocen transferów poza EOG;
- harmonogram retencji, protokoły usuwania oraz dowody szkoleń, audytów, przeglądów i działań naprawczych.

Dokumentacja musi odzwierciedlać rzeczywiste procesy. Sam fakt posiadania formularza, umowy lub zgody nie stanowi dowodu zgodności, jeżeli organizacja działa inaczej.

ŁÓDZKIE CENTRUM FIZJOTERAPII

Rozdział III. Cele, podstawy i zasady przetwarzania

§8. Zasady RODO

Zasady określone w art. 5 RODO stosuje się łącznie. Każdy proces musi posiadać zdefiniowany cel, podstawę prawną dla danych zwykłych i – gdy dotyczy – warunek z art. 9 RODO, minimalny zakres, regułę dostępu, okres przechowywania, sposób realizacji obowiązku informacyjnego i adekwatne zabezpieczenia.

§9. Główne procesy i podstawy

1. W ramach działalności leczniczej dane są przetwarzane w szczególności w celu rejestracji, identyfikacji pacjenta, kwalifikacji, udzielania i dokumentowania świadczeń, zachowania ciągłości opieki, rozliczeń, udostępniania dokumentacji, realizacji praw pacjenta, bezpieczeństwa i jakości oraz obowiązków publicznoprawnych.

2. Podstawę przetwarzania ustala się odrębnie dla każdego celu. W procesie leczenia co do zasady nie opiera się przetwarzania danych niezbędnych do świadczenia zdrowotnego na zgodzie RODO, jeżeli właściwą podstawę stanowi obowiązek prawny, umowa lub art. 9 ust. 2 lit. h RODO wraz z prawem krajowym.

3. Zgoda jest wykorzystywana tylko tam, gdzie jest dobrowolna, konkretna, świadoma i możliwa do wycofania bez negatywnych skutków dla świadczenia, w szczególności dla nieobowiązkowego marketingu, publikacji wizerunku albo dodatkowego wykorzystania fotografii. Zgoda na świadczenie zdrowotne i zgoda RODO są odrębnymi instytucjami.

4. Dane pracowników, kandydatów, kontrahentów, osób kontaktowych, uczestników usług niemedycznych i użytkowników strony internetowej przetwarza się na odrębnych, udokumentowanych podstawach, adekwatnych do celu.

§10. Minimalizacja i prawidłowość

1. Rejestracja nie prowadzi pełnego wywiadu medycznego. Informacje o stanie zdrowia przyjmuje wyłącznie w zakresie koniecznym do właściwego skierowania zgłoszenia lub rozpoznania sytuacji wymagającej pilnej reakcji, zgodnie z PO-01/2026.

2. Nie kopiuje się dokumentów tożsamości ani nie utrwala pełnych numerów dokumentów, chyba że wyraźny przepis lub szczególna, udokumentowana potrzeba prawna tego wymaga.

3. Dane kontaktowe weryfikuje się z pacjentem. Treść przypomnień o wizycie i komunikacji organizacyjnej nie może ujawniać rozpoznania ani wrażliwego rodzaju świadczenia osobie postronnej.

4. Automatycznie kopiowane szablony, listy odbiorców i rekordy pacjentów podlegają weryfikacji. Scalanie lub rozdzielanie rekordów wykonuje się zgodnie z procedurą i z zachowaniem historii zmian.

§11. Obowiązek informacyjny

Administrator przekazuje informacje wymagane art. 13 lub 14 RODO w sposób warstwowy, zwięzły i zrozumiały, najpóźniej w terminie przewidzianym prawem. Klauzule są dostosowane do konkretnego procesu i nie mogą zastępować informacji o prawach pacjenta ani informacji medycznej.

Dowód realizacji obowiązku informacyjnego może wynikać z systemu, formularza, potwierdzenia elektronicznego, oznaczenia wersji klauzuli lub udokumentowanego sposobu jej udostępnienia; nie wymaga się rutynowo podpisu pacjenta, jeżeli przepisy tego nie nakazują.

Rozdział IV. Dane o zdrowiu, tajemnica i dokumentacja medyczna

§12. Dane szczególnych kategorii

Dane o zdrowiu, dane genetyczne i biometryczne wykorzystywane do jednoznacznej identyfikacji przetwarza się wyłącznie przy istnieniu podstawy z art. 6 RODO oraz właściwego wyjątku z art. 9 ust. 2 RODO. Zakres dostępu wynika z roli w konkretnym procesie opieki, a nie wyłącznie ze stanowiska, zatrudnienia w placówce lub technicznej możliwości wglądu.

