**Nr sprawy: ZP/31/2025**  **załącznik nr 2 do SWZ**

**Opis przedmiotu zamówienia**

Przedmiotem Zamówienia jest dostawa licencji wdrożenie, świadczenie serwisu gwarancyjnego i nadzoru autorskiego kreatora elektronicznego dzienniczka pacjenta (dalej kreatora EDP) służącego do tworzenia Elektronicznych Dzienniczków Pacjenta (EDP). EDP to aplikacja webowa służąca do zdalnego gromadzenia danych zebranych bezpośrednio od pacjentów uczestniczących w badaniu klinicznym, zgodnie z obowiązującymi przepisami prawnymi oraz wytycznymi Dobrej Praktyki Klinicznej (ICH GCP).

Projekt „Doskonalenie i zwiększenie potencjału naukowo-badawczego istniejących Centrów Wsparcia Badań Klinicznych przy Uniwersytecie Medycznym w Łodzi, w celu kompleksowego świadczenia usług w obszarze badań klinicznych - CWBK 2” w ramach środków Krajowego Planu Odbudowy i Zwiększania Odporności, Komponentu D Efektywność, dostępność i jakość systemu ochrony zdrowia, Inwestycji D3.1.1 Kompleksowy rozwój badań w zakresie nauk medycznych i nauk o zdrowiu, w którym Agencja Badań Medycznych pełni rolę Jednostki Wspierającej. będzie realizowany w ramach konkursu ABM/2024/7/KPO, organizowanego przez Agencję Badań Medycznych z siedzibą w Warszawie. Beneficjentem Projektu jest Uniwersytet Medyczny w Łodzi. Uniwersytet zobowiązany jest zapewnić trwałość Projektu przez okres 5 lat od dnia zakończenia realizacji Projektu (okres trwałości Projektu).

**Termin realizacji:**

Zamówienie będzie realizowane w terminie: w terminie 10 miesięcy liczonych od dnia podpisania umowy, jednak nie później niż do dnia 28 lutego 2026 r. Zamawiający zastrzega jednocześnie, że wdrożenie musi zostać zakończone w terminie 6 miesięcy liczonych od dnia podpisania umowy.

Realizacji niniejszej umowy obejmuje następujące etapy:

a) Etap 1 – Analiza i wykonanie dokumentacji przedwdrożeniowej

b) Etap 2 – Prace programistyczne i wdrożeniowe

c) Etap 3 – Testy walidacyjne

d) Etap 4 – Przeprowadzenie szkoleń

Szczegółowy harmonogram realizacji zostanie ustalony przez Strony po zawarciu umowy. Harmonogram może podlegać zmianom w toku realizacji umowy. Zmiany harmonogramu nie wymagają zawarcia aneksu do umowy. W przypadku zmiany harmonogramu ze strony Zamawiającego Wykonawca jest uprawniony zgłosić zastrzeżenia do proponowanej zmiany, ale ostateczna decyzja w tym zakresie należy do Zamawiającego. Zamawiający zastrzega sobie nadto prawo odmowy dokonania zmian harmonogramu na wniosek Wykonawcy.

