GDAŃSKI UNIWERSYTET MEDYCZNY

AGENCJA BADAŃ MEDYCZNYCH

MODYFIKACJA 23.07.2024 **Załącznik 3 do SWZ**

OPIS PRZEDMIOTU ZAMÓWIENIA

Spis treści

MODYFIKACJA 23.07.2024 **Załącznik 3 do SWZ**

Na potrzeby realizacji założeń projektu Interdyscyplinarnego Pomorskiego Centrum Medycyny Cyfrowej, Gdański Uniwersytet Medyczny planuje dokonać zakupu środowiska wykonawczego, usług, narzędzi, asysty technicznej i gwarancji dla Platformy IP_CMC pozwalającej na wdrożenie innowacyjnych instrumentów w zakresie cyfryzacji.

1. Określenie przedmiotu zamówienia

Przedmiotem zamówienia jest zakup środowiska wykonawczego, usług i narzędzi umożliwiających wytworzenie, instalację i konfigurację, a także uruchomienie produkcyjne oraz zapewnienie asysty technicznej i gwarancji dla Platformy Interdyscyplinarnego Pomorskiego Centrum Medycyny Cyfrowej, pozwalającej na wdrożenie innowacyjnych instrumentów w zakresie cyfryzacji. Na terenie Gdańskiego Uniwersytetu Medycznego (GUMed) utworzono Interdyscyplinarne Pomorskie Centrum Medycyny Cyfrowej (IP_CMC) które przygotowuje odpowiednie środki informatyczne i organizacyjne do przetwarzania danych medycznych dla prowadzenia badań naukowych w obszarze medycyny, w tym niekomercyjnych badań klinicznych. Platforma IP_CMC zapewnia dostępność danych zanonimizowanych w postaci elektronicznej oraz narzędzi do ich automatycznej analizy, agregowania, przetwarzania do postaci użytecznej dla konkretnego projektu badawczego. Platforma IP_CMC umożliwia użycie przez badaczy odpowiednich narzędzi uczenia maszynowego, sztucznej inteligencji oraz przetwarzających duże zbiorniki danych do udowadniania tez naukowych, identyfikację nowych, nieznanych wzorców i trendów, automatyczną segmentację przypadków (badawczych, diagnostycznych, itd.), automatyczne rozpoznawanie wzorców (np. miejsc patologicznych, guzów, itp.) na obrazach i inne, nieosiągalne dotychczas efekty. Platforma IP_CMC posiada duże zbiory danych tabularycznych, obrazowych (wysokiej jakości) i omicznych. Zakres danych udostępnianych przez IP_CMC zawiera dane kliniczne pacjentów Uniwersyteckiego Centrum Klinicznego (UCK), dane demograficzne, dane populacyjne, dane genetyczne.

W celu realizacji założeń projektu Interdyscyplinarnego Pomorskiego Centrum Medycyny Cyfrowej zostanie zbudowana Platforma IP_CMC do przetwarzania i analizy danych medycznych, w oparciu o którą będą działały wirtualne laboratoria badawcze. W wyniku prowadzenia prac badawczych w wirtualnych laboratoriach zostanie w przyszłości wytworzony szereg rozwiązań informatycznych, narzędzi i algorytmów sztucznej inteligencji, np.:

1. Narzędzia do oceny CAC (Coronary Artery Calcium) score.
2. Narzędzia do analiz rozedmy w badaniach tomografii komputerowej klatki piersiowej, zarówno standardowej jak i niskodawkowej.
3. Wirtualny Patolog – zbiór narzędzi do standaryzacji, segmentacji i ewaluacji (np. oceny tzw. TIL-Tumor-Infiltrating Lymphocytes score) skanów barwionych wycinków tkankowych.
4. Narzędzia automatyzujące przeprowadzanie analiz biostatystycznych i bioinformatycznych przez badaczy do samodzielnego wykorzystania.
5. Autorskie algorytmy AI, które oceniają potencjalne zachowanie pacjenta i prawdopodobieństwo stosowania terapii.

Na potrzeby realizacji przedmiotu zamówienia niezbędne będzie dostarczenie przez Wykonawcę następujących komponentów:

1. Repozytorium Danych Tabularycznych – środowiska hurtowni danych lub Data Lakehouse lub podobnego typu utrzymującego dane medyczne zgodnie z międzynarodowym standardem FHIR. Repozytorium będzie zasilane poprzez połączenie ze źródłowymi systemami za pomocą plików płaskich. Projekt techniczny opisujący łączność za pomocą strumienia komunikatów API.

2. Repozytorium Danych Obrazowych i Omicznych – środowiska umożliwiającego odrębne przechowywanie oraz archiwizację dużych plików danych, referencyjnych danych obrazowych oraz omicznych w plikach obiektowych oraz referencji do tych obiektów/plików.
3. Anonimizator danych tabularycznych, danych omicznych oraz danych obrazowych – opartego na algorytmach sztucznej inteligencji wraz z modułem autodetekcji kodów i terminologii medycznych.
4. Komponentów Bezpieczeństwa – odpowiedzialnych za bieżący monitoring i kontrole dostępu do danych oraz przeciwdziałania potencjalnym atakom, przy założeniu, że Platforma nie jest otwarta na Internet.
5. Chmury Obliczeniowej - środowiska uruchomieniowego w obszarze Unii Europejskiej do uruchomienia wszystkich komponentów Platformy IP_CMC.
6. Sprzęg z Partnerami zewnętrznymi (zawierający API oraz mechanizmy wymiany danych plikowych) – umożliwiającego zasilanie i wymianę plików z systemami źródłowymi z danymi tabularycznymi, obrazowymi i omicznymi oraz obsługę procesu ETL odpowiedzialnego za pobieranie danych źródłowych, z tym że dla sprzęgu API zostanie przygotowany jedynie projekt techniczny bez implementacji (wykonania)
7. Indywidualnych Laboratoriów Wirtualnych do celów statystycznych i badań naukowych – zawierających Workspace'y umożliwiające samodzielną analizę przez klinicystów udostępnianych przez IP_CMC wybranych danych, generowanie fenotypów badawczych i budowy zaawansowanych modeli klasy AI/ML.
8. W celu realizacji powyższych założeń Wykonawca zobowiązany będzie do:
    a. Zaprojektowania i wykonania Platformy dla IP_CMC, realizującej określone w OPZ funkcjonalności minimalnie w zakresie wymienionych powyżej komponentów.
    b. Zaprojektowania interfejsów integracyjnych dla systemów Partnerów współpracujących z IP_CMC (bez implementacji) oraz zaprojektowanie i wykonanie integracji z UCK poprzez pliki.
    c. Implementacji Interfejsów Integracyjnych do eksportu wyników prac z Laboratoriów Wirtualnych.
    d. Dostarczenie usług wsparcia w integracji systemów dziedzinowych i Platformy IP_CMC.
    e. Współpracy z Zamawiającym w zakresie doprecyzowania raportów i analiz do dostarczenia dla celów zarządzania i nadzoru nad działaniem IP_CMC, platformy chmurowej oraz efektywności badań w Laboratoriach Wirtualnych.
    f. Przekazania kodu źródłowego oraz przeniesienie praw autorskich majątkowych (o ile jest to wymagane przez Umowę) lub udzielenie licencji do oprogramowania, w szczególności do wykonanego Oprogramowania dedykowanego, Oprogramowania Systemowego, spełniającego wymagania funkcjonalne i pozafunkcjonalne określone w OPZ.
    g. Udostępnienia wypracowanych i wykonanych interfejsów oraz integracji systemów bez jakichkolwiek obciążeń licencyjnych.
    h. Dostawy silników baz danych oraz pojemników na pliki i obiekty, na którym ma się opierać działanie Platformy IP_CMC wraz z niezbędną liczbą licencji do pracy wyżej wymienionego Oprogramowania, w tym wymaganych dla kadry Zamawiającego.
    i. Dostawy Oprogramowania Systemowego niezbędnego do prawidłowego działania infrastruktury technicznej.
    j. Zaprojektowania i wykonanie interfejsów dla poszczególnych komponentów Platformy IP_CMC.

k. Instalacja, wdrożenie, konfiguracja i uruchomienie Oprogramowania na infrastrukturze technicznej chmury obliczeniowej.
l. Przeszkolenia personelu Zamawiającego oraz użytkowników Platformy IP_CMC z obsługi Oprogramowania oraz komponentów technicznych, w tym minimalnie platformy chmurowej, oprogramowania bazodanowego, systemów operacyjnych serwerów, systemów kolejkowych, systemów ETL, usług chmurowych oraz modeli danych.
m. Dostarczenia materiałów szkoleniowych do przeszkolenia personelu w przyszłości.
n. Świadczenia usług gwarancyjnych i asysty technicznej, wobec całości dostarczonego i zrealizowanego przedmiotu zamówienia od daty końcowego odbioru systemu przez okres określony Umową.
o. Realizacji dodatkowych prac, w ramach prawa opcji, w liczbie 2400 osobo godzin pracy zespołu projektowego w ramach prawa opcji Zamawiającego.
p. Dostarczenia kompletnej i aktualnej dokumentacji wdrażanej Platformy zgodnie z listą opisaną w OPZ.
q. Dostarczenia kompletnej i aktualnej dokumentacji projektowej zgodnie z listą opisaną w OPZ.

2. Cele Projektu Interdyscyplinarnego Pomorskiego Centrum Medycyny Cyfrowej

Celem projektu IP_CMC jest umożliwienie przeprowadzenia badań klinicznych za pomocą narzędzi informatycznych w ramach budowanej przez GUMed koncepcji medycyny cyfrowej.

3. Kamienie milowe projektu

Zamawiający zakłada realizację projektu zgodnie z Fazami wskazanymi w załączniku nr 7 do Umowy.

4. Opis wymagań funkcjonalnych i niefunkcjonalnych Platformy

4.1 Definicja wymagań funkcjonalnych i niefunkcjonalnych

Uwzględniając realizację założeń projektu, budowy Platformy IP_CMC, Wykonawca zobowiązany będzie do dotrzymania realizacji wymagań funkcjonalnych i niefunkcjonalnych, opisanych poniżej przez Zamawiającego.

Poprzez wymagania funkcjonalne Zamawiający rozumie funkcjonalność tworzonego oprogramowania. Wymagania niefunkcjonalne określają natomiast pożądane cechy tworzonego systemu. Dotyczą one min. wydajności, dostępności, niezawodności, skalowalności i przenośności.

Zamawiający jako obligatoryjne wymagania niefunkcjonalne określa:

1. Jakość systemu w odniesieniu do bezpieczeństwa, dokładności obliczeń, interoperacyjności oraz zgodności z obowiązującymi standardami.
2. Niezawodność systemu w szczególności w odniesieniu do odporności na awarie, tolerancji dla błędów czy odzyskania pełnej funkcjonalności systemu po wystąpieniu awarii
3. Użytkowanie systemu, takie jak łatwość użytkowania oraz obsługi aplikacji,
4. Efektywność systemu w odniesieniu do zachowania w czasie (np. czasu obliczeń) lub wykorzystania zasobów

5. Zmienność systemu w odniesieniu do stabilności i sprawdzalności systemu, zdolności do analizy i zmiany
6. Możliwości przenoszenia systemu w szczególności dotyczące zdolności adaptacyjnych, zdolności instalacyjnych, możliwości zastąpienia i odpowiedniej zgodności z obowiązującymi standardami

Funkcjonalność Platformy IP_CMC jest powiązana bezpośrednio z realizacją celów dla medycyny cyfrowej wskazanych w projekcie „Tworzenia i Rozwoju Regionalnych Centrów Medycyny Cyfrowej" Agencji Badań Medycznych. Do podstawowych zadań Platformy IP_CMC należeć będzie:

1. Standaryzacja pozyskiwania i przetwarzania danych medycznych dla celów naukowych, analityki i statystyki klinicznej.
2. Gwarantowanie bezpiecznej wymiany danych pomiędzy IP_CMC a Partnerami oraz klinicystami.
3. Utrzymanie danych w zbiornikach danych źródłowych (niezmieniane), danych zgodne z metamodelem IP_CMC, danych zgodne z obowiązującymi standardami tj. HL7 FHIR, DICOM oraz w standardach ustalonych z Zamawiającym.
4. Umożliwienie pracy na danych nieustrukturyzowanych (m.in. obrazowe dokumentacje medyczne oraz pliki omiczne).
5. Ekstrakcja informacji z danych medycznych w formie tekstu ciągłego (np. epikryz).
6. Wykonanie pseudonimizacji danych wejściowych (tabularycznych, obrazowych i omicznych) w buforze dla Partnerów, a także anonimizacji i pseudonimizacji danych na potrzeby dalszej analityki i budowania modeli danych.
7. Dostarczanie narzędzi i algorytmów sztucznej inteligencji (ang. AI), ogólnodostępnych tzw. „z półki", do analiz o charakterze prognostycznym i predykcyjnym oraz udostępnianie pełnego środowiska do samodzielnego budowania modeli AI oraz uczenia maszynowego (ang. ML) w oparciu o kod Python i R.
8. Umożliwienie wsparcia badań klinicznych w odpowiedni sposób zarządzając udostępnianymi zestawami danych.
9. Umożliwienie w przyszłości łatwej implementacji przesyłania danych w sieci Centrów Medycyny Cyfrowej zgodnie z wymaganiami ABM za pomocą wymiany ustandaryzowanych danych poprzez interfejs API REST.
10. Zebranie odpowiedniego potencjału infrastrukturalno-programowego dla obecnego zbioru danych oraz przyszłego rozwoju IP_CMC.
11. Umożliwienie świadczenia usług medycyny cyfrowej w ramach projektów badawczych na różnych polach, tj. Informatyka Medyczna, Telemedycyna, Obrazowanie Medyczne, Analityka Danych Medycznych, Sztuczna Inteligencja w Medycynie w każdej z dziedzin medycyny zajmujących się diagnostyką, leczeniem i profilaktyką chorób.

Tworzona przez Wykonawcę Platforma IP_CMC powinna spełniać wymagania obligatoryjne wskazane poniżej przez Zamawiającego:

MODYFIKACJA 23.07.2024 **Załącznik 3 do SWZ**

Nr	Punkt kontrolny
F.1	Platforma IP_CMC będzie obsługiwać uznane międzynarodowe standardy i profile interoperacyjności, a także ich krajowe specyfikacje pochodne, tj.: 1. HL7 CDA lub/i HL7v2 lub/i L7 FHIR 2. DICOM 3. OMOP lub inny wspierający analizę danych medycznych Format własny oparty o plik JSON obowiązujący obecnie w komunikacji między GUMED a UCK - w celu zachowania kompatybilności. Inne formaty danych są przetwarzane procesami (ETL) na formaty wspierane przez Platformę IP_CMC.
F.2	Procesy anonimizacji i pseudonimizacji danych medycznych będą wdrożone tak, aby uniknąć zmniejszenia lub zamazania wartości badawczej danych, które będą przetwarzane na Platformie IP_CMC. Jednocześnie przyjęte procesy będą odporne na błędy w zapisach i samych danych, a także umieszczanie danych osobowych w miejscach do tego celu nieprzeznaczonych. Mechanizmy będą obsługiwać wiele źródeł pochodzenia danych (wielu Partnerów, wiele kanałów) oraz mnogość formatów danych wejściowych, w tym takich, które są niezgodne z żadnym formatem gwarantującym interoperacyjność. Z tego względu proces anonimizacji i pseudonimizacji powinien być dostosowany do konkretnego formatu danych i rodzaju informacji zawartych w zbiorze medycznym.
F.3	Mechanizmy anonimizacji i pseudonimizacji dostępne są z poziomu narzędzi i katalogu usług Platformy IP_CMC i akceptują na wejściu ustrukturyzowane i nieustrukturyzowane dane oraz dane obrazowe i omiczne. Uczenie tych mechanizmów poprawnego i pełnego działania na danych osobowych następuje w wydzielonym środowisku. Proces anonimizacji i pseudonimizacji danych polega na określeniu modelu z wyuczonymi kryteriami maskowania oraz wyborze metody maskowania z katalogu usług. Jednocześnie przetwarzanie procesów maskujących może odbywać się ręcznie, dynamiczne "on the fly" i również w sposób wsadowy.

F.4	W kontekście ochrony danych osobowych i wrażliwych Platforma IP_CMC będzie wspierać następujące funkcje: 1. usuwanie informacji identyfikujących jednoznacznie pacjenta, a w przypadku braku takiej możliwości odkładanie takich danych do wydzielonej Poczekalni Partnera, 2. anonimizacja danych obejmuje usuwanie wszystkich informacji, które mogą identyfikować pacjenta, tj: imię, nazwisko, identyfikator pacjenta, adres, korelacje z bazami Partnerów, statusu VIP itp. W przypadku przetwarzania danych nie będących danymi osobowymi, ale które mogą sugerować konkretną osobę dane medyczne należy wymieszać zgodnie z przyjętym algorytmem z Zamawiającym, np. przesuwając cały set danych w czasie, dodając reguły hash'ujące oraz ustalić odpowiednią metodę z Zamawiającym 3. zmiana identyfikatorów unikalnych (ID) - konieczne jest dokonanie zmiany ID w sposób, który uniemożliwia identyfikację pacjenta. W tym celu w Poczekalni Partnera albo na wejściu do IP_CMC musi być możliwy wybór czy zastosować anonimizację nieodwracalną czy pseudonimizację odwracalną (mapowanie realnych ID na ID wymyślone zgodnie z bazą będącą w gestii Partnera lub GUMed), 4. szyfrowanie danych, aby dodatkowo zabezpieczyć informacje, zwłaszcza gdy istnieje ryzyko powiązania danych medycznych zanonimizowanych z realną osobą na podstawie skojarzeń i relacji, 5. odpowiedzialna i inteligentna ochrona danych - głównym wymaganiem dla mechanizmów ochrony danych osobowych jest oprócz kwestii bezpieczeństwa zachowanie informacji medycznych w formie mającej wartość naukową oraz przydatnej w kontekście badań klinicznych czy analiz, 6. kontrolowanie dostępu do danych jest wymagane na każdym poziomie pracy na Platformie CMC, w szczególności dostęp do Poczekalni Partnera powinni mieć wyłącznie pracownicy Partnera, 7. dokumentowanie dla celów audytowych proces anonimizacji i pseudonimizacji dla zapewnienia transparentności.
F.5	Platforma IP_CMC zapewnia bezpieczne środowisko dostępu do zaufanych danych, umożliwia wdrożenie automatyzowanych procesów AI, integrowanie z AI oraz aplikacjami chmurowymi w ramach współpracy grupowej wielu osób o różnych kompetencjach (osoby techniczne, merytoryczne). A także umożliwia używanie zintegrowanych zestawów narzędzi umożliwiających naukowcom, programistom i analitykom możliwość bardzo szybkiego wdrożenia modeli analitycznych z wykorzystaniem dedykowanych zewnętrznych API.
F.6	Na Platformie IP_CMC dostępne są dedykowane usługi umożliwiające budowę, uruchamianie modeli i obsługę modeli uczenia maszynowego przy pomocy kart graficznych (GPU). Platforma zapewnia możliwość budowania modeli głębokich sieci neuronowych ze wsparciem obliczeń na GPU.

F.7	Proces przygotowywania modeli do analiz w laboratoriach będzie się składał minimalnie z następujących kroków: 1. Ekstrakcja danych z Data Lakehouse 2. Pozyskiwanie danych 3. Rozkładanie danych 4. Rozumienie i badanie jakości danych 5. Przeprowadzenie uczenia modeli 6. Eksperymenty z danymi 7. Wprowadzenie modelu na realnej pracy 8. Utrzymanie modelu
F.8	Każdy zestaw danych wpadający do Data Lakehouse zostanie zaindeksowany przez odpowiedni moduł służący do katalogowania danych. Moduł ten oprócz przechowywania referencji do danych, co pozwoli na przeszukiwanie katalogu, będzie też zawierał informacje o wymaganej retencji danych i ustawieniach dot. sposobu pozyskania i czasu życia danych.
F.9	Dane kliniczne powinny być udostępnione w kontrolowanym środowisku z możliwością audytu kto, w jakiej formie i kiedy udostępnił dane. Klinicyści będą korzystać z modułu dostępu do danych, gdzie będą przeglądać i przeszukiwać wachlarz dostępnych danych, jak również składać wnioski o przygotowanie danych i ich udostępnienie w części laboratoryjnej. Wniosek o dostęp musi zostać zaakceptowany przez operatora Platformy IP_CMC przed udostępnieniem danych. Jednocześnie dane zaakceptowane powinny być widoczne wyłącznie w zbiorze danych (ang. Data Mart) wnioskującego. System zapamięta kto, kiedy i o jakie dane wnioskował, w celach audytu oraz kontroli dostępu.
F.10	Wykonawca przygotuje zbiory uczące i zapytania (ang. Prompt) dla modeli anonimizujących dane osobowe oraz modeli ekstrachujących informacje z tekstu ciągłego (np. epikryz) na potrzeby wykonania anonimizacji danych importowanych do Platformy IP_CMC od Partnerów.
F.11	Skuteczność rozwiązań anonimizujących powinna wynosić F1 >= 0.99, również z tekstu ciągłego (np. epikryz). W przypadku nieosiągnięcia takiego wyniku Wykonawca przygotuje rozwiązanie, które przypadki wątpliwe będzie kierował do ludzkiego moderatora, który podejmie decyzję o anonimizacji.
F.12	Skuteczność modelu ekstrahującego informacje z tekstu ciągłego (np. epikryz) powinna wynosić F1 >= 0.85.
F.13	IP_CMC zakłada otrzymywanie danych w różnorodnych formatach, dlatego integracja i standaryzacja danych jest jednym z ważniejszych celów IP_CMC. Z tego powodu Platforma IP_CMC musi być rozwiązaniem automatyzującym logistykę związaną z pozyskiwaniem i dostępem do danych.
F.14	Platforma IP_CMC będzie przygotowana w taki sposób, aby można było przeprowadzić certyfikację rozwiązania na zgodność z wymaganiami procedur, standardów i mechanizmów informatycznych zapewniających bezpieczeństwo przetwarzanych danych i informacji oraz zapewniających ciągłość działania systemu. W tym szeroko rozumiany IT Governance i Data Governance (wdrożenie norm ISO 27001 i 22301 oraz spełnienie wymagań regulacji RODO).