§13. Tajemnica zawodowa i poufność

1. Obowiązki RODO nie zastępują tajemnic zawodowych i tajemnicy informacji związanych z pacjentem. Ujawnienie wymaga jednocześnie podstawy prawnej, uprawnionego odbiorcy, właściwego celu i ograniczenia zakresu.

2. Rozmowy, konsultacje interdyscyplinarne, teleporady i przekazywanie zaleceń prowadzi się w warunkach poufności. Nie omawia się pacjentów w przestrzeni ogólnodostępnej ani w obecności osób, których udział nie jest niezbędny.

3. Obowiązek poufności trwa po zakończeniu współpracy. Ustanie dostępu technicznego nie zwalnia z tajemnicy.

§14. Dokumentacja medyczna

1. Dokumentacja medyczna jest prowadzona, korygowana, przechowywana i zabezpieczana zgodnie z PO-03/2026 oraz aktualnymi przepisami. Dane w dokumentacji nie mogą być usuwane lub modyfikowane w sposób zacierający pierwotny wpis i historię zmian.

2. Fotografie wykonywane dla celu diagnostycznego lub dokumentacyjnego stanowią część dokumentacji medycznej, jeżeli spełniają wymagania przyporządkowania, integralności i retencji. Wykorzystanie fotografii do edukacji, nauki, promocji lub publikacji wymaga odrębnej analizy podstawy, anonimizacji albo wyraźnego zezwolenia – zgodnie z PO-04/2026.

3. Dane o świadczeniu przekazywane płatnikowi, zakładowi ubezpieczeń, operatorowi pakietu lub pracodawcy ogranicza się do zakresu wynikającego z prawa i umowy. Samo finansowanie świadczenia nie daje prawa do pełnej dokumentacji ani informacji o stanie zdrowia – zgodnie z PO-05/2026.

Rozdział V. Upoważnienia i zarządzanie dostępem

§15. Zasady nadawania dostępu

1. Dostęp nadaje się według zasady najmniejszych uprawnień, potrzeby wiedzy i rozdzielenia obowiązków. Upoważnienie wskazuje kategorie danych, osoby, operacje, systemy, komórkę, okres i ograniczenia. Dostęp techniczny musi odpowiadać treści upoważnienia.

2. Każdy użytkownik posiada indywidualny identyfikator. Kont wspólnych nie stosuje się, chyba że wyjątkowa właściwość urządzenia uniemożliwia inne rozwiązanie; wówczas wdraża się dodatkową identyfikowalność i plan usunięcia wyjątku.

3. Dostęp nadaje się przed rozpoczęciem czynności, zmienia niezwłocznie po zmianie roli i odbiera najpóźniej z chwilą ustania potrzeby. Obejmuje to system medyczny, pocztę, dyski, aplikacje, pomieszczenia, klucze, urządzenia i zdalny dostęp.

4. Uprawnienia są przeglądane okresowo oraz po zmianach organizacyjnych, długiej nieobecności, incydencie lub zmianie dostawcy. Konta nieaktywne blokuje się zgodnie z oceną ryzyka.

§16. Obowiązki użytkowników

Użytkownik nie udostępnia danych ani danych uwierzytelniających osobom nieuprawnionym, blokuje urządzenie przy odejściu, weryfikuje adresata i załączniki, nie używa prywatnych skrzynek, chmur i komunikatorów, nie wykonuje nieuprawnionych kopii, fotografii lub zrzutów ekranu oraz nie wynosi dokumentacji i nośników bez udokumentowanej potrzeby i zabezpieczenia.

Zgoda Kierownika nie legalizuje czynności sprzecznej z prawem, tajemnicą zawodową albo zasadą minimalizacji.

Rozdział VI. Prawa osób i udostępnianie danych

§17. Prawa z RODO

1. Administrator obsługuje – zależnie od podstawy i okoliczności – prawo do informacji, dostępu i kopii, sprostowania, usunięcia, ograniczenia, przenoszenia, sprzeciwu, wycofania zgody, niepodlegania wyłącznie zautomatyzowanej decyzji oraz skargi do Prezesa UODO.

