**Nr sprawy: ZP/20/2025 Załącznik nr 2 do SWZ**

**Opis przedmiotu zamówienia**

Przedmiotem Zamówienia jest dostawa licencji, wdrożenie, świadczenie serwisu gwarancyjnego Systemu Podstawowej Dokumentacji Badania Klinicznego (eTMF) z podziałem na Akta Sponsora (eTMF Sponsora) i Akta Badacza (eISF), który będzie wspierał zarządzanie dokumentacją badań klinicznych. System ma na celu zwiększenie efektywności i bezpieczeństwa procesów związanych z przechowywaniem, zarządzaniem i przetwarzaniem dokumentacji badawczej 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).

Szczegółowy opis przedmiotu zamówienia

1. **Wytyczne ogólne**
   1. Wytworzenie systemu Podstawowej Dokumentacji Badania Klinicznego (eTMF) z podziałem na Akta Sponsora (eTMF Sponsora) i Akta Badacza (eISF) pozwalającego na utrzymanie dokumentacji zgodnie z wytycznymi Guideline for Good Clinical Practice E6, na podstawie Modelu Referencyjnego TMF (TMF Reference Model, Version 3.2.0, CDISC Europe Foundation).
   2. System 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), Guideline on computerised systems and electronic data in clinical trials (EMA/INS/GCP/112288/2023), 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.
   3. System ma pozwalać na kompleksowe zarządzanie dokumentacją prowadzonego badania wszystkim uprawnionym osobom, zgodnie z przyznanym poziomem uprawnień.
   4. System umożliwia przechowywanie dokumentów związanych z badaniem, nie wchodzących w skład eTMF.
   5. System umożliwia stworzenie osobnych zbiorów dokumentacji dla wielu badań.
   6. System umożliwia umieszczenie pliku jednocześnie do wielu lokalizacji (eTMF Sponsora i eISF) za pośrednictwem jednej operacji w systemie (np. W przypadku protokołu badania klinicznego, przez umieszczenie przez osobę upoważnioną przez Sponsora dokumentu w systemie, może on być widoczny w obu sekcjach).
   7. System ma umożliwiać dostęp poprzez stronę www na podstawie zdefiniowanych uprawnień w module administracyjnym.
   8. Dostęp do wszystkich funkcji systemu 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.
   9. 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. Walidacja powinna wykrywać oraz oznaczać wszelkie błędy lub niespójności w danych.
   10. System także musi zostać zwalidowany i utrzymywany w stanie zwalidowanym, zgodnie z obowiązującymi wymaganiami opisanymi w punkcie 1.2, przy czym proces walidacji powinien być udokumentowany przez Wykonawcę.
2. **Gwarancja**
   1. Zamawiający oczekuje udzielenia na wdrożony system gwarancji producenta na okres 3 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:
      * 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);
      * 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 wraz z wykazem zmian.
   9. Udzielona gwarancja obejmuje nadto:
      1. zapewnienie ciągłości i poprawnego działania Systemu, łącznie z utrzymaniem systemu w stanie zwalidowanym;
      2. obsługę zgłoszeń serwisowych;
      3. aktualizację oprogramowania systemowego lub serwerowego w ramach licencji posiadanych przez Zamawiającego, ewentualnie sygnalizowanie zasadności nabycia przez Zamawiającego dodatkowych licencji zapewniających właściwe działanie Platformy Sprzętowo-Systemowej;
      4. aktualizację certyfikatów;
      5. aktualizację dokumentacji użytkownika (minimum jeden raz na rok lub w przypadku wprowadzenie znaczących zmian do systemu);
      6. opracowanie dokumentacji zawierającej procedury przywracania działania Systemu po Błędzie Systemu i procedury ciągłości działania Systemu;
      7. wykonywanie kopii bezpieczeństwa Systemu (zgodnie z procedurą bezpieczeństwa obowiązującą u Zamawiającego).
      8. zdalne konsultacje i porady w zakresie eksploatacji Systemu przez Zamawiającego, dotyczące zagadnień informatycznych i merytorycznych związanych z użytkowaniem Systemu;
      9. zdalne wsparcie pracowników Zamawiającego – help desk w zakresie obejmującym użytkowanie Systemu.
3. **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.
   7. Dostawca powinien niezwłocznie zgłaszać Zamawiającemu wszelkie potencjalne poważne naruszenia, w tym naruszenia bezpieczeństwa, o których się dowiedział (np. poprzez powiadomienie od innych sponsorów badań korzystających z tego samego systemu), jeśli mogą one mieć jakikolwiek wpływ na wiarygodność i odporność danych oraz na bezpieczeństwo i prawa uczestników badania klinicznego, których dane zostały wprowadzone do systemu.