F.15	Platforma IP_CMC zawiera, oprócz zbiorników danych także przestrzeń badawczą w środowisku zinformatyzowanym i również wspiera użycie narzędzi do analizy biostatystycznej i bioinformatycznej, uczenia maszynowego, tworzenia i testowania algorytmów sztucznej inteligencji.
F.16	Sposób prezentacji i dostępu do danych będzie wspierał wyszukiwanie kontekstowe. Wyszukiwanie odbywa się po określonej liście atrybutów.
F.17	Dostarczona zostanie funkcjonalność Modułu Feasibility umożliwiająca: • spójne prezentowanie danych pochodzących z różnych źródeł (nałożenie abstrakcji na zaimportowane dane), poprzez jednolite nazwy trybutów, łączenie grup danych w zdefiniowane typy obiektów takie jak np.: diagnoza, hospitalizacja, badanie, lekarz oraz musi pozwalać na łatwe wyszukiwanie pacjentów według zadanej kwerendy, • zakres danych zaimportowanych z różnych źródeł, musi być zgodny z minimalnym zakresem danych wskazanym w standardzie FHIR; tworzenie zapytań bez posiadania specjalistycznej wiedzy z zakresu obsługi baz danych, programowania czy statystyki; Użytkownik z podstawową wiedzą medyczną powinien być w stanie wygenerować zapytanie, • tworzenie kryteriów definiowania i wyszukiwania grup pacjentów z posiadanej bazy danych, • wyszukiwanie grup pacjentów na podstawie dowolnie zdefiniowanych schematów leczenia, • wyświetlenie wszystkich innych zdarzeń występujących między dwoma zależnymi w czasie zdarzeniami, • zawężenie wyników wyszukiwania do danego przedziału czasu np. ostatni miesiąc, ostatni kwartał, dowolny zakres dat itp. • definiowanie kryteriów wyszukiwania (w tym opartych o schematy leczenia).

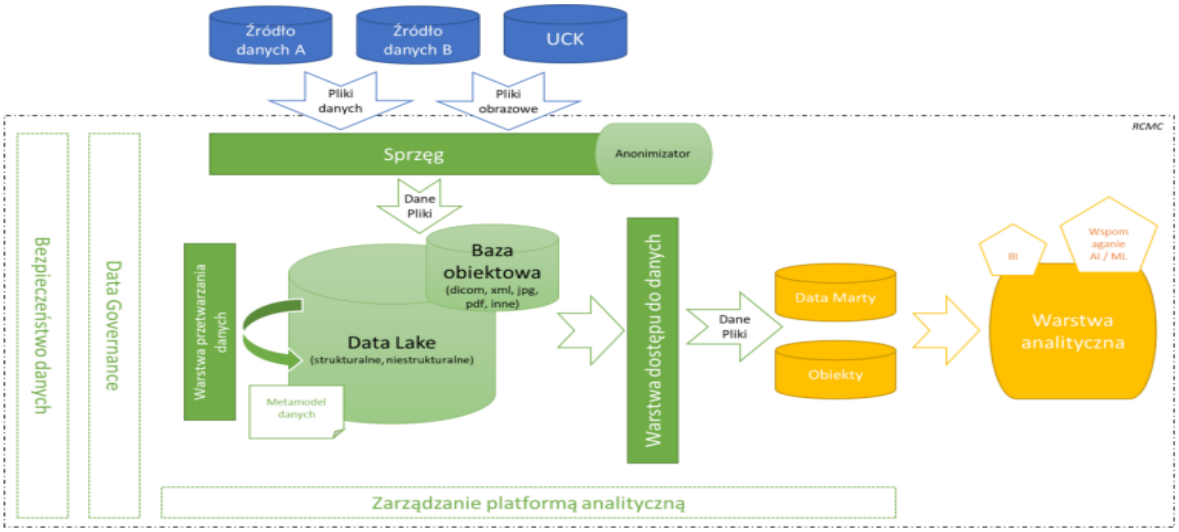
4.2 Wymagania ogólne dla architektury Platformy IP_CMC

W celu realizacji założeń projektu Interdyscyplinarnego Pomorskiego Centrum Medycyny Cyfrowej zostanie zbudowana Platforma przetwarzania i analizy danych medycznych, w oparciu o którą będą działały wirtualne laboratoria badawcze. Dostęp do danych zgromadzonych w IP_CMC będą mieć dostęp zarówno poszczególni naukowcy czy badacze, jak i partnerzy Gdańskiego Uniwersytetu Medycznego, np. inne uczelnie czy środowiska naukowe.

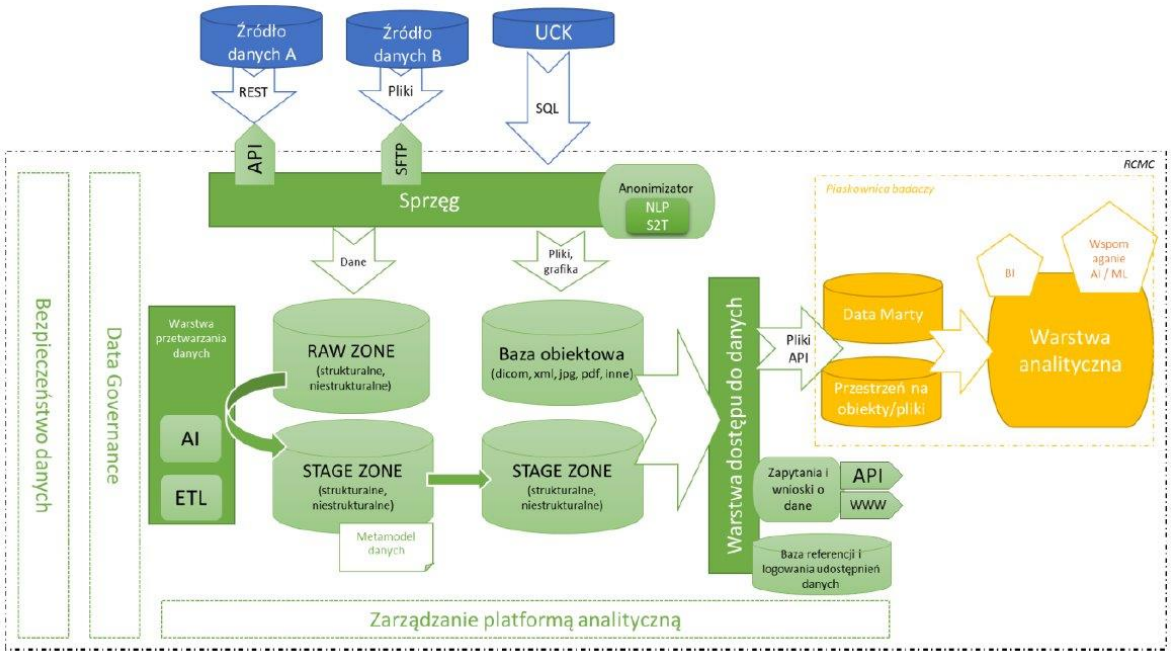
Szczegółowe założenia architektury Platformy IP_CMC działającej w środowisku chmurowym przedstawiono na poniższych rysunkach architektonicznych, ilustrujących przepływy danych na styku z dostarczycielami danych (część niebieska) oraz przepływy wewnętrzne (część zielona). Na architekturze wskazano część IP_CMC odpowiedzialną za analitykę danych, czyli za udostępnianie danych dla naukowców w układzie danych wymaganym do badań – tę część analityczną zaznaczono kolorem pomarańczowym

MODYFIKACJA 23.07.2024 **Załącznik 3 do SWZ**

Schemat ogólny architektury IP_CMC działającego w środowisku chmurowym:

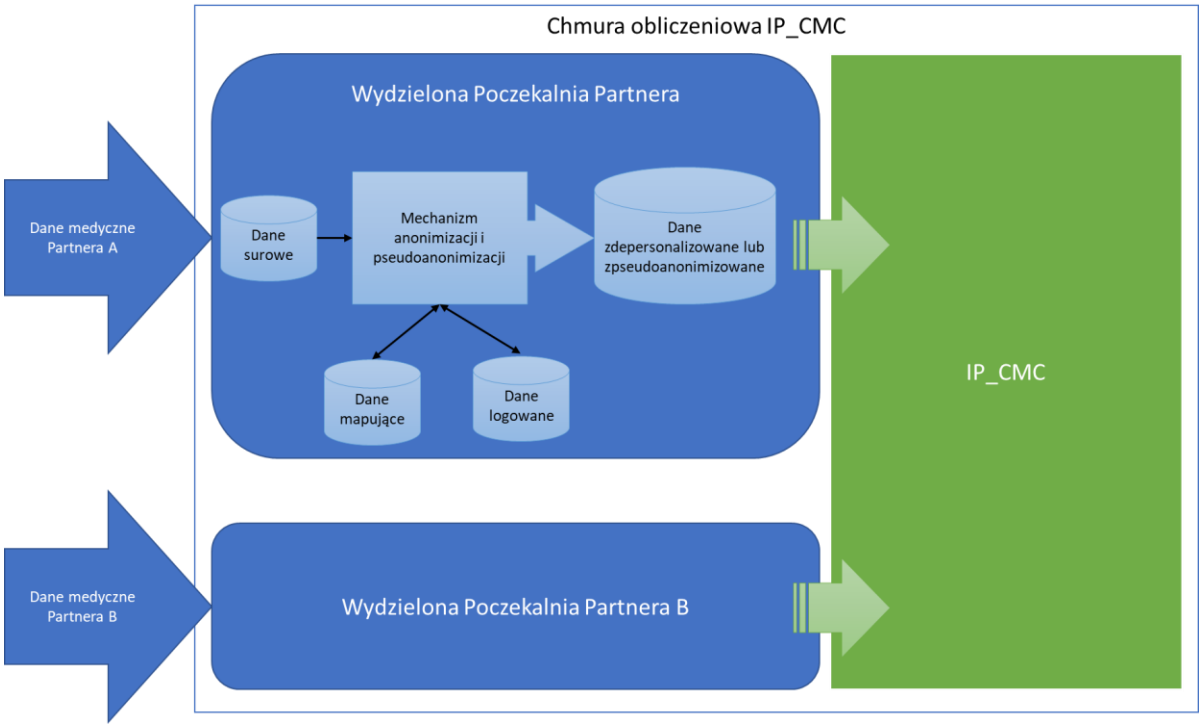


Schemat szczegółowy architektury IP_CMC działającego w środowisku chmurowym:



MODYFIKACJA 23.07.2024 **Załącznik 3 do SWZ**

Schemat współpracy między GUMed a Partnerami w zakresie przekazywania danych do IP_CMC i anonimizacji/pseudoanonimizacji:



Wykonawca zobowiązany będzie do zaprojektowania, instalacji i konfiguracji Platformy złożonej z systemów operacyjnych, maszyn wirtualnych, oprogramowania systemowego oraz aplikacyjnego i innych niezbędnych komponentów w taki sposób by w ramach realizacji zamówienia Zamawiający otrzymał kompletną, gotową do działania Platformę IP_CMC, spełniającą założenia architektury informatycznej wskazanej przez Zamawiającego.

GUMed w miarę posiadanych możliwości będzie wspierał zbieranie wymagań i dostarczy Zamawiającemu obecnie posiadaną wiedzę nt. modeli danych, transformacji i sprzęgów danych. GUMed udostępni posiadane opisy baz danych oraz dokumentację mapowania danych pomiędzy modelem danych wejściowych od strony Partnera na struktury FHIR.

Pliki tabularyczne z systemu HIS, obrazowe z systemu PACS oraz pliki z danymi omicznymi będą wystawiane przez Partnera UCK samodzielnie i udostępniane dla GUMed w Poczekalni.

GUMed wraz z partnerami wskaże, które dane w plikach są wrażliwe i muszą maja podlegać automatycznej anonimizacji i/lub pseudoanonimizacji w procesie zasilania.

W ramach budowanego rozwiązania Platformy IP_CMC nie będą stosowane mechanizmy szukania korelacji danych dla jednego tzw. złotego rekordu pacjenta. Korelacja danych będzie zagwarantowana przed zasileniem danych tj. w systemach partnerów. Poza zakresem prac jest też budowanie modułu dla zarządzania zgodami pacjentów do celów badań klinicznych.

Piaskownica badaczy, czyli inaczej Wirtualne Laboratoria, zostaną uruchomione dla indywidualnych potrzeb laboratoriów. Gotowość środowiska dla laboratorium do działania i udostępnienia badaczom zostanie zweryfikowana na podstawie scenariuszy użycia określonych w wymaganiach.

4.3 Wymagania z zakresu Chmury

Na potrzeby Platformy IP_CMC Wykonawca będzie dysponował i wdroży rozwiązanie chmury obliczeniowej zgodnej z wymaganiami obligatoryjnymi, opisanymi poniżej. Jako chmurę obliczeniową przyjmuje się rozwiązanie sprzętowo-programowe dostępne poprzez sieć komputerową publiczną lub prywatną posiadające zdolność obsługi serwerów wirtualnych, baz danych wirtualnych, urządzeń sieciowych wirtualnych i fizycznych oraz świadczenie co najmniej 100 usług chmurowych w modelu SaaS, w szczególności z obszaru Zdrowia (ang. HealthCare), tj.:

- Doznania pacjenta i użytkownika (interfejs, usługi behawioralne),
- Zarządzanie populacyjne pacjentami,
- Optymalizacja obsługi pacjenta,
- Narzędzia Data Science dla obszaru Zdrowia,
- Narzędzia przetwarzania danych złożonych typu Data Lakehouse.

Wykonawca ponosi koszty utrzymania działającej Chmury Obliczeniowej spełniającej wymagania Zamawiającego przez cały okres Umowy, czyli koszt wszystkich usług wymaganych dla działania i utrzymania Platformy IP_CMC w chmurze obliczeniowej przez okres rozwoju platformy i do końca świadczenia Asysty Technicznej.

Wymagania obligatoryjne Zamawiającego:

Nr	Punkt kontrolny
CH.1	Chmura obliczeniowa, którą wykorzystuje IP_CMC, umożliwia skalowalność, tj. umożliwia dynamiczne dostosowywanie zasobów (np. obliczeniowych, pamięciowych) w zależności od bieżących potrzeb, np.: 1. Możliwość replikacji zasobów na różnych geograficznych obszarach. W przypadku awarii w jednym regionie, ruch może być przekierowany na inny, minimalizując przestoje. 2. Mechanizmy automatycznego odtwarzania (auto-scaling) pozwalają na dynamiczne dostosowywanie zasobów w razie potrzeby.
CH.2	Chmura obliczeniowa, którą wykorzystuje IP_CMC, umożliwia elastyczność, tj. umożliwia łatwe tworzenie i zarządzanie maszynami wirtualnymi (PaaS, Iaas), usługami chmurowymi (SaaS), kontenerami oraz innymi zasobami.
CH.3	Chmura obliczeniowa, którą wykorzystuje IP_CMC, umożliwia obsługę wielu typów obciążeń np. usług chmury obliczeniowej, silników baz danych, usługi przetwarzania danych, analiza big data, uczenie maszynowe, serwisy webowe i inne.
CH.4	Podstawowe bezpieczeństwo na poziomie zarządzania Chmurą gwarantują mechanizmy kontroli dostępu, szyfrowania danych w spoczynku i w ruchu oraz monitorowania zdarzeń.
CH.5	Chmura umożliwia autoryzację i uwierzytelnianie użytkowników oraz zarządzanie ich uprawnieniami (zarządzanie tożsamością dostępu do Chmury), w tym: 1. Uwierzytelnianie (Authentication): Wymagane jest, aby użytkownicy dostarczali prawidłowe dane uwierzytelniające przed uzyskaniem dostępu do zasobów. 2. Autoryzacja (Authorization): W chmurze obliczeniowej można definiować role, polityki dostępu i grupy, aby precyzyjnie zarządzać autoryzacją. 3. Role i uprawnienia: Uprawnienia określają, jakie operacje są dozwolone na danym zasobie (np. odczyt, zapis, usuwanie).

	4. Grupy: Można przypisać użytkowników do grup, a następnie przypisać role lub polityki dostępu do tych grup lub polityki dostępu do usług. 5. Audyt i monitorowanie: Śledzenie kto, kiedy i jak korzysta z zasobów. Dzienniki zdarzeń (logs) oraz narzędzia monitorujące pozwalają na wykrywanie nieprawidłowości i podejrzanych aktywności. 6. Single Sign-On (SSO): umożliwia użytkownikom logowanie się tylko raz, a następnie dostęp do platformy bez konieczności ponownego uwierzytelniania.
CH.6	Chmura posiada mechanizmy tworzenia kopii zapasowych (backup oraz archiwizacja) oraz mechanizmy długoterminowego przechowywania danych.
CH.7	Chmura umożliwia uruchamianie różnych systemów operacyjnych (Windows, Linux, MacOS).
CH.8	Chmura umożliwia integrację z istniejącymi systemami w GUMed, w tym platforma chmurowa powinna umożliwiać integrację z zewnętrznym systemem zabbix oraz wazuh.
CH.9	Chmura udostępnia narzędzia do monitorowania zużycia zasobów oraz kosztów, zgodne z Cloud Finanacial Managment. Minimalne komponenty, które powinny być dostępne to: 1. monitor wydatków: informacja o aktualnie wyliczonych kosztach utrzymania chmury z możliwością wskazania okresu jakiego dotyczą np. tydzień, miesiąc, kwartał, własne kryteria; 2. planowanie i prognozy dotyczące wydatków na chmurę: na podstawie dotychczasowego zużycia powinna być możliwość przewidzenia wydatków; 3. koszty instancji: monitorowanie kosztów poszczególnych instancji i klastrów; 4. koszty usług: monitorowanie kosztów różnych usług w chmurze, takich jak udostępnione aplikacje, usługi i bazy danych.
CH.10	Chmura udostępnia mechanizmy pełnego monitoringu na poziomie sprzętowym, usług oraz silników danych, w tym minimalnie: 1. konfigurowalny Dashboard złożony z Widgetów pokazujących różne aspekty wykorzystania zasobów, sprzętu, usług, baz danych, 2. automatyczne śledzenie: automatyczne zbieranie danych o wykorzystaniu zasobów, takich jak CPU, pamięć, przepustowość sieci, liczba żądań itp., 3. powiadomienia: System powinien wysyłać powiadomienia w przypadku: awarii, przekroczenia limitów lub innych istotnych zdarzeń, których konfigurację można skonfigurować w Chmurze, 4. wskaźniki zdrowia: monitorowanie stanu usług, maszyn wirtualnych, baz danych i innych zasobów dostępnych w Chmurze, 5. logi: Dzienniki zdarzeń (logs) przechowują informacje o działaniach użytkowników, błędach, dostępie do zasobów itp.
CH.11	Panel zarządzania Chmurą umożliwia generowanie, w cyklach miesięcznych, tygodniowych i na żądanie, następujących raportów: 1. Regularne raporty: Generowanie raportów o wykorzystaniu zasobów, dostępności usług, kosztach itp. 2. Samodzielnie konfigurowalne (ang. Customize) raporty: możliwość tworzenia własnych raportów z wybranych danych. 3. Trendy i prognozy: na podstawie zgromadzonych danych narzędzia Chmury pozwalają na przewidywanie przyszłego wykorzystania danych lub zasobów.