Szczegółowy opis przedmiotu zamówienia

1. **Wytyczne ogólne**
	1. Wytworzenie systemu kreatora EDP do tworzenia narzędzia wspierającego zbieranie danych przez Badacza w badaniu klinicznym.
	2. Utworzony EDP ma mieć możliwość płynnej integracji z systemem eCRF będącego w posiadaniu Zamawiającego wraz z agregacją danych do eCRF dla konkretnego badania i pacjenta, uzyskanych po uzupełnieniu EDP przez Pacjenta.
	3. Kreator EDP musi być zgodny z wytycznymi „Guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic)” (EMA/INS/GCP/856758/2018) oraz FDA 21 CFR Part 11. aktualną na dzień podpisania protokołu odbioru wersją wytycznych Guideline for Good Clinical Practice E6 oraz Rozporządzeniem Parlamentu Europejskiego i Rady (UE) NR 536/2014 z dnia 16 kwietnia 2014 r. w sprawie badań klinicznych produktów leczniczych stosowanych u ludzi oraz uchylenia dyrektywy 2001/20/W. System musi być każdorazowo aktualizowany do najnowszych wytycznych.
	4. EDP wytworzony w kreatorze EDP musi być dostępny dla pacjentów i zespołu badawczego 24 godziny na dobę, 7 dni w tygodniu.
	5. Kreator EDP powinien zapewniać możliwość dostosowania treści EDP do indywidualnych potrzeb wynikających z protokołu badania klinicznego.
	6. Kreator EDP musi być dostępny poprzez stronę www (zapewniać również odpowiednie skalowanie konieczne, aby zapewnić odpowiedni odczyt na urządzeniach mobilnych) na podstawie zdefiniowanych uprawnień w module administracyjnym.
	7. Kreator EDP oraz wytworzony EDP musi działać co najmniej w polskiej i angielskiej wersji językowej. Użytkownik musi mieć możliwość wybrania wersji językowej.
	8. Kreator EDP musi umożliwiać zapewnienie tworzenia dowolnego typu pytań do EDP z możliwością udzielenia odpowiedzi przynajmniej w formie: liczbowej, opisowej, wizualnej za pomocą skali. Przykładem danych, które zbieranie ma umożliwić EDP są dane uzyskiwane za pomocą m. in. Kwestionariuszy: skal jakości życia np. (np. EQ-5D-5L, SF-36), oceny nasilenia choroby (np. VAS, NRS), wywiadu medycznego (np. wywiad dotyczący samopoczucia, wywiad żywieniowy).
	9. Wytworzony w kreatorze EDP musi umożliwiać śledzenie bezpieczeństwa pacjenta w badaniu poprzez zdalne raportowanie występowania objawów niepożądanych zdefiniowanych przez zamawiającego jako potencjalne AE/SAE.
	10. Kreator EDP powinien zapewniać możliwość wytworzenia nieograniczonej liczby EDP.
	11. Kreator EDP musi umożliwić stworzenie osobnych EDP dla wielu badań równocześnie oraz wypełnianie EDP przez co najmniej 100 pacjentów równocześnie.
	12. Dostęp do wszystkich funkcji systemu, w tym wytworzonego EDP musi być zapewniony z dowolnego miejsca i w dowolnym czasie z poziomu przeglądarek internetowych (zainstalowanych i używanych przez Zamawiającego tj. Google Chrome, Firefox, Microsoft Edge, Safari, w tym zgodność z przeglądarkami stosowanymi w urządzeniach mobilnych) w najnowszych dostępnych wersjach.
	13. Integralność i walidacja danych. System powinien posiadać mechanizmy zapewniające integralność danych i ich odpowiednią walidację podczas wprowadzania, tak aby dane wprowadzone do systemu były dokładne i kompletne. Mechanizmy walidacyjne powinna wykrywać oraz oznaczać wszelkie błędy lub niespójności w danych.
	System a także musi zostać zwalidowany i utrzymywany w stanie zwalidowanym, zgodnie z obowiązującymi wymaganiami opisanymi w punkcie 1.3, przy czym proces walidacji powinien być udokumentowany przez Wykonawcę.
2. **Gwarancja**
	1. Zamawiający oczekuje udzielenia na wdrożony system gwarancji producenta oraz nadzoru autorskiego na okres 2 lat, liczony od dnia podpisania bezusterkowego protokołu odbioru systemu.
	2. W ramach tak rozumianej gwarancji Wykonawca zobowiązany będzie do usunięcia wszelkich wad przedmiotu niniejszego opisu przedmiotu zamówienia, które można zgłaszać Wykonawcy za pośrednictwem systemu JIRA Zamawiającego.
	3. Wymagany czas naprawy zgłoszonego problemu wynosi maksymalnie:
		1. w przypadku Błędu Krytycznego czas naprawy wyniesie do 2 dni roboczych od chwili zgłoszenia Błędu Krytycznego (Błąd krytyczny - awaria oprogramowania, które powstało w wyniku realizacji umowy niespowodowana przez Użytkownika, która prowadzi do zatrzymania eksploatacji, utraty danych lub naruszenia spójności danych, w wyniku których nie jest możliwe prowadzenie działalności z użyciem oprogramowania);
		2. czas naprawy wyniesie do 10 dni roboczych od chwili zgłoszenia Błędu Zwykłego (Błąd zwykły - awaria oprogramowania, które powstało w wyniku realizacji umowy niespowodowana przez Użytkownika, która prowadzi do zakłóceń pracy oprogramowania, utraty danych lub naruszenia spójności danych, a która nie uniemożliwia prowadzenia działalności z użyciem oprogramowania).