4. **Moduł eTMF (electronic Trial Master File)**
   1. System umożliwia utworzenie i skonfigurowanie struktur katalogów dla nieograniczonej liczby badań.
   2. Struktura katalogów:
      * powinna być zgodna z Modelem Referencyjnym TMF (TMF Reference Model, Version 3.2.0, CDISC Europe Foundation),
      * jest automatycznie proponowana dla nowo tworzonych projektów,
      * system umożliwia modyfikowanie struktury katalogów, w tym edycję, dodawanie i usuwanie folderów i podfolderów,
      * system umożliwia wprowadzenie listy ośrodków badawczych.
   3. Elektroniczne przechowywanie i zarządzanie dokumentami:
      * System przechowuje dokumenty badania w ustrukturyzowanym formacie w jednym, ujednoliconym systemie.
      * System umożliwia importowanie dokumentów w różnych formatach (m.in. .pdf, .jpg, .png, .doc, .xls).
      * System umożliwia podgląd importowanych plików.
      * System umożliwia dodawanie komentarzy do importowanych plików.
      * System zapewnia wsparcie dla elektronicznych podpisów (składających się z nazwy użytkownika i hasła) zgodnych z regulacjami prawnymi, umożliwiających autoryzację dokumentów.
   4. Organizacja i klasyfikacja dokumentów:
      * Foldery i podfoldery: Możliwość tworzenia struktury folderów i podfolderów do przechowywania dokumentów, co umożliwia logiczne i intuicyjne grupowanie dokumentów.
      * Metadane: Dodawanie metadanych do dokumentów, w tym m. in.: tytuł, autor, data przesłania, wersja i data, data ważności, co ułatwia wyszukiwanie i sortowanie dokumentów. Ponadto system powinien umożliwiać pełnotekstowe wyszukiwanie dokumentów.
   5. Śledzenie kompletności dokumentacji:
      * Listy kontrolne: Automatyczne generowanie list kontrolnych dla wymaganych dokumentów, w tym dla poszczególnych ośrodków badawczych.
      * Monitorowanie statusu kompletności dokumentacji w czasie rzeczywistym z możliwością przeglądania brakujących lub niekompletnych dokumentów.
      * System umożliwia weryfikację importowanych plików przez upoważnionych użytkowników poprzez akceptację lub odrzucenie (wraz z podaniem powodu odrzucenia).
      * Powiadomienia i przypomnienia: Automatyczne wysyłanie powiadomień i przypomnień do odpowiedzialnych użytkowników w przypadku brakujących dokumentów lub zbliżających się terminów ważności załączonych dokumentów.
   6. Wersjonowanie dokumentów:
      * Śledzenie wersji: Automatyczne śledzenie wszystkich wersji dokumentów, umożliwiające przeglądanie historii zmian oraz przywracanie poprzednich wersji. System zapewnia korzystanie wyłącznie z najnowszych zatwierdzonych dokumentów.
      * Komentarze i zmiany: Możliwość dodawania komentarzy do wersji dokumentów oraz śledzenie wprowadzonych zmian.
   7. Wyszukiwanie i filtrowanie dokumentów:
      * Zaawansowane wyszukiwanie: Możliwość wyszukiwania dokumentów na podstawie różnych kryteriów, takich jak metadane, treść dokumentu, data utworzenia, autor itp.
      * Filtry: Filtry umożliwiające zawężenie wyników wyszukiwania do określonych kategorii dokumentów lub konkretnych zakresów czasowych.
   8. System umożliwia przypisywanie zadań do użytkowników.
   9. Obsługa szkoleń użytkowników - system umożliwia m. in.:
      * Nadawanie ról i uprawnień Uczestnika w systemie
      * określenie grup uczestników szkoleń,
      * zawiera repozytorium materiałów szkoleniowych, w tym dostęp online i materiały do pobrania z możliwością określenia, które materiały mogą zostać pobrane
      * organizację dokumentów w edytowalnej strukturze (foldery, podfoldery),
      * dodawanie komentarzy do załączonych materiałów szkoleniowych,
      * importowanie certyfikatów użytkowników oraz określenie ich daty ważności,
      * automatyczne przypominanie o kończącej się dacie ważności certyfikatu,
      * generowanie zadań wymagających potwierdzenia zapoznania się z dokumentem przez użytkowników ze wskazanej grupy,
      * wyznaczenie terminu odbycia kursu/szkolenia,
      * tworzenie kursów i szkoleń z wykorzystaniem materiałów szkoleniowych,
      * określenie formy zaliczenia kursu/szkolenia: oświadczenie o odbyciu szkolenia, formularze testowe, quizy,
      * tworzenie wzoru wybranej formy zaliczenia kursu/szkolenia,
      * stworzenie raportu ze szkoleń odbytych przez użytkowników w formie podsumowania zawierającego minimum: tytuł szkolenia, datę odbycia szkolenia, imię i nazwisko uczestnika szkolenia.