2. Odmowa lub ograniczenie wymaga wskazania podstawy i pouczenia. Nie usuwa się prawidłowych wpisów dokumentacji medycznej wyłącznie na żądanie usunięcia danych; ewentualne sprostowanie następuje w sposób przewidziany dla dokumentacji i z zachowaniem historii.

3. Wniosek może zostać złożony dowolnym dostępnym kanałem. Nie uzależnia się jego przyjęcia od formularza. Tożsamość weryfikuje się proporcjonalnie do ryzyka, bez gromadzenia nadmiarowych danych.

4. Wnioski rejestruje się z datami, zakresem, sposobem weryfikacji, decyzją, terminem i sposobem odpowiedzi. Termin wynikający z RODO liczy się od otrzymania wniosku i może zostać przedłużony tylko na warunkach RODO.

§18. Udostępnianie dokumentacji medycznej

1. Udostępnienie dokumentacji następuje zgodnie z prawem pacjenta i PO-10/2026, bez zbędnej zwłoki, w prawnie dopuszczalnej formie wybranej przez osobę uprawnioną. Formularz jest pomocniczy, a celu żądania co do zasady nie wymaga się.

2. Wykaz udostępnień zawiera elementy wymagane ustawowo, w szczególności dane pacjenta, sposób i zakres udostępnienia, dane osoby innej niż pacjent albo organu lub podmiotu, osobę udostępniającą oraz datę. Zdalne wydanie wymaga adekwatnego uwierzytelnienia i zabezpieczenia kanału.

3. Dostęp do danych osobowych na podstawie RODO i udostępnienie dokumentacji medycznej to odrębne tryby. Administrator ustala właściwy tryb na podstawie treści żądania, nie przerzucając tego obowiązku na pacjenta.

Rozdział VII. Odbiorcy, podmioty zewnętrzne i transfery

§19. Kwalifikacja ról

1. Przed przekazaniem danych ustala się, czy podmiot działa jako odrębny administrator, współadministrator, podmiot przetwarzający, osoba działająca z upoważnienia czy ustawowo uprawniony odbiorca. Umowy powierzenia nie stosuje się automatycznie do każdego kontrahenta.

2. Jeżeli zachodzi powierzenie, umowa spełnia art. 28 RODO i określa przedmiot, czas, charakter, cel, rodzaj danych, kategorie osób, obowiązki, poufność, zabezpieczenia, podpowierzenie, pomoc, audyty, zwrot lub usunięcie danych i informowanie o naruszeniach.

3. Przed zawarciem i okresowo w trakcie współpracy ocenia się gwarancje dostawcy, lokalizację danych, podwykonawców, certyfikaty, ciągłość, możliwość eksportu, usunięcia i odzyskania danych oraz warunki zakończenia usługi.

§20. Transfery poza EOG i usługi chmurowe

Dane mogą być przekazywane poza Europejski Obszar Gospodarczy wyłącznie po udokumentowaniu podstawy z rozdziału V RODO, ocenie transferu i wdrożeniu środków uzupełniających, jeżeli są wymagane. Lokalizację wsparcia, kopii zapasowych i podwykonawców ustala się przed uruchomieniem usługi chmurowej lub systemu.

Rozdział VIII. Bezpieczeństwo informacji i ciągłość działania

§21. Zabezpieczenia oparte na ryzyku

Administrator dobiera środki techniczne i organizacyjne na podstawie ryzyka dla praw i wolności osób, uwzględniając poufność, integralność, dostępność i odporność. Środki obejmują odpowiednio kontrolę dostępu, uwierzytelnienie wieloskładnikowe, szyfrowanie, rejestrowanie zdarzeń, aktualizacje, ochronę urządzeń końcowych, segmentację, kopie zapasowe, testy odtworzeniowe i procedury awaryjne.

Zabezpieczenia systemów medycznych, urządzeń zapisujących dane, aparatury i nośników są powiązane z PO-07/2026, PO-08/2026 i PO-11/2026. Serwis urządzenia nie może prowadzić do niekontrolowanego ujawnienia danych; przed przekazaniem do naprawy zabezpiecza się dane i dokumentuje dostęp.

§22. Dokumentacja papierowa i stanowiska pracy

1. Dokumentację papierową przechowuje się w strefach o kontrolowanym dostępie, z uwzględnieniem zasady czystego biurka, ochrony przed pożarem, zalaniem, kradzieżą i dostępem osób postronnych. Przemieszczanie dokumentacji jest identyfikowalne.