	4. Serwis gwarancyjny może się odbywać zdalnie. Dostęp do naprawy w technologii zdalnej realizowany będzie przez Wykonawcę w sposób zgodny z wymaganiami Zamawiającego, które zostaną przedstawione po podpisaniu umowy.
	5. W okresie gwarancji Wykonawca zapewnia usługi serwisowe na cały System, w ramach wynagrodzenia umownego, bez dodatkowej odpłatności.
	6. Wszelkie dokonywane w okresie gwarancji działania (naprawy, przeglądy, aktualizacje, itp.) muszą zakończyć się szczegółowymi protokołami potwierdzającymi realizację zarejestrowanych zgłoszeń błędów. Za szczegółowy protokół uznaje się wątek prowadzony w systemie JIRA Zamawiającego. Za moment zakończenia realizacji wątku uznaje się ustawienie przez przedstawiciela Zamawiającego statusu „Done”.
	7. Dostarczanie, instalację i konfigurację nowych wersji oprogramowania w przypadku zmiany otoczenia prawnego, w celu utrzymania jego zgodności z przepisami prawa.
	8. Dostarczanie, instalację i konfigurację nowych wersji oprogramowania w przypadku, gdy powstała nowa jego wersja z inicjatywy Producenta.
	9. Nadto w ramach udzielonej gwarancji Wykonawca zobowiązany jest do zapewnienia:
3. zapewnienie ciągłości i poprawnego działania Systemu, łącznie z utrzymaniem systemu w stanie zwalidowanym;
4. obsługa Zgłoszeń serwisowych;
5. aktualizacja oprogramowania systemowego lub serwerowego w ramach licencji posiadanych przez Zamawiającego, ewentualnie sygnalizowanie zasadności nabycia przez Zamawiającego dodatkowych licencji zapewniających właściwe działanie Platformy Sprzętowo-Systemowej;
6. aktualizacja certyfikatów;
7. aktualizacja dokumentacji użytkownika (minimum jeden raz na rok lub w przypadku wprowadzenie znaczących zmian do systemu);
8. opracowanie dokumentacji zawierającej procedury przywracania działania Systemu po Błędzie Systemu i procedury ciągłości działania Systemu;
9. wykonywanie kopii bezpieczeństwa Systemu (zgodnie z procedurą bezpieczeństwa obowiązującą u Zamawiającego).
10. **Bezpieczeństwo**
	1. System ma uniemożliwiać wprowadzanie lub modyfikację danych w sposób anonimowy.
	2. System powinien automatycznie wylogowywać lub blokować sesję użytkownika po zadanym czasie braku aktywności.
	3. Szyfrowanie danych w trakcie przesyłania oraz przechowywania.
	4. System zapewnia bezpieczeństwo zdeponowanych danych zgodnie z Normą ISO 9001 oraz ISO 27001 i zgodności z wymaganiami ustawy o ochronie danych osobowych.
	5. System powinien umożliwiać jednoczesną autoryzację użytkowników w oparciu o zewnętrznego dostawcę tożsamości w standardzie OpenID (Office 365), usługę katalogową Active Directory oraz wewnętrzną bazę użytkowników.
	6. System powinien umożliwiać wykorzystanie dwuskładnikowej autoryzacji użytkowników w oparciu o: zewnętrzną aplikację mobilną (Microsoft Authenticator, Google Authenticator), klucz sprzętowy U2F FIDO/FIDO2.
11. **Kreator EDP**
	1. Dostęp zespołu badawczego do danych rejestrowanych bezpośrednio przez pacjenta w czasie rzeczywistym.
	2. Na pojedynczych stronach EDP ma być wyświetlane zawsze tylko jedno pytanie.
	3. Możliwość ustawienia wysyłania automatycznych notyfikacji/alertów do uczestników badania w formie powiadomienia sms/wiadomość mailowa o konieczności wypełnienia EDP oraz braku jego wypełnienia oraz o konieczności przyjęcia leku o konkretnej godzinie.
	4. Wysyłanie automatycznych notyfikacji/alertów w formie powiadomienia sms/wiadomość mailowa do zespołu badawczego o wypełnieniu/braku wypełnienia EDP przez uczestnika badania.
	5. Proaktywne gromadzenie danych dotyczących bezpieczeństwa oraz wysyłanie alertów o potencjalnym wystąpieniu zdarzenia niepożądanego do zespołu badawczego poprzez udostępnianie wprowadzonych przez pacjenta danych badaczom.
	6. Utworzony, w kreatorze, EDP powinien być udostępniony w dostępie ogólnym pod nazwą każdorazowo wskazaną przez Zamawiającego (np. EDP-”akronim\_badania").
	7. Zintegrowane z systemem eCRF posiadanym przez Zamawiającego dane zebrane w wyniku wypełnionego EDP powinny umożliwiać monitorowanie przez Badacza m.in.:
* Compliance przyjmowanych leków (weryfikacja przez Badacza)
* liczbę wypełnionych ankiet w stosunku do liczby zgodnej z harmonogramem
* Generowanie raportu (format xls) z wynikami w formacie: data, pacjent, rodzaj oceny, wynik (liczbowy lub słowny, zależnie od kwestionariusza/pytania);
1. **EDP wytworzony w kreatorze EDP**