<table>
<tr><td>CH.12</td><td>Platforma chmurowa umożliwia uruchamianie różnych typów maszyn zgodnych z architekturą (x86_64, arm).</td></tr>
<tr><td>CH.13</td><td>Platforma chmurowa wspiera HPC (ang. high-performance computing) z użyciem CPU oraz GPU.</td></tr>
<tr><td>CH.14</td><td>Chmura powinna posiadać funkcje monitorujące umożliwiające budowę metryk do pomiarów zdrowia komponentów chmury i usług chmurowych oraz wydajności aplikacji dotyczących atrybutów:
1. wydajności, w szczególności: wykorzystania CPU, wykorzystania pamięci, przepustowości sieci, IOPS,
2. dostępności, w szczególności dostępności lub czasu dostępu do: instancji oraz usługi.</td></tr>
<tr><td>CH.15</td><td>Platforma IP_CMC powinna obsługiwać QoS (ang. Quality of Service), aby zapewnić odpowiednią przepustowość dla aplikacji krytycznych.</td></tr>
<tr><td>CH.16</td><td>Chmura obliczeniowa dla potrzeb IP_CMC powinna umożliwiać konfigurację sieci w chmurze umożliwiające segmentację sieci, aby izolować ruch między różnymi grupami zasobów czy aplikacji.</td></tr>
<tr><td>CH.17</td><td>Dostawca chmury obliczeniowej musi zapewnić co najmniej 2 serwerownie (lub 2 fizyczne miejsca przetwarzania danych) dostępne na terenie Unii Europejskiej. Średni czas dostępu do Chmury przez połączenie IPsec z siedzibą Zamawiającego nie może przekraczać 40ms. Jednocześnie obie serwerownie muszą zapewniać efektywne wykonanie replikacji danych między sobą.</td></tr>
<tr><td>CH.18</td><td>Korzystanie z zasobów chmury obliczeniowej nie może wymagać posiadania lub zakupu przez Zamawiającego dodatkowych licencji.</td></tr>
<tr><td>CH.19</td><td>Chmura gwarantuje minimalnie wydajność przetwarzań ETL danych IP_CMC pozyskiwanych od Partnerów pozwalającą na przetworzenie min. 10TB danych w nocnym oknie serwisowym, tj. od 22 do 6.</td></tr>
<tr><td>CH.20</td><td>Wielkość użycia przestrzeni na dane będzie dostosowana do bieżących potrzeb IP_CMC zgodnie z poniższą tabelą, ale docelowo na koniec Umowy nie mniej niż 1PB danych (wolnorotujących z gwarantowanym dostępem dłuższym niż 2h ale nie przekraczającym 24h zegarowych) i ok. 100GB (szybko-rotujących z gwarantowanym dostępem bieżącym) oraz około 20 VCPU wymagane do utrzymania procesów Platformy IP_CMC oraz analiz w laboratoriach całość rozliczana w ramach indywidualnych limitów ustalonych dla poszczególnych komponentów Platformy IP_CMC.
<table>
<tr><th>Procent wymaganych zasobów dyskowych (przestrzeni na dane)</th><th>Miesiąc trwania Umowy</th></tr>
<tr><td>10%</td><td>0-6</td></tr>
<tr><td>20%</td><td>6-12</td></tr>
<tr><td>40%</td><td>12-24</td></tr>
<tr><td>70%</td><td>24-36</td></tr>
<tr><td>100%</td><td>36 i później</td></tr>
</table></td></tr>
<tr><td>CH.21</td><td>Planowany odzysk (przywrócenie) danych zgromadzonych na nośnikach wolnorotujących i archiwalnych planowany jest miesięcznie na max 5% wykorzystanej przestrzeni na dane.</td></tr>
<tr><td>CH.22</td><td>Planowany transfer miesięczny danych z chmury do środowiska GUMed planowany jest na max 1% wykorzystanej przestrzeni na dane.</td></tr>
</table>

CH.23	Zamawiający przewiduje że będzie docelowo użytkował 24 środowiska Laboratoriów Wirtualnych, z tym, że w roku 2024 będzie takich środowisk 5. Przyrost środowisk – do ilości docelowej - będzie następował proporcjonalnie do czasu trwania Umowy. Laboratorium Wirtualne będzie najczęściej posiadać od 2 do 6 użytkowników. Każde z Laboratoriów Wirtualnych będzie wykorzystywane przez każdego z użytkowników minimalnie przez 80 h w miesiącu.

4.4 Wymagania z zakresu bezpieczeństwa

Wykonawca na etapie projektowania i wytwarzania Platformy IP_CMC uwzględni:

- procedury przetwarzania danych wraz z zasadami i regulacjami dotyczącymi ochrony danych osobowych RODO (privacy by design oraz privacy by default),
- wymagania normy ISO 27001 w zakresie dotyczący IP_CMC i uzgodnionym z Zamawiającym,
- wymagania dyrektywy NIS-2 w zakresie dotyczącym IP_CMC i uzgodnionym z Zamawiającym,
- zakres testów niefunkcjonalnych w zakresie bezpieczeństwa.

Przedmiot Umowy zostanie wykonany z uwzględnieniem wymagań dotyczących ochrony danych osobowych w fazie projektowania oraz zasady domyślnej ochrony danych osobowych zgodnie z motywem 78 oraz art. 25 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

Poprzez Privacy by design Zamawiający rozumie – uwzględnianie ryzyka ochrony danych osobowych w zakresie środków technicznych i organizacyjnych zapewniających ich właściwą ochronę m.in. monitorowanie, testy bezpieczeństwa, zmiany w oprogramowaniu czy nadawaniu uprawnień dla użytkowników.

Poprzez Privacy by default Zamawiający rozumie – domyślną ochronę danych polegającą wyłącznie na przetwarzaniu, okresie przechowywania oraz sposobie udostępniania tylko tych danych osobowych, na które pozwalają obowiązujące przepisy prawa oraz są niezbędne do osiągnięcia konkretnego celu. Funkcjonalność aplikacji umożliwi zbieranie i udostępnienie innych danych osobowych ponad te niezbędne w sytuacji, gdy użytkownik w ramach posiadanych uprawnień dokona zmiany domyślnych ustawień aplikacji.

Konstrukcja Platformy IP_CMC musi zakładać możliwość bezpiecznego udostępnienia danych innym podmiotom, ze szczególnym uwzględnieniem podmiotów publicznych.

Dostarczana Platformy IP_CMC musi spełniać następujące wymagania obligatoryjne:

Nr	Punkt kontrolny
B.1	Platforma IP_CMC wspiera anonimizację i pseudonimizację danych tekstowych w zbiornikach danych tabularycznych, plikach XML czy metadanych towarzyszących plikom obrazowym (np. DICOM), tj. usuwanie lub zastępowanie danych identyfikujących, takich jak imiona, nazwiska, PESEL, adresy, numery telefonów czy opisowe wyrażenia identyfikujące identyfikatorami: 1. losowymi zgodnymi z tabelą mapującą, 2. wyliczanymi na podstawie algorytmów do przekształcania danych w sposób uniemożliwiający identyfikację.

B.2	Platfroma IP_CMC wspiera anonimizację i pseudonimizację danych graficznych, np. w plikach formacie DICOM, JPG lub innych specyficznych dla urządzeń medycznych, tj. automatycznie usuwa informacje identyfikujące z obrazów medycznych, takie jak imiona pacjentów, identyfikatory pacjentów, PESEL, adresy, numery telefonów oraz zastępuje je innymi danymi losowymi lub wyliczonymi zgodnie z przyjętym algorytmem maskowania. Jednocześnie usuwanie danych na obrazach nie wpływa na jakość samych danych obrazowych i ich przydatność do badań klinicznych. Platforma wspiera standardy anonimizacji, takie jak DICOM Anonymization Profile.
B.3	Bezpieczeństwo danych przechowywanych na platformie chmurowej jest zapewnione poprzez szyfrowanie danych w spoczynku i w trakcie przesyłania do Chmury.
B.4	Kontrola dostępu do danych i algorytmów (programów/skryptów) jest zapewniona na poziomie użytkownika, z uwzględnieniem ról i uprawnień.
B.5	Zabezpieczenie dostępu do danych medycznych na Platformie IP_CMC jest zapewnione poprzez dwuetapową (2FA) lub wieloetapową (MFA) weryfikację tożsamości użytkowników wraz z narzędziami do monitorowania logów dostępu i podejrzanych aktywności. Logowanie do zasobów IP_CMC oraz podsystemów IP_CMC za pomocą mechanizmu uwierzytelniania wieloskładnikowego/uwierzytelnianie wielopoziomowe jest wymagane dla wszystkich użytkowników Platformy IP_CMC.
B.6	Na Platformie IP_CMC jest zaimplementowane centralne zarządzanie tożsamościami użytkowników, z uwzględnieniem ich ról i uprawnień z wykorzystanie standardów takich jak SAML, OAuth czy OpenID Connect.
B.7	Platforma IP_CMC musi rejestrować działania użytkowników, dostępu do danych i zmian konfiguracji. Prowadzony jest pełny audyt i logowanie.
B.8	Platforma IP_CMC umożliwia generowanie raportów o bezpieczeństwie, w szczególności umożliwia generowanie raportów bezpieczeństwa dotyczących wykrytych nieudanych prób logowania, wykrytych anomali, wyników działania modułów IDS/IPS (Intrusion Detection System/Intrusion Prevention System).
B.9	Platforma IP_CMC powinna wykorzystywać narzędzia do aktywnego wykrywania i zapobiegania atakom. W tym celu minimalnie Platforma IP_CMC używa narzędzi takich jak firewall oraz IDS/IPS.
B.10	Bezpieczeństwo fizyczne centrów danych wykorzystywanych na potrzeby IP_CMC jest zgodne z normą ISO/IEC 27001 lub normą równoważną. Dostawca chmury musi spełniać standardy bezpieczeństwa fizycznego dostępu do centrów danych.
B.11	Dostawca umożliwia dostęp na prośbę Zamawiającego dla audytorów do przeprowadzenia testów i audytów bezpieczeństwa oraz testów penetracyjnych komponentów Platformy CMC.
B.12	Platforma IP_CMC zapewnia zarządzanie kluczami szyfrowania, tj.: 1. Bezpieczne przechowywanie i rotację kluczy szyfrowania, 2. Zarządzania kluczami szyfrującymi i ich bezpieczną dystrybucję.
B.13	Platforma IP_CMC zabezpiecza dane w transporcie, tj. korzysta z protokołów szyfrowanych, takich jak HTTPS, TLS/SSL do ochrony danych w trakcie przesyłania oraz monitoruje ruchu sieciowego i wykrywa nieprawidłowości w przypadku transportu danych.

B.14	Platforma IP_CMC ogranicza dostęp do danych w zależności od kontekstu, tj. wykorzystuje rozwiązania takie jak np. CASB (Cloud Access Security Broker) do kontroli dostępu na podstawie kontekstu, takiego jak lokalizacja użytkownika, rodzaj urządzenia itp. Platforma IP_CMC stosuje ograniczenia dostępu dla odpowiednich grup użytkowników.
B.15	Platforma IP_CMC będzie stosować odpowiednie zabezpieczenia przed atakami DDoS (ang. Distributed Denial of Service). Oprócz aktywnego monitorowania ruchu sieciowego Platforma IP_CMC automatycznie reaguje na anomalie.
B.16	Wykonawca dostarczy narzędzia do monitorowania podatności konfiguracji oraz oprogramowania oraz umożliwi zarządzanie podatnościami i łataniem komponentów Platformy IP_CMC, tj. instalowaniem łatek bezpieczeństwa aplikacji, modułów i systemów, które wykorzystuje Platforma IP_CMC.
B.17	Platforma IP_CMC będzie zarządzać zdarzeniami bezpieczeństwa, tj. rejestruje i umożliwia analizę zdarzeń bezpieczeństwa, takich jak próby logowania, zmiany konfiguracji, nieprawidłowe próby dostępu itp. Platforma IP_CMC generuje alerty i umożliwia automatyczne reagowanie na podejrzane aktywności np. możliwość blokady adresu IP, loginu użytkownika, itp.
B.18	Bazy danych wykorzystywane w ramach Platformy IP_CMC są odpowiednio skonfigurowane pod względem bezpieczeństwa (ang. hardening) i korzystają ze sprawdzonych bezpiecznych konfiguracji ograniczających m.in. dostęp do portów sieciowych, wyłączających niepotrzebne funkcje czy stosujących silne hasła dostępu. Jednocześnie mechanizmy zarządzania bazami danych umożliwiają planowanie regularnych aktualizacji oprogramowania bazodanowego w celu łatania podatności.
B.19	Platforma IP_CMC posiada mechanizmy monitorowania i logowania dostępu do baz danych, w tym przechowywania i przeglądania logów dostępu, wydawanych komend przez administratorów i śledzenia zdarzeń związanych z bazami danych.
B.20	Platforma IP_CMC oferuje możliwość tworzenia wielu kont o różnych poziomach uprawnień w celu zapewnienia bezpiecznego rozdzielenia zakresu prac administracyjnych na różne osoby w organizacji. Rozwiązanie bazodanowe pozwala na blokowanie dostępu do danych użytkownikom o wysokich uprawnieniach administracyjnych.
B.21	Systemy operacyjne wykorzystywane na Platformie IP_CMC są bezpiecznie skonfigurowane (ang. hardening), m.in. mają wyłączone niepotrzebne usługi i ograniczoną ilość otwartych portów do minimum, tam, gdzie jest to możliwe są wdrożone mechanizmy kontroli dostępu do systemu operacyjnego i systemu plików, itp.
B.22	Lokalizacje sieciowe, fizyczne czy między centrami danych - wykorzystywane w ramach Platformy IP_CMC - są połączone punkt w punkt (ang. Site-to-Site) za pomocą bezpiecznych połączeń, np. szyfrowanych łączy VPN.
B.23	Serwery i usługi Platformy IP_CMC oraz lokalne serwery GUMed kontaktujące się z IP_CMC muszą autoryzować się nawzajem, aby uniknąć ataków typu “man-in-the-middle”.
B.24	Dostęp administracyjny do Platformy IP_CMC i jej zasobów musi być realizowany przez serwer pośredniczący (ang. proxy) oraz z zastosowaniem szyfrowanego tunelu IPSec VPN.
B.25	Wykonawca dostarczy zaporę ogniową dla ruchu wychodzącego oraz ruchu przychodzącego. Zapora ogniowa powinna umożliwiać filtrowanie ruchu w warstwach 3,

	4 i 7. Zamawiający wymaga funkcjonalności IPS. Zapora ogniowa musi być dostarczona w formule PaaS i powinna opierać się na co najmniej dwóch komponentach logicznych. Zapora ogniowa powinna posiadać wydajność wystarczającą do działania w pełnym paśmie sieciowym wykorzystywanym przez Zamawiającego.
B.26	Wykonawca gwarantuje odpowiednie metody, które pozwolą na stosowanie bezpiecznych tuneli komunikacyjnych i szyfrowaną transmisję danych pomiędzy chmurą a lokalnymi zasobami GUMed.
B.27	Platforma IP_CMC wspiera wewnątrz samej platformy jednokrotne logowanie (ang. Single Sign-On, SSO) na poziomie typowych operacji nieuprzywilejowanych, tj. dostęp do typowych operacji dla poszczególnych komponentów wymaga tylko raz logowania opartego o MFA lub 2FA. Dla operacji uprzywilejowanych, w tym operacji administracyjnych czy dostępu do komponentów krytycznych, dostęp jest możliwy zawsze wyłącznie po logowaniu MFA lub 2FA.
B.28	Wykonawca opracuje plany reagowania na incydenty bezpieczeństwa dot. działania Platformy IP_CMC.
B.29	Dostęp zdalny do Platformy IP_CMC oraz jej komponentów jest możliwy wyłącznie z sieci GUMed przez serwery pośredniczące. Wymagane jest umożliwienie pracownikom zdalnym bezpieczny dostęp do zasobów Platformy IP_CMC w chmurze obliczeniowej poprzez VPN.
B.30	Platforma IP_CMC nie będzie udostępniana w Internecie. Dostęp do niej z Internetu nie będzie możliwy.

4.5 Wymagania z zakresu wydajności i dostępności

Dostarczana przez Wykonawcę Platforma IP_CMC musi spełniać następujące wymagania obligatoryjne, w zakresie wydajności i dostępności, gwarantując jednocześnie poprawne działanie Platformy IP_CMC przy zmiennym jej wykorzystaniu przez użytkowników w czasie, zmianach w otoczeniu i adaptacji do wdrażanych stopniowo procesów/usług na platformie:

Nr	Punkt kontrolny
DO.1	Platforma IP_CMC ma być dostępna dla użytkowników w systemie 24/7/365 z ustalonym wskaźnikiem dostępności SLA, tj. 99%.
DO.2	Platforma IP_CMC i jej komponenty będą dostępne przez cały okres trwałości projektu.
DO.3	Minimalna gwarantowana ilość użytkowników korzystających jednocześnie z aplikacji to 200 jednoczesnych sesji.
DO.4	Potencjalni użytkownicy mogą pochodzić z lokalizacji z Europejskiego Obszaru Gospodarczego.
DO.5	Maksymalny czas odpowiedzi aplikacji (tj. pojawienia się jakiejkolwiek informacji na ekranie świadczącej o pracy Systemu) na działanie użytkownika to 2 sekundy.
DO.6	Kolorystyka, czcionki i design interfejsu aplikacyjnego muszą być zgodne z kolorystyką GUMed i wytycznymi dotyczącymi dostępności dla systemów
DO.7	Platforma IP_CMC gwarantuje dostępność do historii zmian danych, logów z czynności użytkowników, historii zmian parametrów, historii zmian kodu skryptów i kodu źródłowego.

MODYFIKACJA 23.07.2024 **Załącznik 3 do SWZ**

DO.8	Zagwarantowany jest stały dostęp z sieci GUMed do zasobów Platformy IP_CMC z przepustowością pozwalającą na bezproblemowe korzystanie przez użytkowników z platformy.
DO.9	Platforma IP_CMC umożliwi wyświetlenie zaprojektowanej przez Wykonawcę informacji o czasowej niedostępności serwisu z powodów technicznych.
DO.10	Wykonawca zobowiązany jest wykonać po fazie stabilizacji oraz na koniec okresu gwarancyjnego optymalizację mającą na celu poprawę wydajności oraz zapewnienie bezawaryjnej pracy Platformy IP_CMC.
DO.11	System musi być dostępny dla osób z niepełnosprawnością. W związku z tym rozwiązanie musi być zgodne ze wszystkimi wytycznymi WCAG 2.0 zawartymi w załączniku nr 4 do Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
DO.12	Wykonawca zapewni dostępność narzędzi (np. skrypty, narzędzia pomiarowe, narzędzia monitorujące, narzędzia administracyjne) do pełnienia monitoringu dostępności i wydajności Platformy IP_CMC.
DO.13	Platforma IP_CMC zapewni wydajność interfejsu użytkownika umożliwiającą płynną nawigację pomiędzy modułami. Do zdeterminowania tego wskaźnika będą brane pod uwagę: 1. czas potrzebny przeglądarce na otrzymanie pierwszego bajtu danych z serwera (TTFB - Time to First Byte): poniżej 1.8s, 2. czas potrzebny przeglądarce na zareagowanie na pierwsze dane wejściowe użytkownika, takie jak kliknięcie łącza (FID - First Input Delay): poniżej 300ms, 3. czas potrzebny na uwidocznienie pierwszego elementu treści na stronie (FCP - First Contentful Paint): poniżej 2s, 4. czas potrzebny do pełnego załadowania i uwidocznienia największego elementu treści na stronie (LCP - Largest Contentful Paint): poniżej 4s.
DO.14	Platforma IP_CMC zapewni określone w wymaganiu DO.13 czasy dla wszystkich określonych scenariuszy użycia.
DO.15	Platforma IP_CMC zapewni minimalną przepustowość dyskową na poziomie umożliwiającym jednoczesny zapis (10GB) oraz odczyt danych (10GB) przesyłanych z strumieniowych w ciągu 1h.
DO.16	W Platformie IP_CMC bazy danych zapewnią minimalną wydajność baz danych na poziomie: 1. Ilość transakcji baz danych na sekundę: min 600 transakcji/s. 2. Czas odpowiedzi bazy danych (średni czas odpowiedzi na 1000 zapytań SQL): poniżej 1s.
DO.17	Platforma IP_CMC zapewni minimalna przepustowość sieciowa: 1. Przepustowość sieciowa: 1Gbit. 2. Opóźnienia sieciowe (średni czas odpowiedzi na 1000 żądań HTTPS): poniżej 100ms.

DO.18	Platforma IP_CMC będzie wykorzystywać - o ile to będzie konieczne z punktu widzenia zagwarantowania poziomu SLA - Load Balancer o minimalnej przepustowości: 1. Ilość obsłużonych żądań na sekundę: 2000 przy 200 użytkownikach 2. Czas przełączania ruchu między serwerami (średni czas przekierowania żądania): maksymalnie 50ms.
DO.19	Chmura gwarantuje minimalną wydajność przetwarzań ETL danych IP_CMC pozyskiwanych od Partnerów o przepustowości min. 3Gbit/s.

4.6 Metamodel

Dostarczana przez Wykonawcę Platforma IP_CMC musi spełniać wymagania określone m.in. przez Agencję Badań Medycznych w zakresie formatów danych wymaganych do wymiany z ośrodkami medycznymi i badawczymi. Przyjęte przez Zamawiającego podejście do modelu danych zostało opisane poniżej. Zamawiający zakłada, że dane mogą być przechowywane w wielu różnych formatach i zbiornikach danych niezgodnych nawet z poniższym metamodelem, ale dostęp do danych i ich wymiany powinien być możliwy w ramach przyjętego metamodelu. Zamawiający dopuszcza zapis i przechowywanie danych - dodatkowo do wskazanego metamodelu - w formatach:

- źródłowych,
- wynikających z potrzeb technicznych, np. dla lepszej wydajności platformy,
- archiwalnych na potrzeby przechowywania długoterminowego danych,
- wyliczeniowych i syntetycznych na potrzeby raportowania i analizy danych.

