**OPIS PRZEDMIOTU SZACOWANIA**

1. Przedmiotem zamówienia jest: Wdrożenie systemu do obsługi Krajowej Sieci Onkologicznej
2. Wymagane funkcjonalności:

1. Podstawowa obsługa procesów KSO (SOLO I/II)

* Szybkie zakładanie nowych pacjentów i rejestrowanie wniosków, ograniczone do kluczowych funkcji.
* Intuicyjny, uproszczony interfejs zapewniający sprawne wdrożenie
i codzienną pracę personelu operacyjnego.

2. Rozszerzona funkcjonalność i zaawansowane moduły (SOLO III)

* Dodatkowy zakres narzędzi, obejmujący m.in. kompleksowe zarządzanie uprawnieniami i zaawansowany obieg dokumentów.
* Pełna kontrola nad systemem, w tym obsługa konsultacji wewnętrznych (np. w ramach konsyliów).
* Interfejs dostosowany do roli administratora lub zaawansowanego użytkownika, z dostępem do większej liczby funkcji konfiguracyjnych.

3. Różne widoki i poziomy dostępu w zależności od uprawnień

o Widok SOLO I/II:

* + - * Skoncentrowany na podstawowych zadaniach (rejestrowanie pacjentów i wniosków).
			* Ograniczona liczba dostępnych modułów i opcji, co pozytywnie wpływa na czytelność.
			* Uproszczone formularze i ścieżki pracy dla użytkowników, którzy nie potrzebują zaawansowanych funkcji.

o Widok SOLO III:

* + - * Pełna funkcjonalność systemu, w tym konfigurowanie ról
			i zezwoleń użytkowników dla SOLO I/II.
			* Rozbudowane narzędzia i raporty, umożliwiające kontrolę
			i nadzór nad procesami w szerszym zakresie.
			* Możliwość centralnego monitorowania i zarządzania wieloma instancjami (placówkami) w jednym panelu.

4. Centralne zarządzanie rolami i dostępami

* Definiowanie ról użytkowników w jednym miejscu, z podziałem na uprawnienia dotyczące SOLO I/II i SOLO III.
* Możliwość szybkiego nadawania lub modyfikowania dostępu, co wpływa na bezpieczeństwo i efektywność pracy.

5. System uwierzytelniania z kodami jednorazowymi

* Dodatkowa warstwa bezpieczeństwa, minimalizująca ryzyko nieuprawnionego dostępu.
* Wsparcie dla kodów SMS, aplikacji mobilnych czy innych mechanizmów autoryzacji.

6. Funkcje zgodne z wymogami KSO

* Moduły tworzenia pacjentów, koordynatorów, przypadków i wniosków, zgodnie z formalnymi ścieżkami onkologicznymi.
* Usprawnione zarządzanie procesem leczenia dzięki automatyzacji i integracji kluczowych danych.

7. Zaawansowane kalendarze i harmonogramy

* Planowanie wizyt i konsultacji z uwzględnieniem dostępności członków zespołu medycznego.
* Możliwość łatwego przesuwania terminów i aktualizowania grafików w czasie rzeczywistym.

8. Automatyczne walidacje danych

* Sprawdzanie poprawności PESEL, statusu wniosku i wymaganych pól przy wprowadzaniu informacji.
* Zmniejszenie liczby błędów i przyspieszenie obiegu dokumentów.

9. Elastyczne licencjonowanie i obsługa wielu jednostek

* Dodawanie nieograniczonej liczby użytkowników i placówek w ramach jednej licencji.
* Skalowalne rozwiązanie, przystosowane do rozwoju sieci placówek.

10. Generowanie podsumowań w PDF (np. konsultacji MDT)

* Automatyczne tworzenie dokumentacji ze spotkań MDT.
* Ułatwione raportowanie i archiwizacja przebiegu konsyliów.

11. Podgląd historii zmian

* Rejestracja wszystkich aktualizacji wniosków i innych kluczowych danych.
* Możliwość śledzenia i weryfikacji kroków oraz danych wprowadzanych w procesie.

12. Możliwości rozwojowe i dodatkowe moduły

* Architektura systemu pozwalająca na łatwe rozszerzanie funkcjonalności (np. nowe raporty, integracje, dedykowane formularze).
* Elastyczność dostosowywania rozwiązań do konkretnych potrzeb placówki.