	1. EDP powinien posiadać możliwość dodawania kont dla pacjentów w danym Ośrodku Badawczym przez Głównego Badacza/Koordynatora.
	2. Interfejs EDP ma umożliwiać adaptacje wyglądu przez uczestnika badania w zakresie kontrastu obrazu, wielkości czcionki.
	3. Możliwość powrotu do pytania i modyfikacji wcześniej wpisanej odpowiedzi przez uczestnika badania przed zamknięciem ankiety na danym etapie.
	4. Dwustopniowy alert zamknięcia/wysłania ankiety przez pacjenta – zabezpieczenie przed przypadkowych wysłaniem ankiety.
	5. Dane z wypełnianych przez Pacjentów/Uczestników badań, ankiet/e-dzienniczka powinny agregować się do konkretnego pacjenta w utworzonym formularzu eCRF w systemie posiadanym przez Zamawiającego.
2. **Procedura odbioru, scenariusze testowe**
	1. Wykonawca przygotuje scenariusze testowe, na podstawie których Zamawiający dokona testów akceptacyjnych i odbiorowych.
	2. Scenariusze testowe muszą umożliwiać przejście przez wszystkie funkcjonalności systemu oraz wszystkie jego warianty (ścieżki).
	3. Scenariusze muszą być przygotowane w sposób umożliwiający ich przeprowadzenie przez osobę, która wcześniej nie pracowała w systemie i nie zna jego założeń i funkcjonalności.
	4. Przed przystąpieniem do realizacji testów przez Zamawiającego, muszą one zostać przez niego zaakceptowane.
	5. Poprawne przejście wszystkich scenariuszy jest podstawą do podpisania bezusterkowego protokołu odbioru produktu.
	6. Każdy zauważony podczas realizacji scenariuszy testowych błąd zostanie zgłoszony w systemie JIRA Zamawiającego i obsługiwany tam do chwili potwierdzenia przez Zamawiającego jego naprawy.
3. **Moduł administracyjny**
	1. Autoryzacja użytkowników musi odbywać się za pośrednictwem wdrożonego u Zmawiającego mechanizmu SSO (Single Sign-on) opartego o mechanizm OAuth w usłudze Microsoft365.
	2. Zarządzanie dostępem do systemu odbywać się powinno w oparciu o grupy w usłudze Active Directory Zamawiającego. Dodanie użytkownika do odpowiedniej grupy powinno skutkować umożliwieniem mu logowania w oparciu o mechanizm opisany w punkcie 5.5. Szczegółowe uprawnienia do wykonywania poszczególnych operacji w systemie i pełnienia w nim właściwych ról, powinno odbywać się w module administracyjnym systemu. System musi umożliwiać równolegle z mechanizmem opartym o AD, zarządzanie kontami użytkowników oraz dostępem do systemu, w oparciu o wewnętrzny (systemowy) mechanizm, niezależny od AD, w tym nadawanie haseł lokalnie za pośrednictwem systemu.
	3. Użytkownik z rolą Administratora Systemu ma możliwość nadawania indywidualnym użytkownikom oraz grupom użytkowników niezależnych uprawnień do modułów i zawartych w nich funkcji. Uprawnienia powinny być tak skonstruowane, aby można było je nadawać z dokładnością do rodzaju wykonywanej operacji tj. osobne uprawnienia na odczyt danych, ich wprowadzanie czy modyfikację.
	4. System umożliwia obsługę badań prowadzonych w kilku jednostkach badawczych poprzez rozbudowany system uprawnień użytkowników. System umożliwia ograniczenie widocznych danych tylko do pacjentów z danej jednostki dla określonych użytkowników indywidualnych oraz grup użytkowników.
	5. Uprawnienia użytkowników powinny być zdefiniowane w formie pozwoleń (to co nie jest dozwolone jest zabronione). Każdy użytkownik powinien posiadać początkowo minimalną liczbę uprawnień oraz domyślnie jego konto powinno być nieaktywne. Administrator może zmienić status konta na aktywne.
	6. System posiada widok listy wszystkich użytkowników przypisanych do badania wraz z następującymi danymi: e-mail, imię i nazwisko, data dodania do badania, data modyfikacji uprawnień, status użytkownika, data nadania i odebrania dostępów użytkownikom.
	7. System umożliwia wysłanie pierwszego hasła oraz jego resetowanie poprzez przesłanie kodu aktywacyjnego na e-maila użytkownika.
4. **Przechowywanie i archiwizacja**
	1. System zapewnia szyfrowanie dokumentów podczas przechowywania oraz zapewnia ich bezpieczeństwo przed nieautoryzowanym dostępem.
	2. System umożliwia archiwizację zakończonych badań oraz dokumentów, z dostępem do archiwów na żądanie.
5. **Wymagania techniczne**
	1. System musi być wyposażony w mechanizm automatycznego tworzenia cyklicznych kopii zapasowych (backup) wraz z możliwością ich łatwego przywrócenia. Mechanizm ten będzie zgodny z posiadanym przez Zamawiającego systemem backupu CommVault. Polityka backupów zostanie określona na etapie analizy przedwdrożeniowej.
	2. Wykonanie kopii zapasowej nie może wymagać przerwania pracy przez użytkowników.