Wymagania obligatoryjne Zamawiającego:

Nr	Punkt kontrolny
ME.1	System umożliwia zasilanie danymi zapisanymi w plikach (typ XML, JSON lub tekstowy płaski) zgodnymi ze standardem FHIR 4 lub wyższym, co najmniej dla następujących zasobów: A. Patient B. Organization C. Encounter D. Procedure E. Condition F. Observation G. DiagnosticReport H. ClinicalImpression I. Composition J. ImagingStudy K. Endpoint L. Device M. GenomicStudy N. Specimen O. DocumentReference P. Medication Q. MedicationAdministration

ME.2	System umożliwia dodanie różnych nowych typów zasobów do procesu zasilania i przetwarzania w miarę rozwoju standardu FHIR lub konieczności zasilania innymi obiektami niż wyżej wymienione.
ME.3	System w procesie zasilania automatycznie weryfikuje zgodność plików źródłowych ze standardem FHIR 4 lub wyższym.
ME.4	System publikuje zestaw raportów technicznych dotyczących procesu pobierania, przetwarzania i kontroli jakości pobieranych danych źródłowych i ich zgodności z metamodelem IP_CMC.
ME.5	System umożliwia przechowywanie danych zapisanych zgodnie ze standardem FHIR w obiektach bazy danych.
ME.6	W każdej tabeli zasobu poszczególne kolumny odpowiadają strukturze zasobu zdefiniowanej w standardzie FHIR (min. wersja 4). Przykładowo: dla zasobu „Obserwacja" będą to ID, META, IMPLICITRULES, LANGUAGE, TEXT, CONTAINED, EXTENSION, MODIFIEREXTENSION, IDENTIFIER, BASEDON, TRIGGEREDBY, PART OF, STATUS, CATEGORY, CODE, SUBJECT, itd.
ME.7	Dla zasobów złożonych utworzone są dodatkowe obiekty w relacji 1:N umożliwiające odpowiednią indeksację i przeszukiwanie.
ME.8	Dla obiektów binarnych (dane obrazowe, dane omiczne) system przechowuje referencję do ich lokalizacji w repozytorium danych obrazowych i omicznych.
ME.9	Zapewnienie jakości i rzetelności danych w bazie opartej o metamodel będzie oparte o: 1. Rejestr kluczy do wszystkich zasobów pojedynczego pacjenta. 2. Rejestr atrybutów wrażliwych w ramach obiektów (np.: dane osobowe). 3. Rejestr atrybutów podlegających anonimizacji w procesie. 4. Rejestr obiektów z restrykcyjnym dostępem (np.: dostęp do tych danych tylko dla określonych ról użytkowników). 5. Rejestr (log) odpytań wykonanych do usług wewnętrznych. 6. Rejestr (log) wykonanych zapytań na danych.
ME.10	Wykonawca wykona analizę metamodelu wejściowego Platformy IP_CMC (dostarczonego przez Zamawiającego) i zaimplementuje go w części platformy określanej jako RAW.
ME.11	Wykonawca wykona wspólnie z Zamawiającym analizę potrzeb w zakresie budowania kohort pacjentów i zaimplementuje odpowiedni metamodel wykorzystywany w Laboratoriach Platformy CMC.
ME.12	Wykonawca zaimplementuje Metamodel dla zdjęć obrazowych, metadanych DiCOM oraz plików omicznych.
ME.13	Wykonawca przygotuje wspólnie z Zamawiającym dokumentację oraz walidatory danych dla używanych przez Platformę IP_CMC metamodeli wejściowych.

4.7 Opis wymagań dla architektury technicznej

Wykonawca dostarczy koncepcję architektoniczną i realizacyjną w ramach prowadzonych prac zawierającą wszelkie wymagania dotyczące architektury Platformy IP_CMC. Wykonawca będzie bazował na dobrych praktykach oraz standardach dziedzinowych przy opracowaniu architektury oraz przygotuje Architekturę zgodnie z poniższymi wymaganiami Zamawiającego. Wykonawca zdefiniuje na poziomie Architektury m. in. założenia i ograniczenia architektoniczne, analizę dot.: integralności,

niezawodności, dostępności oraz wskaże zasady integracji i interoperacjonalności rozwiązania. Architektura dostarczona przez Wykonawcę będzie spójna i kompletna i zostanie wykonana z wykorzystaniem stosownych metod modelowania zgodnie z wymaganiami OPZ.

Dla architektury technicznej Zamawiający definiuje następujące wymagania obligatoryjne:

Nr	Punkt kontrolny
A.1	Platforma IP_CMC musi posiadać architekturę trójwarstwową (Warstwa prezentacji, Warstwa logiki biznesowej, Warstwa dostępu do danych) oraz odpowiednią separację zasobów, co pozwala na izolację każdej z warstw architektury trójwarstwowej.
A.2	Platforma IP_CMC musi zapewniać obsługę standardu kodowania znaków UNICODE oraz standardów znaków specyficznych dla danych zapisywanych w urządzeniach medycznych producentów i plikach Dicom.
A.3	Projektowane interfejsy zewnętrzne Platformy IP_CMC będą zgodne ze standardami i profilami interoperacyjności oraz powinny pozwalać na integrację z innymi systemami GUMED i Partnerów stosowanymi przy badaniach klinicznych.
A.4	Platforma IP_CMC powinna umożliwiać zdefiniowanie automatycznych (cyklicznych) eksportów i transformacji danych (pliki tabularyczne/XML, omiczne, obrazy) w modelu ETL przez administratorów i deweloperów Zamawiającego.
A.5	Zaczytany plik XML/JSON powinien być zapisany w tabeli w bazie danych w sposób umożliwiający zaindeksowanie danych i przeszukiwanie zbioru danych w sposób efektywny.
A.6	Platforma IP_CMC powinna umożliwiać automatyczną wysyłkę wiadomości e-mail w oparciu o zdarzenia w systemie w celu informowania: administratorów, operatorów i klinicystów. Wybór zdarzeń i warunków wyzwalających powinien być możliwy do konfiguracji przez administratorów Platformy CMC.
A.7	Wykonawca zaprojektuje architekturę Platformy IP_CMC biorąc pod uwagę, że Zamawiający planuje uzupełnić platformę o rozwiązanie klasy BI (Business Intelligence), które umożliwia planowanie, przeprowadzanie wielowymiarowych analiz i raportowanie w oparciu o dedykowany DataMart z danymi.
A.8	System powinien umożliwiać tworzenie perspektyw na podstawie wielowymiarowych atrybutów (wymiarów) pozwalających ograniczyć widok dla użytkownika tylko do pewnego podzbioru obiektów dostępnych dla niego.
A.9	Platforma IP_CMC będzie posiadać zintegrowane narzędzia do zarządzania platformą i jej komponentami, w tym narzędzia do zarządzania i konfiguracji wszystkich usług wchodzących w skład Platformy IP_CMC (PaaS, IaaS, SaaS), w tym bazami danych, usługami chmurowymi, usługami analitycznymi, usługami transformacji danych i anonimizacji. Narzędzia te powinny udostępniać możliwość tworzenia i wykonywania skryptów automatyzujących przez Administratorów lub sam System.
A.10	System powinien umożliwiać rejestrowanie (logowanie) zapytań wykonywanych przez użytkowników, a następnie umożliwiać na podstawie zgromadzonych informacji na automatyczną optymalizację wydajności systemu (np. automatyczne projektowanie agregacji pozwalające na przyspieszenie wykonywania najczęściej wykonywanych zapytań do bazy danych).
A.11	W ramach architektury danych zostanie dostarczona:

	1. identyfikacja i charakterystyka obszarów danych gromadzonych w sposób trwały w obrębie poszczególnych elementów systemu, 2. identyfikacja i charakterystyka obszarów danych wymienianych z systemami zewnętrznymi, np. Partnerami czy systemami GUMed 3. identyfikacja bezpośrednich relacji zachodzących pomiędzy obszarami danych, 4. relacje pomiędzy danymi gromadzonymi w systemie a obiektami i zasobami w architekturze biznesowej demonstrujące biznesowe znaczenie poszczególnych elementów danych. Architektura Danych powinna być udokumentowana w narzędziu Enterprise Architect oraz zgodnie z zapisami OPZ w części "Zarządzanie projektem" oraz "Dokumentacja".
A.12	Przygotowana przez Wykonawcę Architektura Technologiczna obejmować będzie co najmniej: 1. identyfikację i charakterystykę wszystkich elementów infrastruktury techniczno-systemowej Platformy IP_CMC na poziomie IaaS, PaaS, SaaS, 2. powiązanie zidentyfikowanych elementów architektury technologicznej Platformy IP_CMC z elementami architektury Zamawiającego, 3. wskazanie parametrów i standardów działania, w tym wolumentaria i wymagania sprzętowe (minimalne, optymalne, maksymalne), komponentów infrastruktury IT, systemów i oprogramowania oraz warunków środowiskowych dla stacji roboczych i aplikacji, 4. identyfikację i charakterystykę elementów sieci WAN, LAN, VLAN, DMZ i innych elementów komunikacyjnych wymaganych do działania Platformy CMC. Architektura technologiczna powinna być udokumentowana w narzędziu Enterprise Architect w notacji Archimate oraz zgodnie z zapisami OPZ w części "Zarządzanie projektem" oraz "Dokumentacja".
A.13	Przygotowana przez Wykonawcę Architektura Biznesowa musi: 1. uwzględniać obowiązujące przepisy prawa, 2. być gotowa na projektowane (oczekiwane w najbliższej przyszłości) przepisy prawa, 3. w pełni reprezentować procesy Zamawiającego w obszarze IP_CMC, 4. identyfikować i charakteryzować biznesowe obiekty i zasoby informacyjne wykorzystywane do komunikacji pomiędzy procesami Zamawiającego, 5. identyfikować i charakteryzować działania biznesowe (modelowane jako procesy, funkcje, aktywności, usługi biznesowe lub inne klasyfikatory reprezentujące działania biznesowe), 6. identyfikować i charakteryzować poszczególnych aktorów i ich czynności oraz odpowiedzialności w zakresie procesów IP_CMC, 7. uwzględniać uzgodnienia poczynione z Zamawiającym na etapie projektu. Architektura biznesowa powinna być udokumentowana w narzędziu Enterprise Architect w notacji Archimate oraz zgodnie z zapisami OPZ w części "Zarządzanie projektem" oraz "Dokumentacja".
A.14	Dla zapewnienia wysokiej sprawności i skuteczności działania przetwarzania dużych zbiorów danych wymaganym jest, aby Platforma IP_CMC pracowała w oparciu o elastyczne i skalowalne usługi chmury obliczeniowej umożliwiające - minimalnie - na dostęp na żądanie do mocy obliczeniowej, przestrzeni na dane, podstawowych silników baz danych SQL oraz noSQL, silników baz obiektowych, usługi analizy danych, środowisk

	programistycznych Python oraz R i wykonywania kodu w trybie serverless, usługi przetwarzania wsadowego i strumieniowego, usługi zarządzania metadanymi, usługi integracji danych, usługi wirtualizacji, usługi kognitywne.
A.15	Elementy Platformy IP_CMC realizujące podstawowe funkcje muszą zostać dostarczone w postaci klastra lub innego rozwiązania równoważnego gwarantującego dotrzymanie poziomu SLA, jednak nie jest wymagane, aby klaster opierał się o niezależne lokalizacje.
A.16	Platforma IP_CMC ma być oparta o koncepcję Data Lakehouse i musi być zgodna z koncepcją Centrum Medycyny Cyfrowej opisaną w załączniku "Schemat teleinformatycznej architektury systemu ośrodka IP_CMC".
A.17	Platforma IP_CMC może korzystać z rozszerzeń funkcjonalności dostawcy chmury obliczeniowej o standardy i wzorce integracyjne wykorzystywane w służbie zdrowia, jednak tylko wtedy, gdy zagwarantowane jest bezpieczeństwo i wyłączność stosowania takiej usługi na potrzeby GUMED.
A.18	Komunikacja synchroniczna wewnątrz Platformy IP_CMC powinna być oparta o interfejs REST API i mikroserwisy, a komunikacja asynchroniczna o brokery wiadomości np. Kafka albo pliki tekstowe.
A.19	Korzystanie z łączy bazodanowych np. DB-Link między komponentami platformy nie jest rekomendowane i każdorazowo powinno być zaakceptowane przez Zamawiającego.
A.20	Mechanizmy Platformy IP_CMC muszą zapewniać mechanizm chroniący przed przypadkowymi usunięciami zasobów i komponentów.
A.21	Wykonawca zaproponuje i uzgodni z Zamawiającym sposób integracji z lokalnymi zasobami obliczeniowymi i dyskowymi GUMed.
A.22	Podstawowe obszary logiczne danych wykorzystywane przez Platformę IP_CMC to: 1. POCZEKALNIA PARTNERA (dane źródłowe Partnera zarządzane przez Partnera) 2. RAW (dane źródłowe zarządzane przez GUMed) 3. STAGE (dane wstępnie przetworzone) 4. CUBES & CURATED, DATA MARTS (dane przygotowane dla Laboratoriów Wirtualnych)

4.8 Wymagania w zakresie oprogramowania, kodu źródłowego i warunków licencyjnych

W ramach realizacji Zamówienia Wykonawca będzie opracowywał i przekazywał Zamawiającemu kod źródłowy Oprogramowania Dedykowanego. Kod Źródłowy będzie na bieżąco opracowywany zgodnie ze standardem ustalonym przez Zamawiającego i Wykonawcę w ramach Analizy przedwdrożeniowej z uwzględnieniem następujących założeń:

1. W zakresie kodu programu jako standard, wprowadza się pokrycie testami jednostkowymi na poziomie minimum 40% metod.
2. Kod Źródłowy będzie przekazywany Zamawiającemu wraz z:
   a. Kompletnym wykazem narzędzi programistycznych, bibliotek (z licencją na korzystanie z nich, o ile mają zewnętrzny charakter) i innych elementów niezbędnych do doprowadzenia takiego Kodu Źródłowego do formy wykonywalnej. Ponadto na żądanie Zamawiającego Wykonawca zobowiązany jest udzielić Zamawiającemu lub osobie wskazanej przez Zamawiającego dodatkowych informacji niezbędnych do doprowadzenia danego Kodu Źródłowego do formy wykonywalnej.

b. Skryptami kompilacyjnymi i uruchomieniowymi, plikami konfiguracyjnymi oraz niezbędną dokumentacją pozwalającą na jego rozwijanie przez Zamawiającego lub inne podmioty, którym Zamawiający takie czynności powierzy.
c. Komentarzami, w szczególności komentarzami umieszczonymi w trakcie realizacji Umowy (Wykonawca nie będzie usuwał komentarzy oraz innych informacji technicznych z Kodu Źródłowego, przed jego dostarczeniem Zamawiającemu).

3. Wykonawca zobowiązuje się do niestosowania jakichkolwiek technik lub ograniczeń, które uniemożliwiłyby Zamawiającemu odczyt lub zapisywanie Kodu Źródłowego.

Wykonawca przyjmuje do wiadomości, że niewykonanie lub nienależyte wykonanie przez Wykonawcę któregokolwiek z obowiązków odnoszących się do Kodu Źródłowego, uniemożliwia zamknięcie Fazy Umowy i/lub zamknięcie zgłoszenia gwarancyjnego i/lub zamknięcie zgłoszenia w ramach Opcji.

W zakresie oprogramowania, kodu źródłowego i warunków licencyjnych, Zamawiający w szczególności wymaga od Wykonawcy spełnienia następujących punktów kontrolnych:

Nr	Punkt kontrolny
OP.1	W obszarze prowadzenia analiz na Platformie IP_CMC Wykonawca umożliwi wykonywanie skryptów napisanych w języku Python oraz dostarczy biblioteki lub metody przy pomocy, których będzie możliwość integracji z modułami Platformy CMC.
OP.2	W obszarze prowadzenia analiz na Platformie IP_CMC Wykonawca umożliwi instalację na Platformie IP_CMC oprogramowania Jupyter Notebook.
OP.3	W obszarze prowadzenia analiz na Platformie IP_CMC Wykonawca dostarczy możliwość zainstalowania interpretatora języka R, oprogramowania RStudio oraz integrację z bibliotekami CRAN oraz Bioconductor.
OP.4	Wykonawca dostarczy lub umożliwi na Platformie IP_CMC instalację kompilatora języka C np. gcc.
OP.5	Wykonawca zobowiązuje się dostarczyć wszystkie wymagane licencje na oprogramowanie, które będą wykorzystywane w ramach realizacji projektu oraz wykorzystywane przez Platformę IP_CMC. Licencje muszą być zgodne z obowiązującymi przepisami i umożliwiać pełne wykorzystanie funkcjonalności oprogramowania.
OP.6	Licencje powinny obejmować również narzędzia do obsługi platformy, zarządzania kodami źródłowymi oraz instalacji komponentów platformy. Licencje powinny obejmować też oprogramowanie potrzebne do zarządzania infrastrukturą (np. systemy operacyjne, narzędzia do monitorowania, zarządzania zasobami, zarządzania kontenerami).
OP.7	Licencja musi dopuszczać udostępnienie sprzęgu oraz projektowanego mechanizmu API na zewnątrz Platformy CMC.
OP.8	Licencje muszą umożliwiać m.in. instalację aplikacji na serwerach (stanowiskach wieloosobowych).
OP.9	Dostarczone licencje komercyjne lub akademickie muszą umożliwiać instalację w środowisku Platformy IP_CMC i realizację wszystkich celów istnienia i działania Platformy CMC.
OP.10	Wykonawca powinien dostarczyć pełną dokumentację licencji wraz z informacjami o zakresie, ograniczeniach i warunkach użytkowania.
OP.11	Prekompilowane komponenty, które przygotowuje wykonawca, muszą być złożone w postaci kodu źródłowego w repozytorium kodu źródłowego np. Git.

OP.12	Wykonawca zobowiązuje się do przedstawienia wszystkich bibliotek i oprogramowania, które użył do zbudowania platformy w formie wykazu obejmującego nazwę biblioteki, wersję, rodzaj licencji, nazwę producenta i/lub stronę internetową producenta oraz wskazanie miejsca użycia biblioteki.
OP.13	Wykonawca zobowiązuje się do dostarczenia wszystkich skryptów kompilacyjnych i uruchomieniowych, plików konfiguracyjnych wraz z niezbędną dokumentacją pozwalającą na dalsze rozwijanie Platformy IP_CMC przez Zamawiającego.
OP.14	Wykonawca zobowiązuje się udzielić Zamawiającemu dodatkowych informacji niezbędnych do doprowadzeniu danego kodu źródłowego do formy wykonywalnej.
OP.15	Wykonawca zobowiązuje się do niestosowania jakichkolwiek technik lub ograniczeń, które uniemożliwiałyby Zamawiającemu odczyt lub zapisywanie kodu źródłowego, skryptów, konfiguracji i danych.
OP.16	Kod źródłowy musi być w repozytorium kodu rozbity na poszczególne gałęzie reprezentujące wersje produkcyjne, rozwojowe i testowe zgodnie z dobrymi praktykami CI/CD.
OP.17	Dla poszczególnych ról użytkowników w Platformie IP_CMC zostanie dostarczona wymagana minimalna liczba licencji użytkowników: 1. Administrator Systemu – 8 2. Architekt Infrastruktury – 4 3. Developer – 10 4. Analityk Danych – 7 5. Data Scientist – 7 6. Użytkownik Zaawansowany – 100 7. Użytkownik Podstawowy – 300 8. Specjalista ds. Bezpieczeństwa - 4
OP.18	Licencja dla użytkowników musi być typu pływającego (ang. floating) czyli na stałe niezwiązana z konkretnym użytkownikiem.
OP.19	Kod źródłowy musi być sprawdzony przez narzędzie do sprawdzania jakości dostarczanego kodu np. Amazon CodeGuru lub inne tego typu narzędzie.
OP.20	Kod źródłowy napisany w języku Python musi być zgodny ze standardem PEP8.
OP.21	Interfejs Platformy IP_CMC musi być zgodny ze standardem W3C.
OP.22	Na dostarczone elementy przedmiotu zamówienia w zakresie wytworzenia Oprogramowania Dedykowanego Wykonawca przekaże prawa autorskie w możliwością samodzielnej rozbudowy i rozwoju.

4.9 Wymagania w zakresie sprzętu i urządzeń

W ramach zamówienia Wykonawca będzie zobowiązany do realizacji kompletu prac niezbędnych do uruchomienia produkcyjnego dostarczanej Platformy IP_CMC, w tym do instalacji oprogramowania standardowego i dedykowanego oraz wsparcia w przygotowaniu wymaganych zasobów sprzętowych po stronie Zamawiającego. W ramach realizacji zamówienia Wykonawca spełni następujące wymagania dot. środowiska Platformy IP_CMC:

Nr	Punkt kontrolny
SU.1	Platforma IP_CMC jest oparta o rozwiązanie chmury obliczeniowej.