13. Aktualizacje w ramach usługi

* Regularne dostarczanie poprawek i ulepszeń systemu, w tym dotyczących bezpieczeństwa.
* Brak dodatkowych kosztów za standardowe aktualizacje, gwarantujące ciągłe utrzymanie zgodności z wymogami formalnymi i prawnymi.
1. Wymagania techniczne i jakościowe

Elastyczność technologiczna: Zaproponowany system powinien zostać oparty na nowoczesnych technologiach i sprawdzonych architekturach, spełniających poniższe wymagania:

* + Frontend: Interfejs użytkownika systemu powinien zostać zrealizowany jako aplikacja web z wykorzystaniem nowoczesnego frameworka front-end (np. Angular, React, Vue lub równoważnego). Rozwiązanie to ma zapewnić wysoką interaktywność i responsywność aplikacji webowej.
	+ Backend i integracja: Logika aplikacji (back-end) powinna zostać zaimplementowana z użyciem architektury wielowarstwowej lub mikroserwisowej, co umożliwi skalowanie systemu oraz jego łatwą rozbudowę. Poszczególne moduły lub usługi powinny komunikować się za pomocą dobrze udokumentowanego interfejsu API, zgodnego z zasadami REST (np. RESTful API wykorzystujące format JSON) lub równoważnego standardu wymiany danych.
	+ Konteneryzacja: Do wdrożenia i uruchomienia systemu należy wykorzystać technologię konteneryzacji w celu zapewnienia przenośności i powtarzalności środowiska (np. kontenery Docker, Podman lub równoważne rozwiązanie kontenerowe). Konteneryzacja umożliwi łatwe wdrażanie aplikacji oraz utrzymanie spójnych warunków pracy pomiędzy środowiskami (deweloperskim, testowym i produkcyjnym).
	+ Baza danych: Warstwa przechowywania danych powinna opierać się na relacyjnym systemie zarządzania bazą danych (RDBMS) gwarantującym transakcyjność i integralność danych (np. PostgreSQL, Oracle, Microsoft SQL Server, MySQL lub równoważnym). Baza danych powinna zapewniać odpowiednią wydajność oraz możliwość skalowania wolumenu danych wraz z rozwojem systemu.
	+ Standardy i bezpieczeństwo: Wszystkie zastosowane rozwiązania techniczne i architektoniczne powinny odpowiadać aktualnym standardom branżowym, zapewniając wysoki poziom bezpieczeństwa, wydajności i niezawodności systemu. Ponadto należy stosować najlepsze praktyki (m.in. aktualne wersje frameworków i bibliotek, właściwe mechanizmy uwierzytelniania i autoryzacji, szyfrowanie transmisji danych oraz ochronę danych wrażliwych), tak aby system SOLO był odporny na typowe zagrożenia i spełniał obowiązujące wymagania w zakresie ochrony danych.

Zamawiający wymaga aby dostarczone oprogramowanie znajdowało się w infrastrukturze On-prem Zamawiającego. Zamawiający dysponuje serwerem o poniższych parametrach:

Procesor: Intel® Xeon® Gold 5218B CPU @ 2.30GHz

Pamięć operacyjna (RAM): 16 GB DDR4 ECC

Dysk twardy: 1 TB

Środowisko wirtualizacyjne: Vmware lub Proxmox

Zamawiający wymaga wdrożenia dostarczonego rozwiązania w zakresie co najmniej instalacji, konfiguracji i szkoleń użytkowników.

1. Ogólne wymagania dotyczące bezpieczeństwa

Wykonawca zobowiązany jest do zapewnienia, że tworzone oprogramowanie spełnia aktualne standardy bezpieczeństwa informatycznego, w szczególności:

* Zapewnia ochronę danych osobowych i danych wrażliwych zgodnie z RODO,
* Uwzględnia zasadę **privacy by design** oraz **security by design**,
* Spełnia wymagania zawarte w **OWASP Top 10** oraz **OWASP API Security Top 10**.

5. Wymagane testy bezpieczeństwa

Przed odbiorem końcowym wykonawca zobowiązany jest do przeprowadzenia następujących testów i przedstawienia ich wyników w formie raportu:

5.1. Testy penetracyjne (pentesty)

* Zakres: aplikacja webowa, API, zaplecze administracyjne.
* Metoda: white-box lub grey-box.
* Raport musi zawierać: opis znalezionych podatności, ich klasyfikację wg CVSS, rekomendacje naprawcze.

5.2. Testy podatności (vulnerability scan)

* Zautomatyzowane skanowanie aplikacji.
* Wymagana eliminacja wszystkich podatności o ocenie CVSS ≥ 7 przed odbiorem.

5.3. Testy bezpieczeństwa API

* Sprawdzenie poprawności autoryzacji przykładowo: rate limiting, input validation, ochrony tokenów.
* Ochrona przed nadużyciami typu "mass assignment", "broken object level authorization".

5.4. Testy transmisji danych

* Wymagane jest szyfrowanie komunikacji z użyciem TLS 1.2 lub wyższego.
* Zakaz przesyłania danych wrażliwych w nieszyfrowanej postaci (np. HTTP, e-mail plaintext).

5.5. Testy kontroli dostępu

* Testy uprawnień i izolacji danych między użytkownikami.
* Weryfikacja mechanizmów logowania i odzyskiwania dostępu.