	3. Zamawiający wymaga, aby w ramach wdrożenia zainstalowane zostało w infrastrukturze Zamawiającego środowisko Produkcyjne oraz Testowo-Szkoleniowe systemu. Środowisko wytwórcze (developerskie) Wykonawca zapewnia we własnym zakresie i w ramach własnej infrastruktury. Wykonawca musi zapewnić niezbędne licencje na oprogramowanie do obsługi tych środowisk.
	4. Wykonawca zapewni zgodność systemu z wymaganiami ustawy o ochronie danych osobowych (Dz. U. 2018 poz. 1000) i rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r (RODO).
	5. Na Systemie zostaną przeprowadzone testy bezpieczeństwa zgodnie z wytycznymi OWASP (OWASP Web Security Testing Guide).
	6. System musi być zgodny z Ustawą o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz. U. 2019 poz. 848) oraz Ustawie o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018 poz. 1560).
	7. System powinien działać sprawnie przy jednoczesnym użytkowaniu przez co najmniej 100 osób. Maksymalny czas operacji wykonywanych przez System, związanych z interakcją Użytkownika z Systemem, nie może być dłuższy niż 3 sekundy.
	8. System powinien być dostępny całodobowo, a czynności techniczne wykonywane w czasie najmniejszego ruchu po ówczesnym uzgodnieniu terminu okna serwisowego z Zamawiającym.
	9. Wykonawca zapewni dostępność Systemu na poziomie 99% w skali roku.
	10. System musi działać co najmniej w polskiej oraz angielskiej wersji językowej. Użytkownik musi mieć możliwość wybrania wersji językowej.
	11. System musi posiadać podręcznik użytkownika w polskiej oraz angielskiej wersji językowej. System musi być wyposażony w wyszukiwarkę do przeglądania podręcznika użytkownika.
	12. Wykonawca przeprowadzi szkolenia personelu z obsługi dostarczonego rozwiązania.
	13. System musi być zbudowany w architekturze trójwarstwowej (warstwa danych, warstwa aplikacyjna, warstwa prezentacji).
	14. Warstwa danych musi wspierać możliwość pracy na następujących systemach bazodanowych, w wersjach aktualnie wspieranych przez producenta: Oracle/PostgreSQL, MS SQL, MySQL/MariaDB.
	15. Warstwa aplikacyjna musi umożliwiać wdrożenie serwera aplikacyjnego na następujących platformach, w wersjach aktualnie wspieranych przez producenta: Microsoft Windows, GNU/Linux (dystrybucje Debian lub RedHat/CentOS).
	16. Warstwa prezentacji musi być oparta o tzw. „cienkiego klienta” przeglądarkę sieci web. Oprogramowanie musi być kompatybilne z przeglądarkami EDGE, Chrome oraz Firefox w wersjach aktualnie wspieranych przez producenta.
	17. Moduł uwierzytelniania użytkowników musi mieć możliwość integracji z bazą LDAP/Active Directory oraz mechanizmem OpenID, na podstawie, której będzie następowała autoryzacja operatora systemu.
	18. System powinien wspierać mechanizmy SSO (Single Sign On) w celu automatycznego uwierzytelnienia operatora na podstawie danych logowania do systemu operacyjnego klienta
	19. System musi wspierać architekturę SOA, zapewniać interfejsy i umożliwiać komunikację z innymi systemami dziedzinowymi poprzez mechanizmy WebService z wykorzystaniem protokołów komunikacyjnych SOAP/HTTP oraz języka WSDL lub REST.
	20. Generowane lub przechowywane w systemie dokumenty elektroniczne muszą być gromadzone w Centralnym Repozytorium Dokumentów Elektronicznych. Komunikacja pomiędzy wdrażanym systemem a Centralnym Repozytorium Dokumentów Elektronicznych musi odbywać się z wykorzystaniem protokołu CMIS. Dokumenty elektroniczne zgromadzone z poziomu systemu dziedzinowego w repozytorium nie mogą być modyfikowane.
	21. Warstwa prezentacyjna systemu musi być przystosowana do poprawnego wyświetlenia zawartości okna systemu na monitorach komputerów o rozdzielczości nie mniejszej niż HD (1366x768). Interfejs musi być wykonany w technologii responsywnej i dostosowywać się do wielkości ekranu dla urządzeń mobilnych.
	22. System powinien być zintegrowany z posiadanym przez Zamawiającego systemem elektronicznej karty obserwacji pacjenta (eCRF) w zakresie min.: połączenia/osadzenia kreatora EDP z możliwością podpięcia gotowego EDP do konkretnego badania klinicznego oraz agregacji przypisania danych do odpowiedniego pacjenta, z możliwością generowania raportów w formacie xls z poszczególnych ocen (data, pacjent, pytanie, odpowiedź (słowna lub liczbowa).
	23. Gotowość zintegrowania systemu z posiadanym przez Zamawiającego systemem typu CTMS w zakresie oznaczania badań, dla których uruchomiono EDP. Szczegółowe wytyczne dotyczące integracji zostaną ustalone zostaną na etapie analizy przedwdrożeniowej.