SU.2	Środowisko uruchomieniowe Platformy IP_CMC będzie wspierać zarówno klasyczne środowiska uruchomieniowe na serwerach fizycznych lub wirtualnych, różne systemy operacyjne (Linux, Windows) oraz środowiska kontenerowe oparte na orkiestratorach.
SU.3	Dostęp do Platformy IP_CMC dla użytkowników działa w oparciu o istniejące komponenty sieci komputerowej Zamawiającego.
SU.4	Urządzenia VPN wymagane do podłączenia się użytkowników do Platformy IP_CMC przewidziane są wyłącznie w wersji softwareowej.
SU.5	Podłączenie się Partnerów do wydzielonych usług Platformy IP_CMC przewidziane jest poprzez Poczekalnię oraz za pomocą łączy szyfrowanych VPN punkt-punkt. Nie jest planowana instalacja urządzeń fizycznych.

5. Szkolenia użytkowników

Wykonawca w ramach realizacji przedmiotu zamówienia przeszkoli wskazane przez Zamawiającego osoby w zakresie wiedzy niezbędnej do przejęcia, aby współtworzyć, utrzymywać oraz rozwijać dostarczoną Platformę.

Celem szkoleń jest przekazanie uczestnikom wiedzy dotyczącej funkcjonowania dostarczanej Platformy wraz z rozwiązaniami infrastruktury informatycznej, w tym w szczególności nauczenie uczestników obsługi Platformy w stopniu pozwalającym na samodzielną pracę, dalszą administrację, utrzymanie oraz rozwój, a także dalsze przekazywanie wiedzy dotyczącej obsługi Platformy innym użytkownikom.

Szczegóły dotyczące szkoleń w ramach realizacji przedmiotu zamówienia:

Maksymalna liczba osób przewidzianych do udziału w szkoleniach	60 osób
Przewidywany termin realizacji usługi	Szkolenia realizowane sukcesywnie. Powinny się rozpocząć w terminie określonym w Załączniku nr 7 do Umowy.
Maksymalna liczba godzin przypadająca na 1 dzień szkolenia	1 dzień szkoleniowy wynosi 8 godzin szkolenia
Zakres szkolenia wymagany przez Zamawiającego	Wymagania opisane w punkcie 5.2 OPZ
Wymagania obligatoryjne i fakultatywne	Wymagania obligatoryjne i fakultatywne szczegółowo opisane zostały przez Zamawiającego w w punkcie 5.2 OPZ

5.1 Informacje dodatkowe

Szkolenia odbędą się w uzgodnionym terminie pod warunkiem, że Zamawiający zrekrutuje wymaganą grupę osób. Jeżeli nie uda się zrekrutować wymaganej liczby uczestników do uruchomienia szkolenia, Zamawiający ustali z wykonawcą nowy termin realizacji szkolenia. Informację o niezrekrutowaniu uczestników Zamawiający przekaże Wykonawcy najpóźniej 7 dni przed szkoleniem.

Zamawiający nie zapewnia transportu, noclegu ani wyżywienia trenerowi podczas wszystkich realizowanych szkoleń.

MODYFIKACJA 23.07.2024 **Załącznik 3 do SWZ**

5.2 Wymagania w zakresie szkoleń

Wykonawca w ramach realizacji przedmiotu zamówienia przeszkoli wskazane przez Zamawiającego osoby w zakresie wiedzy niezbędnej do przejęcia, aby współtworzyć, utrzymywać oraz rozwijać dostarczoną Platformę. Szkolenia powinny obejmować całość zagadnień niezbędnych do samodzielnej administracji Platformy IP_CMC.

Zamawiający wymaga od Wykonawcy realizacji szkoleń w następującym zakresie:

Nr	Punkt kontrolny
Sz.1	Wykonawca przeprowadzi szkolenia podstawowe i zaawansowane w dedykowanym zakresie dla poszczególnych ról. Zakres szkoleń powinien obejmować użytkowanie i administrowanie dostarczoną Platformą, zgodnie z wymogami opisanymi w OPZ.
Sz.2	Wykonawca przeprowadzi szkolenia dla wskazanych przez Zamawiającego ról we wskazanych ilościach osób: 1. Administratora Systemu - 4 osoby 2. Architekta Infrastruktury IT - 3 osoby 3. Developera oraz osób odpowiedzialnych za utrzymanie i rozwój systemu - 6 osób 4. Analityków Danych, Data Scientist i użytkowników zaawansowanych - 12 osób 5. Specjalistę ds. Bezpieczeństwa - 2 osoby 6. Użytkowników podstawowych - 30 osób
Sz.3	Wykonawca przeprowadzi szkolenie dla Administratora Systemu obejmujące minimalnie następujący zakres zagadnień: 1. ogólna architektura i analiza budowy Platformy, 2. ogólna architektura, zarządzanie i monitorowanie środowiskiem chmurowym, 3. kontrola pracy i bezpieczeństwa Platformy, 4. kontrola pracy interfejsów zasilania i procesów ETL, 5. kontrola i zarządzanie rozliczenia zasobów, 6. kontrola modułów równoważenia obciążenia i autoskalowania dla instancji maszyn wirtualnych, 7. administracja użytkownikami i uprawnieniami użytkowników oraz grup użytkowników, 8. administracja zarządzania tożsamością i dostępem do zasobów, 9. parametryzacja i kontrola pracy środowiska systemu, 10. parametryzacja i kontrola pracy oraz usługami danych systemu, 11. monitorowanie maszyn wirtualnych, 12. integracja infrastruktury z zasobami chmurowymi i lokalnymi, 13. przekazywanie, pobieranie i zarządzanie danymi, 14. optymalizacja zasobów i minimalizacji kosztów Platformy, 15. automatyzacja wdrażania usług infrastruktury, 16. zarządzanie i sterowanie przepływem ruchu w ramach systemu, 17. konfigurowanie kopii zapasowych, plików i folderów, alertów platformy, 18. praca z raportami - interfejs narzędzia, obszary robocze i jego funkcje, ustawienia osobiste i preferencje, uruchomienie raportów predefiniowanych i wizualizacji formularzy, tworzenie raportów, list, tabel przestawnych, miar wyliczanych na raportach, tworzenie formatowania warunkowego na raportach, 19. wizualizacja danych, wykresy, histogramy.

MODYFIKACJA 23.07.2024 **Załącznik 3 do SWZ**

Sz.4	Wykonawca przeprowadzi szkolenia dla Architekta Infrastruktury obejmujące wymagany zakres zagadnień: 1. ogólna architektura i analiza budowy Platformy, 2. ogólna architektura, zarządzanie i monitorowanie środowiskiem chmurowym, 3. architektura rozwiązań odpowiedzialnych za kontrolę pracy, bezpieczeństwa Platformy, zarządzanie i rozliczanie zasobów, 4. architektura bazy danych, 5. architektura dostępu do danych oraz zarządzania danymi, 6. architektura odpowiadającej za monitorowanie maszyn wirtualnych, 7. projektowanie pod kątem wysokiej dostępności, skalowalności i łatwości utrzymania Platformy, 8. architektura narzędzi pracy i modelu danych.
Sz.5	Wykonawca przeprowadzi szkolenia dla Developera oraz osób odpowiedzialnych za utrzymanie i rozwój systemu, obejmujące minimalny, wymagany zakres zagadnień: 1. architektura i budowa Platformy, 2. narzędzia pracy i bezpieczeństwa Platformy, 3. model danych, 4. konfigurowanie i zarządzanie słownikami, 5. konfigurowanie i zarządzanie konceptami (pojęciami), 6. konfigurowanie interfejsów zasilania i procesów ETL, 7. konfigurowanie środowiska pracy oraz ustawień Platformy, 8. konfigurowanie aplikacji oraz monitoring serwisu, 9. konfigurowanie bazy danych, 10. konfigurowanie uruchomionych algorytmów AI/ML, 11. konfigurowanie narzędzi analitycznych, 12. eksplorowanie miejsc wdrożenia usług w aplikacjach Platformy, 13. tworzenie rozwiązań z wykorzystaniem dostępnych obiektów Platformy, 14. tworzenie zaawansowanych raportów dynamicznych, 15. skalowanie aplikacji dostępnych w usługach Platformy.
Sz.6	Wykonawca przeprowadzi szkolenia dla Analityków Danych, Data Scientist i użytkowników zaawansowanych, obejmujące minimalny, wymagany zakres zagadnień: 1. model danych, 2. budowa kohorty (fenotypu) w oparciu o interfejs, 3. budowa kohorty (fenotypu) w oparciu o SQL, 4. zarządzanie fenotypami, 5. generowanie feature store dla fenotypu (SQL/Python), 6. zarządzanie i udostępnianie feature store, 7. przetwarzanie danych obrazowych, 8. udostępnianie danych obrazowych, 9. projektowanie rozwiązań do uczenia maszynowego, 10. eksplorowanie obszaru roboczego usług Platformy, 11. praca z danymi w usługach platformy, 12. praca z obliczeniami w usługach platformy, 13. automatyzowanie wyboru modelu uczenia maszynowego za pomocą dostępnych usług Platformy.

Sz.7	Wykonawca przeprowadzi szkolenia dla Specjalisty ds. Bezpieczeństwa, obejmujące minimalny, wymagany zakres zagadnień: 1. analiza przypadków związanych z bezpieczeństwem w chmurze, 2. praktyczne scenariusze i ćwiczenia laboratoryjne, 3. monitoring i audytowanie, 4. narzędzia do monitorowania aktywności w chmurze, 5. audytowanie zgodności z regulacjami i standardami bezpieczeństwa aplikacji w chmurze, 6. zagadnienia związane z bezpieczeństwem kodu, 7. przeprowadzanie testów penetracyjnych w środowisku chmurowym, 8. zarządzanie zdarzeniami bezpieczeństwa (SIEM), 9. wprowadzenie do systemów SIEM, 10. analiza zdarzeń bezpieczeństwa w chmurze, 11. kontrola dostępu, 12. zarządzania tożsamościami i dostępem (IAM), 13. mechanizmy uwierzytelniania i autoryzacji, 14. zarządzanie kluczami i szyfrowanie, 15. szyfrowanie w ruchu i w spoczynku, 16. bezpieczne przechowywanie i zarządzanie kluczami.
Sz.8	Wykonawca przeprowadzi szkolenia dla Użytkowników Podstawowych, obejmujące minimalny, wymagany zakres zagadnień: 1. dostęp i przegląd udostępnionych danych oraz bezpiecznego korzystania z Platformy i udostępnionych danych, 2. proces wnioskowania o dane, 3. budowa kohorty (fenotypu) w oparciu o interfejs, 4. praca z narzędziami analitycznymi w oparciu o udostępnione dane, 5. raportów.
Sz.9	Szkolenia zostaną przeprowadzone przez Wykonawcę w wymiarze czasowym dostosowanym do zakresu danego szkoleniu, nie krótszym jednak niż 2 dni szkoleniowe przypadające na każdą z ról.
Sz.10	Terminy szkoleń Wykonawca uzgodni z Zamawiającym.
Sz.11	Szkolenia będą prowadzone przez Wykonawcę w trybie stacjonarnym w siedzibie GUMed lub zdalnie - zgodnie z decyzją Zamawiającego.
Sz.12	Szkolenia składają się z dwóch bloków: części teoretycznej (20% czasu) oraz części warsztatowej z ćwiczeniami (80% czasu).
Sz.13	Wykonawca przeprowadzi szkolenia przy zachowaniu odpowiedniej wielkości grupy (maksymalnie 10 osób - 1 grupa). Wykonawca dopasuje ilość grup szkoleniowych do charakteru zespołu biorącego udział po stronie Zamawiającego w projekcie.
Sz.14	Szkolenia dostarczają wymaganą wiedzę, w tym wiedzę techniczną oraz uczą uczestników praktycznego użycia funkcjonalności Platformy IP_CMC i niezbędnych narzędzi do realizacji procesów IP_CMC oraz wymaganych zadań po stronie pracowników GUMed pełniących role użytkowników, administratorów i operatorów Platformy CMC.

Sz.15	Wykonawca zobowiązany jest do zorganizowania i pokrycia wszelkich kosztów Wykonawcy związanych z przeprowadzeniem szkoleń.
Sz.16	Wykonawca opracuje plany szkoleń zawierające szczegółowy zakres tematyczny, w podziale na role oraz uwzględniając liczbę i skład uczestników szkoleń, co najmniej 14 Dni Roboczych przed planowanym szkoleniem, chyba że ustalony zostanie krótszy termin.
Sz.17	Wykonawca zobowiązany jest do dostarczenia materiałów szkoleniowych i pomocy szkoleniowych (bryki, pomoce dydaktyczne, prezentacje, zeszyt ćwiczeń, kod źródłowy lub skrypty wykorzystywane do realizacji ćwiczeń) w celu kontynuowania szkoleń przez Zamawiającego w przyszłości. Materiały powinny być w języku polskim i angielskim.
Sz.18	Szkolenia będą prowadzone w języku polskim.
Sz.19	Wykonawca dostarczy stosowne materiały szkoleniowe i pomoce szkoleniowe w niezbędnej ilości 3 Dni Roboczych przed planowanym szkoleniem w formie elektronicznej (na elektronicznym nośniku danych, w formie gotowej do wydruku)
Sz.20	Materiały i pomoce szkoleniowe muszą być napisane w prosty i przejrzysty sposób, ułatwiający zrozumienie i wykorzystanie Platformy IP_CMC oraz szybkiego i skutecznego wyszukiwania rozwiązania wyjścia z problematycznych sytuacji. Materiały szkoleniowe dla trenerów przygotowane będą w sposób umożliwiający samodzielne zorganizowanie i przeprowadzenie szkoleń dla użytkowników i muszą zawierać co najmniej konspekt szkolenia wraz z zakresem szkolenia z podziałem na jednostki szkoleniowe, opis celów głównych i szczegółowych wraz z opisem spodziewanych efektów, przykłady szkoleniowe oraz opis sposobu przeprowadzania zajęć.
Sz.21	Wykonawca ma obowiązek zapewnić wykładowców, trenerów szkoleniowych posiadających odpowiednie kwalifikacje zawodowe oraz doświadczenie (dydaktyczne/trenerskie) umożliwiające w sposób efektywny przeprowadzić zajęcia pozwalający uczestnikom przyswoić przekazywaną wiedzę merytoryczną i praktyczną.
Sz.22	Wykładowca/trener oddelegowany przez Wykonawcę do przeprowadzenia szkoleń powinien posiadać certyfikaty, które potwierdzają jego wiedzę, umiejętności i doświadczenie w obszarze technologii wdrażanej Platformy, narzędzi, funkcjonalności oraz powinien posiadać praktyczne doświadczenie z podobnych projektów w obszarach: Big Data, Data Lake, Data Lakehouse, AI/ML, Cloud. Wykładowca/tener musi posiadać certyfikaty dopasowane do technologii stosowanej przy budowie Platformy IP_CMC i oferowane przez firmy technologiczne, takie jak Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), Oracle i inne. Zamawiający wymaga, aby co najmniej jeden z wykładowców posiadał również certyfikat na poziomie architektury wybranej platformy chmurowej, np.: AWS Certified Solutions Architect - Associate, Microsoft Certified: Azure Solutions Architect Expert, Google Cloud Certified - Professional Cloud Architect, Certified Kubernetes Administrator (CKA), CompTIA Cloud+ Certification lub równoważne.
Sz.23	Szczegółowy program szkoleń oraz konspekt zostaną opracowane przez Wykonawcę i przedstawione do akceptacji Zamawiającego w ciągu 7 Dni Roboczych od daty zawarcia umowy. Zamawiający w ciągu 3 Dni Roboczych zaakceptuje go lub odeśle do poprawy. Poprawiony program szkoleń Wykonawca musi przekazać Zamawiającemu w ciągu 3 Dni Roboczych.

Sz.24	Po zakończeniu szkolenia każdej grupy tematycznej Wykonawca zobowiązany będzie do złożenia Protokołu Odbioru szkolenia, zawierającego co najmniej: datę szkolenia, obszar, zakres szkolenia, informacje o osobach przeprowadzających szkolenie, informacje o osobach przeszkolonych, wyniki testów (jeśli były wykonywane) oraz ilość godzin szkolenia. Do protokołu zostanie dołączona lista obecności podpisana przez uczestników szkolenia.
Sz.25	Na zakończenie szkolenia Wykonawca zobowiązany jest przygotować i przekazać uczestnikom szkolenia zaświadczenia potwierdzające udział w szkoleniu.
Sz.26	Fakt przeprowadzenia szkoleń musi zostać potwierdzony podpisami użytkowników Platformy lub listą obecności wygenerowaną on-line; biorących udział w szkoleniu.
Sz.27	Zamawiający udostępni Wykonawcy salę szkoleniową i dostęp do sieci Internet, jeśli szkolenia będą prowadzone w siedzibie Zamawiającego.
Sz.28	Strony podpisują protokół odbioru szkoleń wraz z dołączeniem listy obecności oraz na podstawie dostarczonych materiałów szkoleniowych.
Sz.29	Wykonawca zobowiązany jest do oznaczenia wszelkich materiałów szkoleniowych logotypami oraz informacjami "o projekcie" dostarczonymi przez Zamawiającego.
Sz.30	Zamawiający może uznać szkolenie za przeprowadzone niezależnie od liczby biorących w nim udział uczestników.
Sz.31	Szkolenia zostaną przeprowadzone zgodnie z założeniem realizacji Kamieni Milowych, wskazanych przez Zamawiającego. Terminy szkoleń ustalone zostaną pomiędzy Zamawiającym, a Wykonawcą każdorazowo, ale nie później niż. na 14 dni przed datą przeprowadzenia dedykowanego szkolenia.
Sz.32	Zamawiający zastrzega sobie prawo do zmiany ilości uczestników szkolenia do maksymalnie 50% zakładanej liczby osób przypadającej na jedną grupę, o czym poinformuje Wykonawcę.
Sz.33	Wykonawca przeprowadzi szkolenie ze szczególną dbałością o realizację zajęć zarówno teoretycznych, jak i praktycznych oraz dobór metod szkoleniowych, które Wykonawca wskaże w zaproponowanym programie, zatwierdzonym przez Zamawiającego.

6. Wymagania w zakresie zarządzania projektem

Zamawiający oczekuje, że Wykonawca w ramach realizacji prac projektowych obligatoryjnie spełni wymagania w zakresie dostosowania metodyki zwinnej prac projektowych, iteracyjnego przyrostu wytwarzanego przedmiotu zamówienia (ang. Agile) oraz będzie używał narzędzi zarządczych adekwatnych do warunków projektu i zgodnych z wytycznymi Zamawiającego opisanymi poniżej:

Nr	Punkt kontrolny
PM.1	Podczas realizacji prac Wykonawca będzie stosował metodykę zwinną pracy oraz będzie stosował następujące elementy prowadzenia projektu (lub równoważne): 1. Zarządzanie zakresem produktów, wdrożeń oraz wydań 2. Zarządzanie harmonogramem wdrożenia 3. Zarządzanie budżetem projektu 4. Zarządzanie komunikacją w zespole projektowym oraz z interesariuszami 5. Zarządzanie wykorzystywanymi zasobami

	6. Zarządzanie jakością dostarczanych produktów 7. Zarządzanie wymaganiami oraz dokumentacją 8. Zarządzanie ryzykiem 9. Zarządzanie jakością 10. Zarządzanie zmianą
PM.2	Podczas realizacji prac Wykonawca będzie dostarczał minimalnie następujące dokumenty (produkty z procesu zarządzania projektem): 1. Harmonogram 2. Plan projektu 3. Rejestr ryzyk 4. Analiza przedwdrożeniowa 5. Projekt Techniczny 6. Plan Migracji 7. Plan Testów Akceptacyjnych 8. Raport z Testów 9. Plan Szkoleń 10. Sprawozdanie ze Szkoleń 11. Plan Startu Produkcyjnego 12. Raport z Wdrożenia Systemu 13. Raporty z Realizacji Serwisu Gwarancyjnego Podczas realizacji prac Wykonawca dostarczy wspólnie z Zamawiającym Scenariusze Testów Akceptacyjnych.
PM.3	Wykonawca będzie cyklicznie, nie rzadziej niż raz na kwartał, przedstawiał wyniki przeglądów kontrolnych każdego elementu procesu prowadzenia projektu oraz badał jakość produktów (rezultatów), o których mowa wyżej.
PM.4	Harmonogram zawiera terminy realizacji szczegółowych prac i zadań związanych z realizacją projektu, w tym w szczególności terminy dostarczania rezultatów, odpowiedzialnych, a także udział i obciążenie pracą przedstawicieli Zamawiającego i Wykonawcy. Harmonogram będzie każdorazowo uszczegóławiany przed rozpoczęciem realizacji każdego kolejnego Etapu Projektu.
PM.5	Plan projektu (lub równoważny dokument) zawiera informacje niezbędne do zarządzania projektem, określa cele i potrzeby biznesowe Zamawiającego. Plan Projektu składa się co najmniej z następujących elementów: 1. Struktury organizacyjnej projektu. 2. Reguł jakościowych. 3. Standardów i procedur projektowych, w tym dotyczących zarządzania zmianą, zarządzania wydaniami, zarządzania ryzykiem, zarządzania jakością, zarządzania komunikacją, raportowania. 4. Definicji Rejestrów: Ryzyka, Zmian. 5. Opisu monitorowania postępów prac. 6. Opisu przyjętej metody zarządzania projektem. W ramach Planu Projektu Wykonawca przygotuje szablony dla wszystkich dokumentów projektowych wymaganych przyjętą metodyką pracy, w tym raportów, sprawozdań, rejestrów, notatek, protokołów, itp., które zaakceptuje Zamawiający.