2. W rejestracji zapewnia się dyskrecję rozmów, właściwe ustawienie monitorów, bezpieczny odbiór wydruków i brak widocznych list pacjentów. Dokumentów innych pacjentów nie pozostawia się w teczkach, na drukarkach ani w polu widzenia.

§23. Poczta, komunikacja i teleporady

1. Do komunikacji wykorzystuje się zatwierdzone konta i narzędzia. Przed wysłaniem weryfikuje się odbiorcę, zakres i załączniki; przy danych wysokiego ryzyka stosuje się szyfrowanie lub bezpieczny portal, a hasło przekazuje innym kanałem. Kopii ukrytej używa się przy korespondencji do wielu niezależnych odbiorców.

2. Teleporady prowadzi się zgodnie z PO-02/2026. Ustala się tożsamość, miejsce i możliwość zachowania poufności, informuje o ograniczeniach, dokumentuje świadczenie i posiada plan na wypadek przerwania połączenia lub stanu nagłego. Nie korzysta się z prywatnych kont i komunikatorów.

3. Nie nagrywa się rozmów, wizji ani teleporad bez odrębnej, udokumentowanej podstawy, jasnej informacji, określenia celu, retencji i kręgu dostępu. Zgoda na świadczenie nie oznacza zgody na nagrywanie.

§24. Praca poza siedzibą i urządzenia mobilne

Przetwarzanie poza zatwierdzonym miejscem wymaga oceny ryzyka i zgody organizacyjnej, bezpiecznego urządzenia, szyfrowania, blokady ekranu, ochrony przed osobami domowymi i postronnymi, bezpiecznego połączenia oraz zakazu lokalnego przechowywania danych, jeżeli nie jest ono konieczne. Utratę urządzenia zgłasza się natychmiast.

Rozdział IX. Procesy szczególne wynikające z działalności Podmiotu

§25. Małoletni i przedstawiciele

Dane małoletnich przetwarza się z uwzględnieniem ich praw, wieku i dojrzałości, podstaw działania przedstawiciela ustawowego, praw pacjenta po ukończeniu 16 lat oraz Standardów Ochrony Małoletnich. Sam opiekun faktyczny nie uzyskuje automatycznie pełnego dostępu do dokumentacji ani prawa do wszystkich decyzji.

§26. Fotografie, wizerunek i medycyna estetyczna

Fotografie medyczne wykonuje się tylko w zakresie uzasadnionym świadczeniem, przy użyciu zatwierdzonego urządzenia i bez automatycznego zapisu do prywatnej galerii lub chmury. Zgoda na zabieg, przetwarzanie danych medycznych oraz publikację wizerunku są rozdzielone. Odmowa wykorzystania promocyjnego nie może wpływać na dostęp do świadczenia.

§27. Zajęcia grupowe i usługi niemedyczne

Dla świadczeń zdrowotnych prowadzonych grupowo dokumentację medyczną prowadzi się indywidualnie. Listy obecności nie zawierają rozpoznań ani przeciwwskazań. Dla usług rekreacyjnych zbiera się wyłącznie minimalne dane organizacyjne; ankiety bezpieczeństwa nie stają się automatycznie dokumentacją medyczną i są dostępne tylko osobom, które rzeczywiście ich potrzebują – zgodnie z PO-13/2026.

§28. Współpraca interdyscyplinarna

Wymiana informacji odbywa się między osobami rzeczywiście uczestniczącymi w opiece i tylko w niezbędnym zakresie. Włączenie osoby niewykonującej zawodu medycznego lub podmiotu zewnętrznego wymaga odrębnej oceny podstawy, roli i tajemnicy. Określenie „trener medyczny” nie nadaje prawa dostępu do dokumentacji – zgodnie z PO-14/2026.

§29. Monitoring wizyjny

Jeżeli Administrator stosuje monitoring, jego legalność, cel, obszar, krąg dostępu, oznaczenie, retencję i zabezpieczenia określa Regulamin Organizacyjny i odrębna dokumentacja. Monitoring nie obejmuje dźwięku ani pomieszczeń udzielania świadczeń, sanitarnych, socjalnych lub innych stref szczególnej prywatności, chyba że konkretny przepis dopuszcza wyjątek i spełniono jego warunki.