11. Szkolenia z obsługi kreatora elektronicznego dzienniczka pacjenta (EDP)

11.1. Szkolenia z obsługi kreatora EDP powinny być dostosowane do różnych grup użytkowników i ich zakresu odpowiedzialności w badaniu klinicznym.

Zakres szkolenia powinien obejmować minimum:

**Szkolenia dla przedstawicieli Sponsora (Sponsor/CRO):**

* Podstawowe funkcje kreatora w tym: Logowanie, nawigacja, struktura interfejsu
* Tworzenie elektronicznych dzienniczków pacjenta w tym: Jak tworzyć, modyfikować i zarządzać dzienniczkami pacjentów, w tym definiowanie pytań i formularzy specyficznych dla danego badania klinicznego.
* Uruchamianie dzienniczków w tym: Jak aktywować dzienniczki, aby pacjenci mogli z nich korzystać
* Walidacja danych w tym: Procesy weryfikacji poprawności i kompletności danych wprowadzanych przez pacjentów, jak przeprowadzić analizę walidacji systemu (nie tylko danych) zgodnie z wymaganiami nowej wersji GCP.
* Zarządzanie użytkownikami w tym: Nadawanie i odbieranie uprawnień, definiowanie ról w systemie.
* Audyt i ścieżka audytowa w tym: Przegląd logów systemowych
* Integracja z eCRF w tym: zasady zaczytywania danych uzupełnionych przez Pacjentów EDP do eCRF

**Szkolenia dla ośrodków badawczych (Badacze, Koordynatorzy, Farmaceuci, Inny personel ośrodka**)

* Podstawowe funkcje kreatoraw tym: Logowanie, struktura interfejsu, przeglądanie danych pacjentów.
* Tworzenie i zarządzanie dzienniczkami pacjentów w tym: Jak wprowadzać dane do dzienniczków, modyfikować istniejące wpisy oraz zarządzać formularzami.
* Uruchamianie dzienniczków w tym: Jak aktywować dzienniczki, aby pacjenci mogli z nich korzystać

11.2. Dopuszczalne formy szkoleń:

* Materiały tekstowe i prezentacje PDF
* Filmy szkoleniowe (video tutorials)

**W przypadku wprowadzenia do systemu istotnych zmian funkcjonalnych Wykonawca dostarczy odpowiednie materiały szkoleniowe dotyczące modyfikacji.**

**Zał. nr 2 do SWZ musi być podpisany kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym.**