PM.6	Dokument "Analiza Przedwdrożeniowa" obejmuje wykonanie niezbędnych prac analitycznych i architektonicznych, w tym spotkania, warsztaty i wywiady z pracownikami Zamawiającego, mające na celu opracowanie szczegółowego projektu koncepcji biznesowej, poprawne zaprojektowanie Platformy IP_CMC oraz zaplanowanie wszystkich czynności na etapach: budowy, wdrożenia, migracji danych i testów. W ramach analizy uszczegółowione zostaną wszystkie zapisy OPZ w celu wyeliminowania błędów interpretacyjnych. Analiza obejmuje bezpośrednią współpracę z pracownikami Zamawiającego w siedzibie zamawiającego. Rezultatem prac w trakcie Analizy jest dokumentacja w formacie Word oraz złożona w odpowiedniej notacji w repozytorium Enterprise Architect Zamawiającego (EA), która zawiera co najmniej: 1. diagramy oraz modele wraz z opisami dla wszystkich procesów biznesowych, 2. opisy realizacji procesów biznesowych na Platformie CMC, 3. opis architektury oraz diagramy architektoniczne na poziomie: logicznym, danych i infrastruktury, 4. opis integracji z innymi systemami Zamawiającego i Partnerów Zamawiającego, 5. szczegółowy opis modelu danych w każdym ze zbiorników danych, np: danych surowych (RAW), danych składowanych (STAGE), danych przeliczeniowych i danych syntetycznych (CUBES & CURATED) wraz ze wskazaniem atrybutów obligatoryjnych i opcjonalnych i ich formatów, a w przypadku pól słownikowych przedstawienie zawartości każdego ze słowników, 6. kompletny i szczegółowy opis przyjętych rozwiązań funkcjonalnych wraz z informacjami o użytych narzędziach i ich konfiguracji, 7. zestawienie oczekiwanych testów potwierdzających działanie Platformy CMC, 8. koncepcję środowiska uruchomieniowego Platformy CMC, 9. koncepcję administracji platformą oraz zasad administrowania środowiskiem na poziomie: chmury, aplikacji, infrastruktury i danych, 10. zasady ochrony danych osobowych na Platformie CMC.
PM.7	Dokument "Projekt Techniczny" zawiera co najmniej: 1. Plan Migracji 2. Plan Testów 3. Plan Szkoleń 4. Plan Startu Produkcyjnego 5. Dokładną architekturę Platformy CMC 6. Listę funkcji Oprogramowania wraz z opisem 7. Opis konfiguracji i parametryzacji komponentów Platformy CMC 8. Opis hardeningu silników baz danych oraz dostępu do danych 9. Opis struktur bazy danych, JSONów i zbiorników danych (opis: schematów, tablic, pól oraz opis wzajemnych powiązań) 10. Opis bibliotek i komponentów stron trzecich oraz rozszerzeń i modyfikacji tych bibliotek i komponentów wykonanych na potrzeby Platformy CMC 11. Opis modelu uprawnień, ról wraz z opisem zależności 12. Opis przyjętych standardów bezpieczeństwa i zgodności, zasad bezpieczeństwa i ochrony danych 13. Specyfikację wariantową wymiarów środowiska infrastrukturalnego i usług chmurowych spełniających wymagania wydajnościowe (plan dot. skalowalności)

	14. Koncepcję administrowania Platformą IP_CMC w modelu DevSecOps, CI/CD 15. Plan ciągłości działania, odtworzenia i automatyzacji deploymentu komponentów Platformy CMC 16. Wykaz licencji koniecznych do prawidłowego działania Platformy CMC 17. Wykaz Oprogramowania z wyszczególnieniem komponentów instalowalnych 18. Wykaz dokumentacji zewnętrznej, w przypadku dokonywania referencji w Projekcie Technicznym do dokumentów specyficznych dostawców albo standardów branżowych 19. Opis narzędzi do przeprowadzenia testów automatycznych w modelu CI/CD
PM.8	Dokument "Plan migracji" zawiera minimalnie następujące elementy: 1. Identyfikację źródeł danych i diagramy przepływów; 2. Określenie wolumenu, jakości oraz aktualności danych; 3. Wskazanie narzędzi i sposobu wykonania migracji danych oraz trybu: jednorazowo, cyklicznie; 4. Opis sposobów zapewnienia bezpieczeństwa danych (poufność i rozliczalność); 5. Zdefiniowanie skryptów wykonywalnych dla migracji wraz z opisem ich działania na danych; 6. Opis narzędzi automatyzujących obróbkę danych; 7. Opis narzędzi wspomagających i asystujących w czasie migracji; 8. Opis metody weryfikacji danych oraz narzędzi wykorzystywanych do weryfikacji; 9. Opis narzędzi wykorzystywanych do zapewnienia poprawności procesu wdrożenia.
PM.9	Dokument "Plan Testów" zawiera co najmniej: 1. Zdefiniowany zakres i cele przeprowadzenia Testów: Jednostkowych, Akceptacyjnych, Regresyjnych oraz Odbiorczych 2. Opis sposobu przeprowadzania Testów: Jednostkowych, Akceptacyjnych, Regresyjnych oraz Odbiorczych 3. Harmonogram prowadzenia Testów 4. Wykaz czynności niezbędnych do wykonania przed przeprowadzeniem Testów, np. przygotowanie środowisk i danych 5. Opis struktury organizacyjnej wraz z podziałem odpowiedzialności wymaganych w czasie Testów 6. Opis strategii podejścia do przypadków testowych 7. Wskazanie jasnych kryteriów akceptacji Testów 8. Opis klasyfikacji wykrytych nieprawidłowości i błędów oraz zasad postępowania z nimi 9. Opis zasad i trybu naprawy wykrytych nieprawidłowości 10. Opis zasad sporządzenia Raportu z Testów 11. Szablony dokumentów wymagane do prowadzenia Testów, np. szablony dokumentów WORD, XLS albo szablony w systemie informatycznych do obsługi zgłoszeń. Niezależnie, szczegółowe wymagania dla Testów, Przypadków Testowych, Scenariuszy Testowych - wymagane przez Zamawiającego - są opisane w części "Testy".
PM.10	Dokument "Scenariusze Testów" uwzględniają w szczególności: 1. Opis przypadków testowych 2. Opis kroków testowych

	3. Opis wymaganych danych wejściowych i stanu środowiska Platformy IP_CMC na dzień przeprowadzenia Testów 4. Opis kryteriów poprawności danego przypadku testowego 5. Definicje postępowania w czasie testów, np. w przypadku nieprawidłowości lub niemożliwości przeprowadzenia przypadku testowego Niezależnie, szczegółowe wymagania dla Testów, Przypadków Testowych, Scenariuszy Testowych - wymagane przez Zamawiającego - są opisane w części "Testy".
PM.11	Dokument "Raport z Testów" zawiera co najmniej: 1. Lokalizację prowadzenia Testów oraz typ Testu, np.: Jednostkowe, Akceptacyjne, Regresyjne albo Odbiorcze; 2. Zakres danych i konfigurację środowiska, w którym przeprowadzono Testy; 3. Wykaz osób przeprowadzających Testy; 4. Terminy przeprowadzenia Testów oraz długość ich trwania; 5. Opis przebiegu Testów wraz z listą przetestowanych scenariuszy testowych i przypadków użycia wraz z podsumowaniem wyników; 6. Wykaz zgłoszonych Błędów; 7. Wykaz zgłoszonych zmian; 8. Wnioski końcowe i zalecenia. Niezależnie, szczegółowe wymagania dla Testów, Przypadków Testowych, Scenariuszy Testowych - wymagane przez Zamawiającego - są opisane w części "Testy", a sam Raport z Testów będzie przygotowywany przez Wykonawcę nie rzadziej niż raz w tygodniu w czasie Etapy Testów.
PM.12	Dokument "Plan Szkoleń" zawiera w szczególności: 1. Wykaz planowanych Szkoleń wraz z specyfikacją zagadnień, zakresem szkolenia i opisem grupy docelowej odbiorców; 2. Harmonogram Szkoleń; 3. Sylabusy dla poszczególnych Szkoleń. Szczegółowe wymagania dotyczące sposobów przeprowadzania szkoleń są w części "Szkolenia".
PM.13	Dokument "Sprawozdanie ze Szkoleń" zawiera: 1. Podsumowanie zakresu i grup docelowych dla przeprowadzonych Szkoleń; 2. Informacje na temat miejsca i formy przeprowadzonych Szkoleń; 3. Listę uczestników Szkoleń wraz z podpiętymi listami obecności; 4. Wyniki testów sprawdzających wiedzę każdego uczestnika po Szkoleniu; 5. Wyniki zbiorcze z ankiet ewaluacyjnych wypełnionych przez uczestników Szkoleń. Szczegółowe wymagania dotyczące sposobów przeprowadzania szkoleń są w części "Szkolenia".
PM.14	Dokument "Plan Startu Produkcyjnego" zawiera: 1. Opis czynności wymaganych do uruchomienia środowiska produkcyjnego; 2. Harmonogram przejścia na środowisko produkcyjne rozpisane z dokładnością do godzin; 3. Harmonogram wstępnych przygotowań (przed dniem migracji); 4. Harmonogram migracji danych; 5. Opis konfiguracji kont Użytkowników oraz przypisanie wymaganych uprawnień i parametrów;

	6. Opis planu awaryjnego na wypadek opóźnień lub błędów, w tym plan wycofania się ze Startu Produkcyjnego; 7. Opis organizacji zespołu wsparcia po Starcie Produkcyjnym (tzw. War Room); 8. Plan Asysty technicznej na etapie stabilizacji po Starcie Produkcyjnym.
PM.15	Dokument "Raport z Wdrożenia Systemu" zawiera: 1. Podsumowanie przebiegu wdrożenia; 2. Szczegółową ewidencję Zgłoszeń realizowanych w zakresie Asysty Technicznej w fazie stabilizacji; 3. Informację o wprowadzonych poprawkach i modyfikacjach w fazie stabilizacji; 4. Raport testów wydajności; 5. Raport z potwierdzeniem od właścicieli biznesowych Platformy IP_CMC oraz od wybranych kluczowych użytkowników, że Platforma IP_CMC działa poprawnie i spełniania wszystkie wymagania zapisane w Zamówieniu; 6. Opis osiągnięcia końcowych efektów i ich zgodności z planem opisanym w Planie Projektu; 7. Raport z zebranych doświadczeń (tzw. lessons learnt).
PM.16	Comiesięczne "Raporty z realizacji Serwisu Gwarancyjnego" zawierają co najmniej: 1. Wykres zawierający: liczbę Zgłoszeń, liczbę Błędów, czas podjęcia, czas obsługi, opóźnienie względem SLA; 2. Raport z liczbą przeprowadzonych konsultacji; 3. Wykaz zastosowanych i zaimplementowanych rozwiązań tymczasowych oraz docelowych; 4. Raport dotyczący wdrożonych aktualizacji; 5. Rozliczenie godzin asysty zgodnie z umową, w tym wskazanie procentu wykorzystania puli godzin asysty.
PM.17	Zamawiający wskaże akceptowalne narzędzie do zarządzania wątkami w projekcie i zadaniami, np. JIRA.
PM.18	Wykonawca będzie się kontaktował z przedstawicielami Zamawiającego między innymi za pomocą narzędzi elektronicznych takich jak: MS Team, JIRA, Sharepoint, MS Office 365, Enterprise Architect.
PM.19	W zależności od poszczególnych etapów i kontekstu Projektu Wykonawca będzie uczestniczył w cyklicznych spotkaniach Daily, Planowaniach, Refinementach, Retrospektywach. Terminy spotkań Wykonawca uzgodni wspólnie z Zamawiającym.
PM.20	Zamawiający powołał Komitet Sterujący i może zobligować Wykonawcę do udziału w spotkaniach jako głos doradczy.
PM.21	W ramach realizacji zakresu Projektu, Wykonawca odpowiada za dotrzymywanie Faz Projektu, zgodnie z Załącznikiem nr 7 do Umowy.
PM.22	Wykonawca przygotuje i dostarczy dokumentację projektowo-wdrożeniową, powdrożeniową, techniczną, zgodną z wymaganiami Zamawiającego opisanymi w OPZ, części "Zarządzanie Projektem", zapewniającą także zrozumienie struktury, funkcji oraz zaleceń dotyczących dalszej pracy nad Projektem.
PM.23	Wykonawca zapewni, że powdrożeniowa dokumentacja projektu IT będzie dokładna, aktualna i łatwo dostępna dla wszystkich zainteresowanych stron.

PM.24	Wykonawca sporządzi i dostarczy Zamawiającemu dokumentację powdrożeniową zawierającą rejestry zmian i wersji dokumentacji wdrożeniowej: Dokumentację dotyczącą historii projektu, w tym wprowadzonych zmian, aktualizacji i wersji Platformy CMC.
PM.25	Wykonawca dostarczy Zamawiającemu dokumentację powdrożeniową architektury systemu, zawierającą szczegółowy opis wdrożonej architektury technicznej Platformy CMC, w tym informacje na temat struktury systemu, warstw aplikacji, komponentów, baz danych, integracji z innymi systemami, informacje o użytych technologiach, frameworkach i bibliotekach.
PM.26	Wykonawca dostarczy Zamawiającemu instrukcje instalacji opisujące krok po kroku instrukcje dotyczące instalacji wszystkich niezbędnych składników Platformy IP_CMC lub aplikacji, wraz z konfiguracją środowiska, a także procedury wdrożenia, w tym wszelkie skrypty automatyzujące te procesy.
PM.27	Wykonawca przekaże Zamawiającemu dokumentację powdrożeniową zawierającą opis konfiguracji dotyczący Platformy CMC, w tym ustawień aplikacji, parametrów serwera, ustawień bazy danych, konfiguracji sieciowej, szczegółowe informacje dotyczące konfiguracji środowiska produkcyjnego, w tym konfiguracji serwerów, baz danych, sieci i innych zasobów IT. Dane dotyczące konfiguracji zabezpieczeń, takie jak firewalle, polityki dostępu itp.
PM.28	Wykonawca w ramach dokumentacji powdrożeniowej dostarczy Zamawiającemu opis procedury aktualizacji zawierające Informacje o tym, jak aktualizować Platformę CMC, w tym opis potencjalnych zagrożeń.
PM.29	Wykonawca dostarczy Zamawiającemu dokumentację opisującą Informacje na temat danych testowych, które mogą być wykorzystane do testowania Platformy IP_CMC po wdrożeniu.
PM.30	Wykonawca przygotuje i przekaże Zamawiającemu instrukcje użytkowania. Dokumentację, instrukcję przeznaczoną dla użytkowników końcowych, zawierającą instrukcje dotyczące korzystania z systemu, obsługi interfejsu użytkownika, wykonywania podstawowych czynności itp. zgodną z wymaganiami określonymi w Rozdziale 13.
PM.31	Procedury użytkowe: Dokumentacja zawierająca opisy procedur i procesów, które należy przestrzegać podczas korzystania z Platformy CMC.
PM.32	Wykonawca dostarczy Zamawiającemu dokumentację zawierającą informacje na temat sposobu raportowania błędów i usterek w systemie, wraz z instrukcjami dotyczącymi sposobu zgłaszania problemów i śledzenia ich statusu.
PM.33	W ramach dokumentacji powdrożeniowej Wykonawca przekaże Zamawiającemu informacje kontaktowe do zespołu wsparcia technicznego, wraz z procedurami zgłaszania pytań, problemów lub żądań pomocy.
PM.34	Wykonawca przekaże Zamawiającemu dokumentację techniczną zawierającą szczegółowe informacje techniczne dotyczące kodu źródłowego, struktury baz danych, API, integracji zewnętrznych systemów itp. Dokumentacja API i interfejsów w tym opisy endpointów, metod i przykłady użycia.
PM.35	W ramach dokumentacji powdrożeniowej Wykonawca dostarczy Zamawiającemu politykę bezpieczeństwa, zawierającą informacje dotyczące polityki bezpieczeństwa systemu, w tym zabezpieczeń, uwierzytelniania, kontroli dostępu, szyfrowania danych itp.

	Plan awaryjny i procedury odzyskiwania danych, szczegółowe procedury na wypadek awarii systemu, w tym plany odzyskiwania po katastrofie i kopie zapasowe.
PM.36	Wykonawca przygotuje i przekaże Zamawiającemu podręczniki dla użytkowników końcowych, w tym instrukcje obsługi systemu, często zadawane pytania (FAQ) i rozwiązywanie problemów.
PM.37	Wykonawca przekaże Zamawiającemu instrukcje aktualizacji, procedury i instrukcje dotyczące aktualizacji systemu, w tym aktualizacji oprogramowania, migracji danych, itp.
PM.38	Dokumentacja powdrożeniowa przygotowana i przekazana Zamawiającemu przez Wykonawcę powinna zawierać dane kontaktowe osób odpowiedzialnych za projekt, wsparcie techniczne i utrzymanie systemu.
PM.39	Wykonawca przekaże Zamawiającemu informacje na temat licencji oprogramowania, zewnętrznych bibliotek, użytych grafik itd.

7. Wymagania w zakresie zespołu projektowego

Zespół projektowy winien składać się z przedstawicieli Wykonawcy i Zamawiającego. Taka konfiguracja pozwoli na płynne procedowanie zadań związanych z przyjętym zakresem jak i wytworzenie produktu zgodnie z wymogami Zamawiającego.

W skład zespołu Wykonawcy muszą wchodzić minimum następujące role oraz osoby spełniające wymagania postępowania, określonego w OPZ. Dla każdej z wymienionych ról Zamawiający szczegółowo opisał wymagany obligatoryjnie minimalny zakres obowiązków i odpowiedzialności:

Nr	Punkt kontrolny
ZP.1	Wykonawca wskaże imiennie osoby zaangażowane w projekt do pełnienia poniższych ról: 1. Koordynatora Projektu Wykonawcy, 2. Architekta rozwiązania, 3. Analityka, 4. Specjalistów wdrożeniowych, 5. Specjalistów do spraw integracji, 6. Programistów, 7. Testerów oprogramowania.
ZP.2	Do obowiązków Koordynatora Projektu Wykonawcy będzie należało: 1. Odpowiedzialność za dotrzymywanie terminów harmonogramu, kamieni milowych i zależności między zadaniami wskazanymi przez Zamawiającego. 2. Koordynowanie działań członków zespołu projektowego Wykonawcy oraz zapewnienie, że każdy wie, jakie są jego zadania i cele. 3. Ścisła współpraca z Kierownikiem Projektu oraz Liderami Trib'ów po stronie Zamawiającego, 4. Zapewnienie płynnej komunikacji między członkami zespołu, interesariuszami. 5. Regularne raportowanie postępu prac oraz ewentualnych problemów i ryzyk związanych z Projektem. Zgłaszanie i potwierdzanie gotowości do odbioru przyrostów Kierownikowi Projektu Zamawiającego. 6. Monitorowanie zużycia zasobów Wykonawcy i podejmowanie działań w celu ich optymalizacji. 7. Identyfikacja problemów i wyzwań projektowych oraz podejmowanie skutecznych działań naprawczych, a także stała komunikacja z Zamawiającym w tym zakresie.