      * potwierdzanie odbytych szkoleń poprzez ponowne zalogowanie się danymi do systemu.
   10. System powinien umożliwiać wysyłanie powiadomień mailowych o zadaniach przydzielonych użytkownikowi w systemie.
   11. Przechowywanie i archiwizacja:
       * Bezpieczne przechowywanie: Szyfrowanie dokumentów podczas przechowywania oraz transmisji, zapewniające ochronę przed nieautoryzowanym dostępem.
       * Archiwizacja: Możliwość archiwizacji zakończonych badań oraz dokumentów, z dostępem do archiwów na żądanie.
   12. System umożliwia generowanie raportów dotyczących statusu kompletności dokumentacji, wersji dokumentów, aktywności użytkowników itp.
   13. Elektroniczna wymiana dokumentów: System umożliwia bezpieczną wymianę dokumentów między użytkownikami oraz zewnętrznymi interesariuszami (np. CRO).
5. **Moduł eISF (electronic Investigator Site File)**
   1. System umożliwia utworzenie i skonfigurowanie struktur katalogów dla nieograniczonej liczby badań.
   2. Integracja z systemem eTMF - dwukierunkowa synchronizacja danych: System umożliwia automatyczną i ręczną synchronizację dokumentów i danych między systemem eISF i eTMF, umożliwiając przesyłanie dokumentów w obie strony.
   3. Elektroniczne przechowywanie i zarządzanie dokumentami:
      * System przechowuje dokumenty badania w ustrukturyzowanym formacie w jednym, ujednoliconym systemie.
      * System umożliwia importowanie dokumentów w różnych formatach (m.in. .pdf, .jpeg, .png).
      * System zapewnia wsparcie dla elektronicznych podpisów zgodnych z regulacjami prawnymi, umożliwiających autoryzację dokumentów.
   4. Organizacja i klasyfikacja dokumentów:
      * Foldery i podfoldery: Możliwość tworzenia struktury folderów i podfolderów do przechowywania dokumentów, co umożliwia logiczne i intuicyjne grupowanie dokumentów.
      * Metadane: Dodawanie metadanych do dokumentów, takich jak tytuł, autor, data utworzenia, typ dokumentu itp., co ułatwia wyszukiwanie i sortowanie dokumentów.
   5. Elektroniczne formularze – System umożliwia Elektroniczne rejestrowanie i śledzenie wybranych czynności w badaniu (np. dziennik szkoleń – rejestrowanie szkoleń zespołu badawczego, w tym daty szkoleń, nazwiska uczestników, tematyka szkoleń; dzienniki wizyt – rejestrowanie wizyt, w tym rodzaju wizyty, dat, uczestników; formularz identyfikacji członków zespołu badawczego).
   6. System umożliwia automatyczne wysyłanie powiadomień i przypomnień do odpowiedzialnych użytkowników w przypadku brakujących dokumentów lub zbliżających się terminów ważności załączonych dokumentów.
   7. Wersjonowanie dokumentów:
      * Śledzenie wersji: Automatyczne śledzenie wszystkich wersji dokumentów, umożliwiające przeglądanie historii zmian oraz przywracanie poprzednich wersji. System zapewnia korzystanie wyłącznie z najnowszych zatwierdzonych dokumentów.
      * Komentarze i zmiany: Możliwość dodawania komentarzy do wersji dokumentów oraz śledzenie wprowadzonych zmian.
   8. Wyszukiwanie i filtrowanie dokumentów:
      * Zaawansowane wyszukiwanie: Możliwość wyszukiwania dokumentów na podstawie różnych kryteriów, takich jak metadane, treść dokumentu, data utworzenia, autor itp.
      * Filtry: Filtry umożliwiające zawężenie wyników wyszukiwania do określonych kategorii dokumentów lub konkretnych zakresów czasowych.
   9. System umożliwia definiowanie ról użytkowników oraz przypisywanie uprawnień dostępu do dokumentów i funkcjonalności systemu na podstawie tych ról (np. ograniczony dostęp do plików/dokumentów (np. kody randomizacji i odślepione dane o zdarzeniach niepożądanych)
   10. System zapewnia szyfrowanie dokumentów podczas przechowywania i transmisji, zapewniające ochronę przed nieautoryzowanym dostępem.