Nagrania przechowuje się nie dłużej niż okres dopuszczalny prawem i uzasadniony celem; ich zabezpieczenie dla postępowania dokumentuje się. Dostęp i eksport nagrań podlegają ewidencji.

§30. Marketing i komunikacja handlowa

Marketing własnych usług, newsletter, profilowanie i komunikacja handlowa są odrębnymi procesami od leczenia. Wymagają właściwej podstawy RODO oraz spełnienia przepisów dotyczących kanału komunikacji. Nie wykorzystuje się danych o rozpoznaniu lub przebiegu leczenia do marketingu bez wyraźnej, dobrowolnej podstawy.

Rozdział X. Retencja, archiwizacja i usuwanie

§31. Harmonogram retencji

Administrator prowadzi harmonogram retencji przypisany do procesów w rejestrze czynności. Dla dokumentacji medycznej stosuje się okresy ustawowe i wyjątki; dla dokumentacji rozliczeniowej, kadrowej, podatkowej, zgód marketingowych, nagrań, skarg i logów – okres wynikający z celu, prawa, przedawnienia i ryzyka. Retencja „bezterminowa” wymaga wyraźnej podstawy i okresowego przeglądu.

§32. Archiwizacja i usuwanie

1. Przed zniszczeniem weryfikuje się upływ okresu, brak obowiązku dalszego przechowania, sporu, kontroli, zabezpieczenia dowodowego lub żądania właściwego organu. Dokumentacji medycznej nie niszczy się według ogólnej decyzji administracyjnej z pominięciem prawa pacjenta.

2. Metodę usunięcia dobiera się do nośnika i poufności. Zlecenie firmie zewnętrznej wymaga właściwej kwalifikacji roli, umowy, bezpiecznego transportu i potwierdzenia zniszczenia. Usuwanie danych z kopii zapasowych następuje zgodnie z cyklem nadpisywania, z blokadą użycia do celów operacyjnych.

3. Protokół wskazuje zakres, podstawę, okres, metodę, osoby, dostawcę i dowód wykonania, bez zbędnego przepisywania danych osób, których dokumenty zniszczono.

Rozdział XI. Naruszenia ochrony danych

§33. Zgłaszanie wewnętrzne

Każda osoba zgłasza natychmiast każde podejrzenie utraty, błędnej wysyłki, nieuprawnionego dostępu, ujawnienia, uszkodzenia, niedostępności, ataku, omyłkowego wpisu lub zagubienia dokumentacji, niezależnie od oceny winy. Najpierw podejmuje tylko działania konieczne dla ochrony pacjenta i ograniczenia szkody, zachowując dowody i nie niszcząc logów.

Podmiot przetwarzający i dostawcy mają obowiązek zawiadomić Administratora bez zbędnej zwłoki w terminie umownym umożliwiającym wykonanie obowiązków w ciągu 72 godzin.

§34. Ocena i decyzje

1. Zespół wyznaczony przez Kierownika ustala moment stwierdzenia naruszenia, charakter, przyczynę, kategorie i przybliżoną liczbę osób oraz rekordów, możliwe konsekwencje, zastosowane środki, ryzyko dla praw i wolności oraz dalsze działania. Jeżeli wyznaczono IOD, zasięga się jego opinii.

2. Naruszenie zgłasza się Prezesowi UODO bez zbędnej zwłoki, w miarę możliwości nie później niż w ciągu 72 godzin od stwierdzenia, chyba że jest mało prawdopodobne, aby skutkowało ryzykiem. Opóźnienie uzasadnia się. Przy wysokim ryzyku zawiadamia się osoby bez zbędnej zwłoki, chyba że zachodzi wyjątek z art. 34 RODO.

3. Wszystkie naruszenia, także niezgłoszone organowi, dokumentuje się w rejestrze wraz z faktami, skutkami, środkami naprawczymi i uzasadnieniem decyzji. Zdarzenie może równocześnie uruchamiać PO-07/2026, procedurę cyberbezpieczeństwa, incydent wyrobu lub obowiązek poinformowania pacjenta.

Rozdział XII. Ryzyko, ocena skutków i projektowanie ochrony

§35. Analiza ryzyka

Ryzyko ocenia się dla konkretnych procesów i aktywów, odrębnie od ryzyka biznesowego, z perspektywy możliwych skutków dla osób. Uwzględnia się charakter, zakres, kontekst i cele, dane o zdrowiu i małoletnich, skalę, monitoring, innowacyjne technologie, dostęp zdalny, dostawców i transfery. Wynik obejmuje ryzyko pierwotne, zabezpieczenia, ryzyko rezydualne, właściciela, działania i termin przeglądu, spójnie z PO-08/2026.