	8. Współpraca z zespołem Wykonawcy w celu rozwiązywania konfliktów i eliminowania przeszkód w realizacji Projektu. 9. Identyfikacja, ocena ryzyk związanym z Projektem, w tym opracowywanie strategii minimalizacji ryzyka oraz stała komunikacja z Zamawiającym w tym zakresie. 10. Monitorowanie potencjalnych zagrożeń i podejmowanie działań prewencyjnych. 11. Zapewnienie, że wszystkie produkty i dostarczone rozwiązania spełniają ustalone standardy jakościowe oraz wymagania Zamawiającego. 12. Monitorowanie procesów kontroli jakości i podejmowanie działań korygujących w razie potrzeby. 13. Zarządzanie procesem wprowadzania zmian w projekcie oraz ocena ich wpływu na harmonogram, koszty i jakość. 14. Zapewnienie, że wszelkie zmiany są właściwie dokumentowane i komunikowane zainteresowanym stronom. 15. Prowadzenie dokumentacji projektowej, w tym planów projektowych, raportów, protokołów spotkań oraz innych istotnych dokumentów. Wymagania dotyczące dokumentacji projektowej Zamawiający opisał w OPZ, części „Zarządzanie Projektem" i „Dokumentacja". 16. Udostępnianie dokumentacji dla zespołu projektowego i zainteresowanych strony. 17. Organizacja szkoleń i warsztatów dla członków zespołu w celu podnoszenia ich umiejętności i efektywności pracy.
ZP.3	Do obowiązków Architekta rozwiązania Wykonawcy będzie należało: 1. Współpraca z interesariuszami w celu identyfikacji i zrozumienia potrzeb użytkowników oraz wymagań funkcjonalnych i niefunkcjonalnych Projektu. 2. Projektowanie architektury rozwiązania, uwzględniając wymagania funkcjonalne, niefunkcjonalne i ograniczenia technologiczne. 3. Określanie struktury Platformy CMC, komponentów, interfejsów i relacji między nimi. 4. Dobór odpowiednich technologii i narzędzi do realizacji architektury rozwiązania. 5. Ocena i analiza różnych technologii pod kątem ich przydatności oraz zgodności z wymaganiami Projektu. 6. Tworzenie prototypów koncepcyjnych i technicznych w celu weryfikacji wybranych rozwiązań oraz prezentacji. 7. Opracowywanie dokumentacji technicznej, w tym specyfikacji architektonicznej, diagramów UML oraz opisów technicznych rozwiązań, modelowanie w języku Archimate. 8. Udzielanie wsparcia zespołowi programistycznemu w zrozumieniu i implementacji przyjętej architektury. 9. Pomoc w rozwiązywaniu problemów architektonicznych i technicznych w trakcie procesu implementacji. 10. Zarządzanie konfiguracją oprogramowania oraz kontrola wersji kodu źródłowego. 11. Określanie i wdrażanie standardów dotyczących zarządzania konfiguracją. 12. Optymalizacja architektury w celu zapewnienia wysokiej wydajności i skalowalności systemu. 13. Identyfikacja i usuwanie wąskich gardeł oraz implementacja rozwiązań poprawiających wydajność. 14. Identyfikacja, ocena i zarządzanie ryzykiem związanym z architekturą rozwiązania.

	15. Opracowywanie strategii minimalizacji ryzyka oraz szybkiego reagowania w przypadku jego wystąpienia. 16. Udzielanie szkoleń i mentoringu dla członków zespołu w zakresie architektury Platformy CMC, oprogramowania oraz nowych technologii.
ZP.4	Do obowiązków Analityka Wykonawcy będzie należało: 1. Przeprowadzenie szczegółowej analizy dokumentacji zamówienia w celu zrozumienia wymagań Zamawiającego oraz specyfikacji technicznych i funkcjonalnych. 2. Przeprowadzenie warsztatów analizy wymagań Zamawiającego, w celu zrozumienia jego potrzeb biznesowych, a także wymagań dotyczących integracji różnych systemów, aplikacji lub usług w ramach wdrożenia Platformy IP_CMC . 3. Zbieranie, organizowanie i przetwarzanie danych z różnych źródeł. Współpraca z interesariuszami Projektu w celu identyfikacji i zrozumienia potrzeb użytkowników oraz wymagań funkcjonalnych i niefunkcjonalnych Projektu. 4. Wykorzystanie technik analizy danych do identyfikacji trendów, wzorców i zależności, które mogą być istotne dla realizacji przedmiotu zamówienia. 5. Tworzenie modeli danych i analizowanie ich w celu przewidywania zachowań, trendów lub wyników biznesowych. 6. Przygotowywanie raportów, prezentacji i wizualizacji danych, które pomagają w zrozumieniu wyników analiz i podejmowaniu decyzji. 7. Współpraca z innymi członkami zespołu projektowego, w tym programistami, architektem i przedstawicielami Zamawiającego, w celu zapewnienia zgodności z wymaganiami i terminami Projektu. 8. Testowanie opracowanych rozwiązań, weryfikacja ich poprawności i skuteczności oraz zapewnienie zgodności z wymaganiami Zamawiającego. 9. Identyfikacja obszarów do optymalizacji i usprawnienia procesów na podstawie analizy danych oraz wyników Projektu. 10. Dokumentowanie procesów analizy danych, podejmowanych decyzji i uzyskiwanych wyników w celu zapewnienia możliwości śledzenia oraz zrozumienia dla zainteresowanych stron. 11. Zapewnienie wsparcia powdrożeniowego, w tym szkoleń dla personelu Zamawiającego oraz udzielanie pomocy technicznej w przypadku problemów związanych z wdrożeniem rozwiązań. 12. Aktywna współpraca z wszystkimi członkami zespołu projektowego i bieżąca komunikacja z zespołem projektowym oraz uczestnictwo w cyklicznych spotkaniach wskazanych przez Zamawiającego.
ZP.5	Do obowiązków Specjalistów Wdrożeniowych Wykonawcy będzie należało: 1. Współpraca z zespołem projektowym w celu opracowania strategii wdrożenia oraz harmonogramu działań, a także monitorowania postępu prac oraz zapewnienia terminowego dostarczenia rozwiązania. 2. Zarządzanie zasobami i czasem pracy po stronie zespołu Wykonawcy, w celu efektywnego wykonania zadań związanych z wdrożeniem Platformy CMC. 3. Ocena niezbędnych integracji, istniejącej infrastruktury, Zamawiającego i identyfikacja potencjalnych wyzwań w procesie wdrożenia. 4. Instalacja i konfiguracja oprogramowania oraz narzędzi niezbędnych do wdrożenia Platformy IP_CMC zgodnie z wymaganiami Zamawiającego.

	5. Testowanie i weryfikacja poprawności konfiguracji Platformy IP_CMC przed przejściem do etapu wdrożenia. 6. Koordynowanie testów po stronie zespołu Wykonawcy, czy przebiegają one zgodnie z wymaganiami Zamawiającego opisanymi w OPZ, części Testy. 7. Opracowywanie i dostosowywanie rozwiązań technologicznych zgodnie z wymaganiami Projektu. 8. Wsparcie integracji Platformy IP_CMC z istniejącymi systemami oraz dostosowywanie do specyficznych potrzeb Zamawiającego. 9. Weryfikacja zgodności z wymaganiami Zamawiającego oraz identyfikacja ewentualnych błędów i niezgodności. 10. Tworzenie dokumentacji analitycznej, technicznej, instrukcji użytkownika oraz raportów z przebiegu Projektu. Wymagania dotyczące dokumentacji projektowej Zamawiający opisał w OPZ, części "Zarządzanie Projektem" i "Dokumentacja". 11. Szkolenie użytkowników końcowych w zakresie konfiguracji, utrzymania, rozwoju i korzystania Platformy CMC. 12. Zapewnianie wsparcia technicznego Zamawiającemu podczas i po zakończeniu wdrożenia Platformy CMC. 13. Rozwiązywanie problemów technicznych, błędów oraz udzielanie porad, konsultacji i wsparcia użytkownikom w zakresie funkcjonalności Platformy CMC. 14. Regularne raportowanie postępu prac oraz ewentualnych problemów lub ryzyk związanych z Projektem. 15. Ocena efektywności procesu wdrożenia Platformy IP_CMC i identyfikacja obszarów do dalszej optymalizacji. 16. Aktywna współpraca z wszystkimi członkami zespołu projektowego i bieżąca komunikacja z zespołem projektowym oraz uczestnictwo w cyklicznych spotkaniach wskazanych przez Zamawiającego.
ZP.6	Do obowiązków Specjalistów ds. Integracji Wykonawcy będzie należało: 1. Współpraca z zespołem projektowym w celu zrozumienia pełnego zakresu integracji oraz określenia wymagań technicznych i biznesowych Zamawiającego. 2. Wdrażanie założeń integracji zgodnie z zaprojektowaną architekturą. 3. Określanie interfejsów i protokołów komunikacyjnych oraz modeli danych potrzebnych do przeprowadzenia skutecznej integracji. 4. Przeprowadzanie implementacji rozwiązań integracyjnych zgodnie z określonymi specyfikacjami i wymaganiami Zamawiającego. 5. Konfigurowanie narzędzi i platform integracyjnych, transformacji danych oraz dostosowanie integracji do reguł biznesowych. 6. Przeprowadzanie testów jednostkowych, integracyjnych i end-to-end w celu sprawdzenia poprawności działania integracji. 7. Identyfikacja i rozwiązywanie ewentualnych błędów oraz niezgodności w procesie integracji. 8. Optymalizacja wydajności i stabilności integracji poprzez identyfikację i usuwanie wąskich gardeł oraz implementację najlepszych praktyk. 9. Dostosowywanie integracji do zmieniających się potrzeb biznesowych i technologicznych Zamawiającego.

	10. Tworzenie dokumentacji technicznej dotyczącej procesu integracji, w tym opisów architektury, schematów danych i konfiguracji Platformy CMC. Wymagania dotyczące dokumentacji projektowej Zamawiający opisał w OPZ, części "Zarządzanie Projektem" i "Dokumentacja". 11. Dokumentowanie procesu testowania i wyników testów integracyjnych. 12. Szkolenie personelu Zamawiającego w zakresie korzystania z zintegrowanych systemów lub aplikacji Platformy CMC. 13. Zapewnienie wsparcia technicznego Zamawiającemu oraz udzielanie porad dotyczących integracji. 14. Regularne raportowanie postępu prac, w tym osiągnięć, problemów i ryzyk związanych z procesem integracji. 15. Przekazywanie informacji zwrotnych do zespołu projektowego w celu ciągłego doskonalenia procesów integracyjnych. 16. Identyfikacja i ocena potencjalnych ryzyk związanych z integracją systemów wraz z opracowywaniem strategii minimalizacji ryzyka oraz szybkiego reagowania w przypadku jego wystąpienia. 17. Aktywna współpraca z wszystkimi członkami zespołu projektowego i bieżąca komunikacja z zespołem projektowym oraz uczestnictwo w cyklicznych spotkaniach wskazanych przez Zamawiającego. 18. Dbanie o płynny przepływ informacji i współpracę w celu osiągnięcia celów projektu integracji.
ZP.7	Do obowiązków Programistów Wykonawcy będzie należało: 1. Odpowiedzialność za pisanie kodu zgodnie z wymaganiami Projektu. 2. Przeprowadzenie testów jednostkowych, integracyjnych i funkcjonalnych swojego kodu, aby zapewnić jego jakość i poprawność. Zakres wymagań dotyczących testów Zamawiający opisał w OPZ, części „Testy”. 3. Identyfikacje potencjalnych błędów w wytworzonym kodzie, analizę i naprawę. 4. Współpraca z zespołem programistów oraz pozostałymi członkami zespołu projektowego, na podstawie efektywnej komunikacji. Wspieranie i pomoc w rozwiązywaniu problemów. 5. Tworzenie dokumentacji technicznej, która opisuje działanie kodu, jego strukturę i wykorzystane technologie. Zakres wymagań dotyczących dokumentacji Zamawiający opisał w OPZ, części „Zarządzanie Projektem” oraz „Dokumentacja”. 6. Utrzymanie Platformy IP_CMC po wdrożeniu odpowiedzialność za jej utrzymanie, naprawa błędów, przeprowadzanie aktualizacji i dostosowywanie do zmieniających się wymagań lub środowiska. 7. Aktywna współpraca z wszystkimi członkami zespołu projektowego i bieżąca komunikacja z zespołem projektowym oraz uczestnictwo w cyklicznych spotkaniach wskazanych przez Zamawiającego.
ZP.8	Do obowiązków Testerów oprogramowania Wykonawcy będzie należało: 1. Zapoznanie się z dokumentacją projektową, specyfikacjami wymagań oraz wszelkimi innymi dokumentami związanymi z Projektem. 2. Opracowanie planu testów, który określi strategię testowania, zasoby, harmonogramy i metryki wydajności.

	3. Przeprowadzanie różnych rodzajów testów na podstawie przygotowanych scenariuszy testowych. Wymagania związane z przeprowadzeniem testów Zamawiający opisał w OPZ, części „Testy". 4. Dokumentowanie wyników testów w formie raportów, które zawierają informacje o wykrytych błędach, problemach wydajnościowych, zgodności z wymaganiami itp. Zakres wymagań dotyczących dokumentacji Zamawiający opisał w OPZ, części „Zarządzanie Projektem" oraz „Dokumentacja". 5. Współpraca z zespołem analitycznym i programistycznym w celu identyfikacji oraz rozwiązania problemów związanych z jakością Platformy CMC. 6. Udoskonalanie procesów testowych poprzez propozycje ulepszeń w procesach testowych i implementacja tych zmian w celu poprawy efektywności i skuteczności testowania. 7. Regularna komunikacja z innymi członkami zespołu projektowego w celu uzgodnienia priorytetów, wymagań i terminów. 8. W razie potrzeby szkolenie innych członków zespołu projektowego w zakresie testowania oprogramowania i narzędzi stosowanych w procesie. 9. Dbałość o to, aby produkt spełniał ustalone standardy jakościowe oraz zgodność z wymaganiami klienta Zamawiającego. 10. Automatyzacja testów w ramach procesów CI/CD/CD oraz wymogów i zasad opisanych w karcie Testy (od T1 do T.32). 11. Koordynacja scenariuszy, zadań testowych, nadzór nad postępem testowania oraz dostarczanie regularnych aktualizacji dotyczących statusu testów. Aktywna współpraca z wszystkimi członkami zespołu projektowego i bieżąca komunikacja z zespołem projektowym oraz uczestnictwo w cyklicznych spotkaniach wskazanych przez Zamawiającego.
ZP.9	Zespół wdrożeniowy Wykonawcy będzie pracował z wykorzystaniem metodyki Agile i podejścia iteracyjnego, do realizacji Projektu.
ZP.10	Wykonawca będzie rozpisywał zadania w ramach realizowanych prac projektowych w systemie Zamawiającego służącego do bieżącego monitorowania i raportowania prac, np. JIRA. Zamawiający dopuszcza integrację wspomnianego systemu z systemem Wykonawcy.
ZP.11	Wykonawca wskaże osobę po swojej stronie pełniącą rolę doradczą na spotkaniach Komitetu Sterującego Zamawiającego.

8. Wymagania w zakresie testów

Proces testowania winien zawierać następujące kroki:

1. Planowanie testów – ustalenie zakresu, celów, scenariuszy testowych i wyznaczenie kryteriów akceptacji.
2. Monitorowanie testów i nadzór nad testami – proces śledzenia postępu testów i wykrywania problemów.
3. Projektowanie testów – opracowanie przypadków testowych oraz scenariuszy testowych.
4. Wykonanie testów – przeprowadzenie testów zgodnie z planem testowym.
5. Analiza wyników testów - ocena wyników testów i ewentualne korekty w oprogramowaniu
6. Raportowanie – przygotowanie raportów z testów i ich wyników

MODYFIKACJA 23.07.2024 **Załącznik 3 do SWZ**

W ramach realizacji zakresu testów Wykonawca zobowiązany jest do spełnienia poniższych wymagań:

Nr	Punkt kontrolny
T.1	Wykonawca zapewni przeprowadzenie następujących typów testów: 1. Testy fukcjonalne 2. Testy akceptacyjne 3. Testy integracyjne 4. Testy jakościowe 5. Testy jednostkowe 6. Testy regresji 7. Testy separacji 8. Testy migracji
T.2	Wykonawca musi zapewnić środowisko dewelopersko – testowe, odpowiadające konfiguracyjnie środowisku produkcyjnemu Zamawiającego.
T.3	W ramach realizacji przedmiotu umowy Wykonawca zobowiązany jest przeprowadzić w obecności i pod nadzorem Zamawiającego zestaw czynności potwierdzających poprawność działania Platformy IP_CMC w ramach Procedury Odbioru. W skład Procedury Odbioru wchodzą minimalnie następujące kroki: 1. Testy fukcjonalne 2. Testy akceptacyjne 3. Testy integracyjne 4. Testy jakościowe 5. Testy jednostkowe 6. Testy regresji 7. Testy separacji 8. Testy migracji 9. Zebranie akceptacji wszystkich interesariuszy projektu.
T.4	Dokumentacja testowa - dla każdego z typów testów - musi zostać opracowana przez Wykonawcę i musi być zatwierdzona przez Zamawiającego i muszą obejmować następujące rodzaje dokumentów: 1. Strategie testowania, 2. Plan testów, 3. Scenariusze testowe, 4. Przypadki testowe, 5. Kryteria akceptacji, 6. Dane do testów.
T.5	Plan i scenariusze muszą być zgodne z powszechnie stosowanymi zasadami i praktykami dla danego typu testów i musza zostać zatwierdzone przez Zamawiającego, w tym również zestawy danych używanych do wykonania testów.
T.6	Plan testów musi określać w szczególności: 1. Ogólne zasady przeprowadzania testów, 2. Opis środowiska testowego, 3. Kolejność wykonywania scenariuszy testowych, 4. Klasyfikację wykrytych problemów testowych,

	5. Kryteria sukcesu dla poszczególnych kategorii testów.
T.7	Scenariusze muszą zapewniać pokrycie wszystkich procesów kluczowych dla działalności Zamawiającego w zakresie dostarczanych modułów. Każdy scenariusz musi określać: 1. Dane, które muszą być wprowadzone do systemu przed uruchomieniem scenariusza, 2. Kolejność czynności, wykonywanych w czasie testu oraz dane wprowadzane do systemu w czasie testu, 3. Oczekiwaną reakcję systemu na wykonane czynności i wprowadzone dane.
T.8	Przypadki testowe i dane testowe, w tym wszelkie materiały eksploatacyjne, dostarczone muszą być przez Wykonawcę i zaakceptowane przez Zamawiającego. Zamawiający zobowiązany jest do współpracy z Wykonawcą przy przygotowywaniu scenariuszy testowych i danych testowych, przeprowadzaniu testów oraz przygotowaniu wyników testów.
T.9	Testy powinny być zautomatyzowane w co najmniej 90% zgodnie z dobrymi praktykami MLOps i DevSecOps.
T.10	Testy muszą zostać przeprowadzone w terminie przewidzianym w harmonogramie, zgodnie z zaakceptowanym planem testów.
T.11	Testy muszą zostać wykonane z użyciem środowiska testowego, chyba że plan testów będzie przewidywał inaczej, na bazie reprezentatywnej próbki danych eksploatacyjnych. Zakres testów nie może wykraczać poza merytoryczny zakres projektu.
T.12	Wynik testu dla Scenariusza Testowego będzie uznany za pozytywny, gdy wyniki testów dla wszystkich Przypadków Testowych zawartych w Scenariuszu Testowym są pozytywne. Wynik testu dla Scenariusza Testowego uzna się za negatywny, gdy wynik testu dla któregokolwiek Przypadku Testowego zawartego w Scenariuszu testowym jest negatywny.
T.13	Wynik testu dla Przypadku Testowego uzna się za pozytywny, gdy opis oczekiwanego rezultatu jest „zgodny” z faktycznie uzyskanym wynikiem po zakończeniu Przypadku Testowego.
T.14	Wynik testu dla Przypadku Testowego uzna się za negatywny, gdy opis oczekiwanego rezultatu jest „niezgodny” z faktycznie uzyskanym wynikiem po zakończeniu Przypadku Testowego. W przypadku, gdy występująca niezgodność jest wynikiem błędnie opisanego Przypadku Testowego, wówczas wynik testu może być uznany za prawidłowy, a błędny opis Przypadku Testowego musi zostać poprawiony przez Wykonawcę. Sytuacja taka musi znaleźć odzwierciedlenie w raporcie z Testów Akceptacyjnych.
T.15	Zamawiający zastrzega sobie prawo do przeprowadzenia Testów Akceptacyjnych dowolnymi wybranymi przez siebie metodami.
T.16	Testy muszą być wykonane na podstawie Scenariuszy Testowych zaakceptowanych przez Zamawiającego.
T.17	Testy Zamawiający uzna za zakończone z sukcesem, gdy zostaną przeprowadzone testy z wykorzystaniem zaplanowanych Scenariuszy Testowych oraz: 1. brak będzie niezakończonych Scenariuszy Testowych z powodu wystąpienia błędów blokujących, 2. brak będzie niezakończonych Scenariuszy Testowych z powodu wystąpienia błędów nieblokujących, których liczba wykracza poza dopuszczalny limit 5 błędów.