   11. System umożliwia rejestrowanie wszelkich operacji na dokumentach (tworzenie, modyfikacja, usunięcie) wraz z danymi o użytkownikach dokonujących tych operacji.
   12. System umożliwia generowanie raportów dotyczących statusu kompletności dokumentacji, wersji dokumentów, aktywności użytkowników itp.
   13. Elektroniczna wymiana dokumentów: System umożliwia bezpieczną wymianę dokumentów między użytkownikami oraz zewnętrznymi interesariuszami (np. CRO).
6. **Śledzenie historii zmian**
   1. System powinien posiadać moduł historii zmian (audit trail), który będzie odpowiedzialny za rejestrowanie zmian w wypełnionych formularzach. Rejestrowana będzie zmiana wartości poszczególnych atrybutów wraz z datą i nazwą użytkownika, który dokonał zmian.
   2. Lista wszystkich zmian danego formularza wraz z powyższymi atrybutami będzie dostępna na ekranie podglądu historii zmian tego formularza.
   3. System powinien tworzyć i utrzymywać log systemu, rejestrujący wszystkich użytkowników systemu i wykonane przez nich najważniejsze czynności z możliwością analizy historii zmienianych wartości danych. W zakres rejestrowanych czynności wchodzą m.in.: dodawanie i edycja dokumentów, edycja dynamicznych formularzy (edycja każdego pola w formularzu), logowanie/wylogowanie z systemu, dane dotyczące stacji roboczej, z której użytkownik się logował (adres IP, dane przeglądarki).
   4. System umożliwia filtrowanie zdarzeń po następujących danych: typ akcji, dane użytkownika dokonującego zmianę, dane użytkownika, wobec którego wprowadzono modyfikacje, zakres dat zdarzeń, typ obiektu (użytkownik/badanie).
   5. Poprzez mechanizm wersjonowania System będzie umożliwiał przywrócenie formularza do dowolnej wcześniej zapisanej jego wersji.
   6. System posiada możliwość wygenerowania całościowego podsumowania badania klinicznego po jego zakończeniu. Na podsumowanie zbierają się wszystkie załączone dokumenty (wygenerowanie eksportu wszystkich plików) i dane wprowadzone poprzez zdefiniowane formularze (generowanie raportu w formacie XLSX, CSV, PDF; generowanie raportu w formacie ustrukturyzowanej tabeli lub listy plików).
7. **Moduł monitorowania**
   1. System posiada wbudowane narzędzia do audytu wewnętrznego i zewnętrznego, umożliwiające generowanie raportów zgodności oraz śledzenie kompletności dokumentacji.
   2. System powinien posiadać odpowiedni moduł do monitorowania wprowadzanych danych. Moduł powinien umożliwiać zadawanie zapytań do danych wprowadzonych w formularzach (data query), jak również zatwierdzanie wprowadzonych danych i zabezpieczanie ich przed niekontrolowaną edycją. System musi zawierać funkcjonalność wysyłania powiadomień mailowych do wybranych użytkowników o utworzeniu data query oraz odpowiedzi na nie – przy czym wysyłka powiadomień musi następować automatycznie, nie może być zależna od osoby zgłaszającej/ odpowiadającej/ dokonującej modyfikacji.
   3. W ramach Modułu Użytkownik z odpowiednimi uprawnieniami powinien mieć możliwość zablokowania danego formularza przed dalszą jego edycją. Możliwość blokowania do edycji zweryfikowanych przez uprawnionych użytkowników formularzy oraz oznaczenia, że dane zostały zweryfikowane, a w przypadku modyfikacji po weryfikacji oznaczenie zakładki, że została ona zmodyfikowana. Zablokowanie formularza powinno być odwracalne (z opcją cofnięcia do ponownej weryfikacji).
   4. System powinien umożliwiać eksport raportu z kontroli danych do formatu PDF.
8. **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.
9. **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 8.1. 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.
10. **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 przez minimum 25 lat po zakończeniu każdego z badań.
11. **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. System będzie zapewniał bezpieczeństwo przetwarzanych i przechowywanych danych (FIPS PUB 199, <https://doi.org/10.6028/NIST.FIPS.199>).
    6. Na Systemie zostaną przeprowadzone testy bezpieczeństwa zgodnie z wytycznymi OWASP (OWASP Web Security Testing Guide).
    7. 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).
    8. 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.
    9. System powinien być dostępny całodobowo, a czynności techniczne wykonywane w czasie najmniejszego ruchu po ówczesnym uzgodnieniu terminu okna serwisowego z Zamawiającym.