6. Zgodność z regulacjami i standardami

Wykonawca zobowiązany jest do zapewnienia, aby system realizował wymagania określone w:

* **Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności (KRI),**
* **Ogólnym Rozporządzeniu o Ochronie Danych Osobowych (RODO),**
* **Zasadach dobrych praktyk bezpieczeństwa aplikacji (zgodnie z aktualną listą OWASP Top 10),**

w zakresie adekwatnym do charakteru systemu, rodzaju przetwarzanych danych oraz jego przeznaczenia w środowisku teleinformatycznym Zamawiającego. W szczególności wymagane jest:

* stosowanie bezpiecznych protokołów komunikacyjnych (np. HTTPS z aktualnym certyfikatem),
* silne mechanizmy uwierzytelnienia użytkowników (np. hasła, MFA),
* kontrola dostępu na poziomie użytkownika i danych,
* rejestrowanie i nadzór nad operacjami w systemie (logi dostępu i działań),
* zapewnienie ciągłości działania oraz szyfrowania danych wrażliwych w spoczynku i transmisji,
* możliwość eksportu danych w otwartych formatach zgodnie z KRI,
* eliminacja podatności zakwalifikowanych jako wysokie lub krytyczne (CVSS ≥ 7),
* przedstawienie dokumentacji bezpieczeństwa (lub jej draftu) na etapie odbioru.

7. Wymagania organizacyjne i procesowe

* Wykonawca przedstawi **Plan Zarządzania Bezpieczeństwem Informacji** w trakcie realizacji zamówienia.
* Wykonawca zobowiązany jest do niezwłocznego (maks. 24h) zgłaszania wszelkich **incydentów bezpieczeństwa** Zamawiającemu.
* Oprogramowanie musi mieć mechanizmy:
	+ Rejestrowania logów dostępu i działań użytkowników,
	+ Backupów danych i ich ochrony,
	+ Automatycznego wylogowania po bezczynności,
	+ Weryfikacji dwuskładnikowej (MFA) dla kont administracyjnych.

8. Zarządzanie podatnościami

Zamawiający zastrzega sobie prawo do zlecenia niezależnego audytu bezpieczeństwa i przekazania wyników Wykonawcy celem wprowadzenia poprawek.

9. Dokumentacja i raportowanie

Wykonawca dostarczy:

* Raport z testów bezpieczeństwa,
* Raport zgodności z OWASP i RODO,
* Instrukcję bezpieczeństwa systemu,
* Dokumentację techniczną zawierającą konfigurację serwera

10. Nadzór techniczny

a) Stabilność i ciągłość działania systemu

* Zapewnienie pełnej operacyjności systemu Zintegrowanego Wsparcia Przepływu Danych w środowisku produkcyjnym.
* Monitoring dostępności usług i infrastruktury w trybie 24/7 z alertowaniem o incydentach oraz awariach.
* Utrzymanie zgodności systemu z aktualnymi wersjami wykorzystywanych technologii, w tym Docker, PostgreSQL, Next.js, React, oAuth, RESTful API.
* Kontrola i utrzymanie integralności baz danych (np. PostgreSQL, Oracle, Microsoft SQL Server, MySQL lub równoważnym) optymalizacja zapytań oraz strategii indeksowania dla poprawy wydajności.
* Gotowość do przeprowadzania testów wydajnościowych i obciążeniowe aplikacji webowych oraz interfejsów API.
* Bieżące aktualizacje i poprawki bezpieczeństwa, w tym przeglądy kodu pod kątem podatności na ataki (CVE, OWASP Top 10).
* Regularne testy disaster recovery oraz utrzymanie strategii backupów dążącej do RTO < 3h i RPO < 1h.

b) Obsługa zgłoszeń i wsparcie techniczne

* Obsługa zgłoszeń serwisowych i technicznych dla jednostek SOLO I / SOLO II oraz centralnej jednostki NIO-PIB
* Priorytetyzacja zgłoszeń krytycznych i awaryjnych (nieobjętych umową wdrożeniową) w systemie ticketowym ITSM z czasem reakcji i rozwiązania:
* Krytyczne (P1) – reakcja 2h od zgłoszenia – rozwiązanie 48 godzin
* Zwykły (P2) – reakcja 48h od zgłoszenia – rozwiązanie 10 dni roboczych
* Utrzymanie systemu ticketowego umożliwiającego zgłaszanie, śledzenie i eskalację incydentów oraz problemów.
* Bieżące wsparcie w zakresie integracji systemu KSO z innymi systemami dziedzinowymi za pomocą API RESTful.

c) Infrastruktura i zarządzanie środowiskiem IT

* Zarządzanie środowiskiem aplikacyjnym i serwerowym dla SOLO I/SOLO II oraz NIO-PIB, w tym zarządzanie kontenerami Docker oraz klastrami Kubernetes (jeśli dotyczy).
* Utrzymanie infrastruktury w Europejskim Obszarze Gospodarczym z zapewnieniem zgodności z RODO oraz regulacjami dotyczącymi ochrony danych medycznych i instytucjonalnych.
* Zapewnienie mechanizmów wysokiej dostępności (HA) i równoważenia obciążenia (load balancing) dla aplikacji frontendowych oraz backendowych.
* Monitorowanie zużycia zasobów infrastrukturalnych (CPU, RAM, IOPS, throughput) oraz proaktywne skalowanie poziome/pionowe.
* Prowadzenie dokumentacji technicznej systemu oraz zmian konfiguracyjnych.

11. Czas trwania umowy: 36 miesięcy