§36. Ocena skutków dla ochrony danych

Przed rozpoczęciem przetwarzania mogącego powodować wysokie ryzyko przeprowadza się ocenę skutków zgodnie z art. 35 RODO, w szczególności przy systematycznym monitorowaniu, przetwarzaniu na dużą skalę danych o zdrowiu, nowej technologii, profilowaniu, połączeniu zbiorów lub przetwarzaniu danych osób szczególnie podatnych. Ocenę aktualizuje się przy zmianie ryzyka. Jeżeli wysokiego ryzyka nie można ograniczyć, Administrator konsultuje się z organem nadzorczym przed rozpoczęciem procesu.

§37. Ochrona danych w fazie projektowania i domyślna ochrona

Nowy system, usługa, formularz, urządzenie, integracja, kanał kontaktu, zajęcia, teleporada, wykorzystanie fotografii lub współpraca z płatnikiem wymagają przed wdrożeniem oceny celów, danych, podstaw, dostępów, retencji, dostawców, obowiązków informacyjnych, bezpieczeństwa i testów. Domyślnie przetwarza się tylko dane niezbędne dla określonego celu.

Rozdział XIII. Szkolenia, audyty i przeglądy

§38. Szkolenia

1. Szkolenie odbywa się przed nadaniem dostępu i jest dostosowane do roli. Obejmuje tajemnicę medyczną, identyfikację pacjenta, rejestrację, phishing, błędną wysyłkę, pracę z dokumentacją, incydenty, teleporady, fotografie, prawa osób i zasady dla małoletnich.

2. Szkolenia przypominające organizuje się według ryzyka, nie rzadziej niż raz na 12 miesięcy dla osób stale przetwarzających dane o zdrowiu, a ponadto po istotnej zmianie lub naruszeniu. Skuteczność weryfikuje się testem, ćwiczeniem lub audytem zachowań.

§39. Audyty i przeglądy

Politykę i jej stosowanie przegląda się nie rzadziej niż raz w roku oraz po zmianie prawa, RPWDL, struktury, zakresu świadczeń, systemu, dostawcy, naruszeniu, wynikach kontroli albo stwierdzeniu nieskuteczności zabezpieczeń. Audyt obejmuje próbki dostępów, dokumentacji, udostępnień, umów, retencji, logów i realizacji zaleceń. Działania korygujące otrzymują właściciela, termin i miernik skuteczności.

ŁÓDZKIE CENTRUM FIZJOTERAPII

Rozdział XIV. Postanowienia końcowe

§40. Dokumenty powiązane i hierarchia

Integralny system dokumentacji obejmuje w szczególności Regulamin Organizacyjny RO-01/2026, Standardy Ochrony Małoletnich, procedury PO-01/2026–PO-14/2026, Politykę Cyberbezpieczeństwa, rejestr czynności, analizę ryzyka, oceny skutków, plan ciągłości, harmonogram retencji, klauzule informacyjne i załączniki RODO-01–RODO-09. Brak dokumentu wykonawczego nie zwalnia z przestrzegania prawa.

§41. Wejście w życie

Polityka wchodzi w życie w dniu wskazanym na stronie tytułowej, po uzupełnieniu danych Administratora, ocenie obowiązku wyznaczenia IOD, zatwierdzeniu rejestru czynności, analizy ryzyka, harmonogramu retencji, listy dostawców i zakresów upoważnień oraz po przeprowadzeniu szkolenia wdrożeniowego.

PRZED ZATWIERDZENIEM: (1) wpisać pełną nazwę Administratora, zakładu i adresy; (2) wskazać IOD albo dołączyć ocenę braku obowiązku; (3) powiązać procesy z rejestrem czynności i klauzulami; (4) zatwierdzić wykaz systemów, dostawców, transferów i uprawnień; (5) ustalić retencję; (6) zweryfikować faktyczne stosowanie monitoringu, fotografii, teleporad i marketingu; (7) zatwierdzić Politykę Cyberbezpieczeństwa i plan ciągłości.

Miejsce i data: Łódź 01.09.2026

Kierownik Podmiotu Leczniczego / osoba uprawniona do zatwierdzenia: .....