    10. Wykonawca zapewni dostępność Systemu na poziomie 99% w skali roku.
    11. System musi działać co najmniej w polskiej oraz angielskiej wersji językowej. Użytkownik musi mieć możliwość wybrania wersji językowej.
    12. System musi posiadać podręcznik użytkownika w polskiej oraz angielskiej wersji językowej. System musi być wyposażony w wyszukiwarkę do przeglądania podręcznika użytkownika.
    13. Wykonawca zobowiązuje się do przeprowadzenia wdrożenia systemu, w tym migracji istniejących danych.
    14. Wykonawca przeprowadzi szkolenia personelu z obsługi dostarczonego rozwiązania.
    15. System musi być zbudowany w architekturze trójwarstwowej (warstwa danych, warstwa aplikacyjna, warstwa prezentacji).
    16. Warstwa danych musi wspierać możliwość pracy na następujących systemach bazodanowych, w wersjach aktualnie wspieranych przez producenta: Oracle/PostgreSQL, MS SQL, MySQL/MariaDB.
    17. 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).
    18. 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.
    19. Moduł uwierzytelniania użytkowników musi mieć możliwość integracji z bazą LDAP/Active Directory oraz mechanizmem OpenID, na podstawie, której będzie następowała autoryzacja operatora systemu.
    20. System powinien wspierać mechanizmy SSO (Single Sign On) w celu automatycznego uwierzytelnienia operatora na podstawie danych logowania do systemu operacyjnego klienta
    21. 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.
    22. 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.
    23. 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.
    24. System powinien być zintegrowany z posiadanym przez Zamawiającego systemem typu CTMS w zakresie min.: nr protokołu, akronim badania, tytuł badania w języku polskim, tytuł badania w języku angielskim, numer Eudra CT, numer EUCT, nazwa Sponsora. Przy tworzeniu nowej bazy dla badania system powinien mieć funkcjonalność polegającą na wyborze badań odpowiednio oznaczonych w systemie CTMS będącego w posiadaniu Zamawiającego (np. w formie listy rozwijalnej).
    25. Gotowość zintegrowania systemu z posiadanym przez Zamawiającego systemem typu CTMS w zakresie oznaczania badań, dla których uruchomiono eTMF. Szczegółowe wytyczne dotyczące integracji zostaną ustalone zostaną na etapie analizy przedwdrożeniowej.
12. **Szkolenia użytkowników**
    1. Wykonawca przeprowadzi szkolenia personelu z obsługi dostarczonego rozwiązania.
    2. Szkolenia z obsługi systemu eTMF powinny być dostosowane do różnych grup użytkowników i ich zakresu odpowiedzialności w badaniu klinicznym.
    3. Zakres szkolenia powinien obejmować minimum:

14.3.1. Szkolenia dla przedstawicieli Sponsora (Sponsor/CRO)

* Podstawowe funkcje systemu eTMF – logowanie, nawigacja, struktura folderów, podstawowe operacje na dokumentach.
* Zasady zarządzania dokumentacją – jak dodawać, aktualizować, zatwierdzać oraz wersjonować dokumenty.
* Zasady tworzenia szkoleń w systemie eTMF.
* Walidacja dokumentacji – procesy weryfikacji poprawności i kompletności dokumentów.
* Zarządzanie użytkownikami – nadawanie i odbieranie uprawnień, definiowanie ról w systemie.
* Audyt i ścieżka audytowa – przegląd logów systemowych, inspekcje regulacyjne.
* Zarządzanie dostępem dla ośrodków badawczych – sposób przydzielania dostępu do określonych dokumentów w ramach eTMF lub eISF.
* Bezpieczeństwo danych – polityka haseł, dostęp do dokumentów, kontrola edycji.

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

* Podstawowe funkcje eISF (electronic Investigator Site File) – logowanie, struktura folderów, przeglądanie dokumentów.
* Przesyłanie i odbieranie dokumentacji – jak dodawać dokumenty do eISF, pobierać dokumenty przesłane przez Sponsora.
* Zasady odbywania szkoleń w systemie eTMF/eISF.
* Weryfikacja wersji dokumentów – jak sprawdzać i zarządzać wersjonowaniem dokumentów, unikanie błędów w archiwizacji.
  1. Dopuszczalne formy szkoleń:
     + Materiały tekstowe i prezentacje PDF – dokumentacja szkoleniowa dostępna w eTMF/eISF.
     + Filmy szkoleniowe (video tutorials) – instruktaże dostępne w eTMF/eISF.
  2. W przypadku wprowadzenia do systemu istotnych zmian funkcjonalnych Wykonawca dostarczy odpowiednie materiały szkoleniowe dotyczące modyfikacji.