T.18	W przypadku wystąpienia Incydentu, który uniemożliwia wykonanie wszystkich zaplanowanych przypadków Testowych i/lub Scenariuszy Testowych, a który nie wynika z winy Wykonawcy, wówczas Zamawiający dopuszcza, aby zakres testów został zmieniony (wyłączenie przypadków i/lub scenariuszy) na podstawie decyzji podjętej przez Zamawiającego.
T.19	W przypadku zakończenia Testów z wynikiem negatywnym, musi zostać ustalony plan powtórzenia testów. Wybór scenariuszy do II tury testów musi zostać przeprowadzony według następujących zasad: 1. Scenariusze Testowe, które otrzymały wynik negatywny z powodu wystąpienie błędów, 2. Scenariusze Testowe dla funkcjonalności powiązanych z funkcjonalnością Scenariusza Testowego, w którym wystąpiły błędy.
T.20	Zamawiający zastrzega sobie prawo przeprowadzenia testów regresji dla scenariuszy z wynikiem pozytywnym.
T.21	Raport z testów musi wykazywać, że dostarczone oprogramowanie współpracuje z systemami, modułami, aplikacjami, które Wykonawca wykorzystał do zbudowania Platformy CMC.
T.22	Wykonawca dopuszcza, że Zamawiający przeprowadzi audytu bezpieczeństwa, konfiguracji platformy, uprawnień, kodu źródłowego przez wskazaną przez Zamawiającego zewnętrzną firmę audytorską. Koszt tego audytu pokrywa Zamawiający.
T.23	Platforma IP_CMC musi przejść kryteria testów wydajnościowych na podstawie poniższych wymagań zamawiającego: 1. Skalowalność: Sprawdzenie przez Wydajność Aplikacji, jak aplikacja dostosowuje się do dynamicznego zwiększania lub zmniejszania obciążenia. 2. Wydajność pod obciążeniem: Testowanie aplikacji pod dużym obciążeniem, w tym testy obciążeniowe, stresowe i wytrzymałościowe. 3. Czas odpowiedzi: Pomiar czasu odpowiedzi aplikacji dla różnych scenariuszy użytkowania. 4. Przepustowość: Określenie maksymalnej liczby żądań, jaką aplikacja może obsłużyć na jednostkę czasu. 5. Zasoby: Raportowanie zużycia zasobów, takich jak CPU, pamięć RAM i dysk. 6. Stabilność: Ocena czy aplikacja działa bez awarii przez dłuższy okres czasu. 7. Testy obciążeniowe w dłuższym okresie: Wykonanie testów wydajnościowych przez bez awarii i incydentów przez dłuższy okres czasu. 8. Testy wpływu skalowania na wydajność: Testowanie automatycznego skalowania aplikacji. 9. Testy wpływu migracji na wydajność: Przetestowanie wydajności aplikacji po migracji do chmury, nowej lokalizacji środowiska obliczeniowego (np. innej chmury obliczeniowej, nowego regionu). 10. Wykonawca przygotuje odpowiednie zestawy danych do testów.
T.24	Platforma IP_CMC musi przejść kryteria testów separacji na podstawie poniższych wymagań zamawiającego: 1. Potwierdzenie, że różne sieci zgodnie z przyjętą i zatwierdzoną architekturą infrastrukturalną są poprawnie oddzielone, aby zapewnić bezpieczeństwo i prywatność.

	2. Potwierdzenie, że urządzenia sieciowe są skonfigurowane zgodnie z przyjętą i zatwierdzoną architekturą infrastrukturalną. 3. Wykonanie podstawowych testów penetracyjnych polegających na weryfikacji istnienia separacji sieci w oparciu o scenariusze testowe. 4. Wykonawca przygotuje odpowiednie zestawy danych do testów.
T.25	Platforma IP_CMC musi przejść kryteria testów migracji na podstawie poniższych wymagań zamawiającego: 1. Potwierdzenie, że usługi Platformy IP_CMC mogą być poprawnie przeniesione z jednej podsieci do drugiej. Kryterium sukcesu będzie przeniesienie usług z jednej sieci do drugiej bez utraty danych i z pełną dostępnością funkcjonalności usług w nowej podsieci. 2. Testy przeniesienia środowiska Platformy IP_CMC na inne chmury obliczeniowe: sprawdzenie możliwości przeniesienia i uruchomienia na innych platformach obliczeniowych przy minimalnym zaangażowaniu developmentu (zmian w oprogramowaniu). 3. Wykonawca przygotuje odpowiednie zestawy danych do testów uwzględniając: a) testowanie nowego systemu (dane uzyskane z różnych źródeł), b) testowanie migracji (dane przesyłane z systemów źródłowych do hurtowni danych), c) testowanie zmian (nowe dane dodawane do hurtowni danych) d) testowanie raportów (walidacja danych, dokonywania obliczeń)
T.26	Dostawca przetestuje samodzielnie i udokumentuje te testy dla każdego z komponentów przed wysyłką, aby upewnić się, że są kompletne i gotowe do użycia przez Zamawiającego.
T.27	Platforma IP_CMC musi przejść kryteria testów funkcjonalnych na podstawie poniższych wymagań zamawiającego: 1. Potwierdzenie, że wszelkie wymagania postawione przed systemem na etapie zamówienia oraz analizy i budowy rozwiązania zostały spełnione na odpowiednio wysokim poziomie jakości. 2. Otrzymanie potwierdzenia ze strony użytkowników końcowych, a także analityków biznesowych/systemowych i testerów, że system funkcjonuje poprawnie. 3. Potwierdzenie możliwości użycia oprogramowania do realizacji celu, do którego zostało stworzone. Testy muszą pokrywać komplet wymagań funkcjonalnych określonych w OPZ w szczególności muszą zawierać wszystkie przypadki użycia dla aplikacji określone na etapie analizy przedwdrożeniowej zarówno w zakresie ścieżek pozytywnych jak i negatywnych scenariusza. 4. Wykonawca przedstawi odpowiednie Logi potwierdzające wykonanie testów funkcjonalnych, na podstawie scenariuszy testowych i przygotowanego zestawu danych testowych, oraz ich statusy (w szczególności zrzuty ekranu w przypadku zgłoszenia defektów). 5. Wykonawca przygotuje odpowiednie zestawy danych do testów.
T.28	Platforma IP_CMC musi przejść kryteria testów bezpieczeństwa na podstawie poniższych wymagań zamawiającego: 1. Wykonawca wykona zaawansowane testy bezpieczeństwa pod kątem przedstawienia rzeczywistego obrazu bezpieczeństwa aplikacji za pomocą przyjętych na rynku narzędzi do skanowania, penetracji i oceny dziur bezpieczeństwa.

	2. Wykonawca wykona kontrolowane próby ataku, które pozwolą Zamawiającemu na ocenę bezpieczeństwa aplikacji poprzez symulację ataku prawdziwego włamywacza komputerowego lub złośliwego użytkownika sieci. 3. Testy zostaną wykonane na kopii realnego środowiska np. w środowisku zwirtualizowanym tak, aby sprawdzić realne, a nie potencjalne zagrożenia zabezpieczenia. 4. Testy dotyczyć będą komponentów aplikacyjnych, usług Platformy IP_CMC oraz systemów zabezpieczeń chroniących dostęp do aplikacji i same środowisko chmurowe. 5. Testy zakończą się analizą sposobu działania systemu (aplikacji) pod kątem bezpieczeństwa informacji przekazywanych i przetwarzanych przez Platformę IP_CMC. 6. Wykonawca zapewni m. in. analizę zarządzania sesjami autoryzowanych użytkowników, analizę informacji zapisywanych po stronie użytkownika, np. w obiektach „cookie", sprawdzenie odporności na ataki typu XSS (Cross-Site Scripting), sprawdzenie odporności na ataki typu XSRF (Cross-Site RequestForgery), weryfikacja znanych podatności – exploity.
T.29	Platforma IP_CMC musi przejść kryteria testów integracji na podstawie poniższych wymagań zamawiającego: 1. Wykrywanie defektów i problemów w interfejsach i interakcjach pomiędzy systemami. 2. Wykonawca wykona testy styków integracyjnych oraz wykona walidację danych znajdujących się w źródle i odbiorniku. 3. Testy musza objąć sprawdzenie zintegrowanego rozwiązania z perspektywy użytkownika systemu pod kątem nowych funkcjonalności wprowadzanych przez zmiany planowane i łaty naprawcze. 4. Scenariusze testowe mogą opierać się na zaślepkach i symulatorach. 5. Wykonawca przygotuje odpowiednie zestawy danych do testów.
T.30	Platforma IP_CMC musi przejść kryteria testów jednostkowe (ang. unit test) na podstawie poniższych wymagań zamawiającego: 1. Testy jednostkowe będą przeprowadzane przez Wykonawcę już w trakcie pracy nad kodem aplikacji. 2. Testy będą weryfikowały poprawność działania pojedynczych elementów (modułów) platformy. 3. Kod źródłowy będący przedmiotem testów jednostkowych musi być możliwy do skompilowania i wdrożenia (ang. deployment) po pozytywnym zatwierdzeniu każdego z testów jednostkowych. 4. Wykonawca przygotuje na bieżąco raport pokrycia kodu testami jednostkowymi, aby umożliwić szybkie potwierdzanie możliwości kompilowania i włączania kodu w gałąź kodu danego wydania. 5. Wykonawca przygotuje odpowiednie zestawy danych do testów.
T.31	Platforma IP_CMC musi przejść kryteria testów regresji na podstawie poniższych wymagań zamawiającego: 1. Sprawdzenie poprawności działania niezmienionych części oprogramowania i sprawdzenie, czy system nie uległ degradacji (regresji) po wprowadzeniu zmian planowanych i łat naprawczych.

	2. Przeprowadzenie analizy wpływu zmian w systemach na istniejące funkcjonalności biznesowe, które nie były modyfikowane w ramach wdrożeń. 3. Wskazanie priorytetów biznesowych dla testowanych procesów oraz ryzyka techniczne i biznesowe systemów/komponentów, w których te procesy są realizowane. 4. Wykonawca przygotuje odpowiednie zestawy danych do testów.
T.32	Gotowość każdego Laboratorium Wirtualnego zostanie potwierdzona min. poprzez test następujących funkcjonalności: 1. selekcja pacjentów spełniających określone kryteria np.: diagnozy, wyniki badań, proces leczenia oraz udostępnienie danych dot. procedur, obserwacji, diagnoz, leczenia, wyników badań dla wyselekcjonowanej grupy. 2. selekcja danych obrazowych pacjentów spełniających określone kryteria 3. przeprowadzenie procesu przetwarzania wyselekcjonowanych danych i obrazów w oparciu o dostępny na platformie wybrany pakiet narzędzi Data Science Testy będą również zawierały sprawdzenie możliwości uruchomienia narzędzi do Data Science: python, język R, MatLab, Statistica oraz uzgodnionych z Zamawiającym: min. 1 narzędzia do ML oraz min. 1 narzędzia do budowy modeli statycznych.

10. Wymagania w zakresie DevOps i automatyzacji

Wykonawca w ramach realizacji przedmiotu zamówienia zobowiązany jest to zastosowania metody zarządzania procesami deweloperskimi zgodnymi z podejściem DevOps lub DevSecOps, które promuje kulturę ciągłej i zintegrowanej współpracy pomiędzy zespołami odpowiedzialnymi za rozwój i utrzymanie oprogramowania. Zamawiający wymaga wyodrębnienia procesów, które będą podlegać automatyzacji w obszarze rozwoju oprogramowania platform (wytwarzania, testowania, wdrażania) oraz utrzymania. Automatyzacji należy poddać rutynowe zadania w ramach tych wyodrębnionych procesów.

W ramach realizacji zakresu DevOps lub DevSecOps Wykonawca zobowiązany jest do spełnienia poniższych wymagań:

Nr	Punkt kontrolny
DEV.1	Platforma IP_CMC umożliwia automatyczne wdrażanie aplikacji na różnych środowiskach (np. testowe, produkcyjne) bez konieczności ręcznej interwencji.
DEV.2	Platforma IP_CMC umożliwia definiowanie infrastruktury jako kod (ang. Infrastructure as Code, IaC), np. przy użyciu formatu YAML lub JSON oraz narzędzi klasy IaC, np. Terraform lub Ansible.
DEV.3	Platforma IP_CMC umożliwia dynamiczne dostosowywanie zasobów w zależności od obciążenia (elastyczność i skalowalność dynamiczną). Wymagane jest automatyczne skalowanie aplikacji w odpowiedzi na wzrost lub spadek ruchu.
DEV.4	Platforma IP_CMC jest zgodna z koncepcją DevOps lub DevSecOps: 1. współpracuje z popularnymi narzędziami DevOps, np. Jenkins, GitLab CI/CD, CircleCI lub równoważnymi, 2. umożliwia integrację kodu, budowanie, testowanie, wdrażanie i dostarczanie oprogramowania, 3. wspiera integrację z repozytoriami kodu, 4. umożliwia automatyczne wdrażanie i monitorowanie postępów wdrożenia.

DEV.5	Przyjęte odejście do DevOps lub DevSecOps w trakcie prac nad Platformą IP_CMC wprowadza zabezpieczenia w całym cyklu życia tworzenia oprogramowania w celu zminimalizowania liczby luk w kodzie.
DEV.6	Platforma IP_CMC umożliwia monitorowanie postępów wdrożenia oraz przegląd zdarzeń i metryk wymaganych dla efektywnego prowadzenia procesów DevOps lub DevSecOps. Na bieżąco są dostępne raporty o dostępności, wydajności i błędach.
DEV.7	Platforma IP_CMC oferuje automatyczne tworzenie kopii zapasowych danych oraz możliwość odtwarzania w razie awarii lub śledztwa dot. problemów (ang. investigation). Polityka backupu danych i retencji przechowywanych danych jest dopasowana do potrzeb Zamawiającego i jego środowisk wspieranych procesami DevOps lub DevSecOps.
DEV.8	Platforma IP_CMC powinna umożliwiać integrację z narzędziami do testowania automatycznego, takimi jak Selenium czy JUnit. Wykonawca zaproponuje efektywne narzędzia do testowania automatycznego dopasowane do charakteru Platformy CMC.
DEV.9	Wykonawca dostarczy wszystkie paczki instalacyjne, kontenery i pliki konfiguracyjne umożliwiające stworzenie i odtworzenie infrastruktury w platformie chmurowej od początku (ang. from the scratch).
DEV.10	Wymagane jest przygotowanie przez Wykonawcę automatyzacji wykonywania testów w procesie wdrażania wraz z odpowiednimi narzędziami, politykami i scenariuszami.
DEV.11	Wykonawca zapewni usługę typu autoscaling.
DEV.12	Wykonawca zbuduje pipeline MLOps dla modeli służących anonimizacji i ekstrakcji.
DEV.13	Wykonawca użyje w pipeline CI/CD narzędzia do badania jakości kodu i jego podatności.
DEV.14	Dostawca zautomatyzuje procesy wytwarzania oprogramowania w uzgodnieniu z Zamawiającym. Automatyzacja dotyczyć ma obszaru CI/CD/CT/CD.

11. Zasady gwarancji

Wykonawca musi zapewnić - dla Platformy IP_CMC - świadczenie usług gwarancyjnych, przez okres nie krótszy niż okres określony w Umowie.

Zamawiający wymaga, aby Wykonawca posiadał aplikację internetową do przyjmowania i obsługi zgłoszeń, będącej podstawą komunikacji między Zamawiającym i Wykonawcą w zakresie zgłoszeń gwarancyjnych. Aplikacja musi posiadać możliwość wysyłania powiadomień na temat zgłoszeń gwarancyjnych na podany adres e-mail oraz musi posiadać możliwość generowania raportów związanych ze zgłoszeniami gwarancyjnymi.

Wykonawca podejmie odpowiednie działania związane z realizacją gwarancji w określonym czasie, tj. reakcję na zgłoszenie Incydentu w czasie nie dłuższym niż oczekiwany czas reakcji oraz podejmie się naprawy oraz usunięcia skutków Awarii w czasie oczekiwanej naprawy. Czasy mogą być różne w zależności od typu Błędu:

1) Błędu krytycznego: czas reakcji to 4 Godziny Robocze, z tym, że maksymalny czas naprawy dla tego typu zgłoszenia to 16 Godzin Roboczych.
2) Błędu niekrytycznego: czas reakcji to 8 Godzin Roboczych, z tym, że maksymalny czas naprawy wynosi 24 Godzin Roboczych.

MODYFIKACJA 23.07.2024 **Załącznik 3 do SWZ**

Powyższe czasy liczone są zawsze od momentu zgłoszenia Incydentu przez Zamawiającego w Dniach Roboczych i Godzinach Roboczych.

Zamawiający dopuszcza rozwiązanie Błędu krytycznego lub niekrytycznego przez zastosowanie rozwiązania tymczasowego (tzw. obejście). Rozwiązanie tymczasowe musi zostać uruchomione we wskazanym maksymalnym czasie naprawy dla poszczególnych kategorii błędów. Jednocześnie rozwiązanie tymczasowe musi zostać usunięte i zastąpione rozwiązaniem docelowym nie później niż 20 Dni Roboczych od daty zgłoszenia Incydentu.

W ramach rozwiązania Incydentu Wykonawca usuwa skutki tego Incydentu m.in. naprawia struktury danych, same dane, instalację i konfigurację oprogramowania oraz komponentów Platformy IP_CMC w ramach Gwarancji.

Zamawiający określa dodatkowo następujące wymagania obligatoryjne:

Nr	Punkt kontrolny
GW.1	Platforma technologicznie powinna być tak przygotowana, aby zapewniać SLA na wszystkie swoje usługi (łącznie z pojedynczą instancją maszyny wirtualnej) na poziomie minimum 99%.
GW.2	Wykonawca zobowiązuje się do udzielania Zamawiającemu wszelkiego typu konsultacji i porad w zakresie zagadnień związanych z funkcjonowaniem Platformy CMC, w ramach okresu Gwarancji.
GW.3	Zamawiający wymaga, aby Wykonawca posiadał aplikację internetową do przyjmowania i obsługi zgłoszeń, będącej podstawą komunikacji między Zamawiającym i Wykonawcą w zakresie zgłoszeń. Aplikacja musi posiadać możliwość wysyłania powiadomień na temat zgłoszeń na podany adres e-mail oraz musi posiadać możliwość generowania raportów związanych ze zgłoszeniami.
GW.4	Zamawiający wymaga, aby Wykonawca przyjmował zgłoszenia w Godzinach Roboczych.
GW.10	Wymagany zakres usług gwarancyjnych w zakresie wdrożonych modułów oprogramowania/systemu, to: 1. Gotowość Wykonawcy do usuwania błędów wdrożonego oprogramowania. 2. Wprowadzanie zmian w oprogramowaniu w zakresie dotyczącym istniejących funkcjonalności, objętych umową, w zakresie wymaganym zmianami powszechnie obowiązujących przepisów prawa lub przepisów prawa wewnętrznie obowiązujących Zamawiającego, wydanych na podstawie delegacji ustawowej, z wyłączeniem oprogramowania standardowego. 3. Zagwarantowanie prowadzenia rejestru zgłaszanych przez użytkowników błędów wdrożonego oprogramowania. 4. Wprowadzanie w trybie pilnym do oprogramowania zmian i poprawek usuwających stwierdzone błędy i luki we wbudowanych mechanizmach i funkcjach zabezpieczeń. 5. Gotowość do odpłatnego wykonania na zlecenie Zamawiającego zaproponowanych przez niego modyfikacji we wdrożonym oprogramowaniu. 6. Dokonanie wspólnie z Zamawiającym przeglądu na koniec okresu Gwarancji i usunięcie stwierdzonych w czasie przeglądu niezgodności na koszt Wykonawcy.
GW.11	Wykonawca w czasie gwarancji musi przekazywać bezpłatnie Zamawiającemu nowe wersje systemu. W szczególności, jeżeli będzie to związane z podniesieniem jakości i funkcjonalności oprogramowania lub usunięciem wykrytych przez Wykonawcę błędów w

	działaniu oprogramowania i/lub podnoszące bezpieczeństwo komponentów Platformy CMC.
GW.12	W okresie gwarancji Wykonawca w ramach realizacji przedmiotu umowy zapewni dodatkowe godziny konsultacyjne/wdrożeniowe/programistyczne, do wykorzystania przez Zamawiającego na realizację zagadnień, które mogą wyniknąć w trakcie eksploatacji systemu. Wykorzystanie godzin pozostaje w wyłącznej dyspozycji Zamawiającego.
GW.13	Zgłaszanie Incydentów (awarii, usterek lub błędów) przez Zamawiającego może następować w jednej z niżej wymienionych form: 1. Pierwszorzędnie przez dedykowany system zgłoszeń Zamawiającego zintegrowany z systemem zgłoszeń Wykonawcy; 2. Telefonicznie w sytuacjach nagłych.
GW.14	W ramach Gwarancji Wykonawca zobowiązany będzie do bieżącego monitorowania zmian w przepisach powszechnie obowiązującego prawa pod kątem konieczności wprowadzenia zmian w Platformie CMC, a następnie ich wdrażania u Zamawiającego na swój koszt.
GW.15	Wykonawca musi zapewnia świadczenie usług gwarancyjnych, przez okres zaoferowany przez Wykonawcę w ofercie, jednak nie krótszy niż ten określony w umowie.
GW.16	Zlecenie i realizacja prac w ramach Gwarancji będzie realizowane w następującym trybie: 1. Strony ustalają sposób wykonania prac gwarancyjnych 2. Przed przystąpieniem do wykonania prac przez Wykonawcę, Strony uzgodnią wstępnie zakres prac tj. termin wykonania 3. Zamawiający każdorazowo będzie zgłaszać Wykonawcy potrzebę wykonania prac w formie pisemnej lub mailowej. 4. Wykonawca wykona prace w uzgodnionym terminie. 5. Wykonawca przystąpi do wykonania prac zgodnie z zakresem określonym w zleceniu, po jego przyjęciu. W przypadku odmowy przyjęcia zlecenia, Wykonawca prześle Zamawiającemu pisemne lub mailowe uzasadnienie odmowy ze wskazaniem rozbieżności pomiędzy zleceniem a wcześniejszymi ustaleniami. 6. Po wykonaniu prac Wykonawca przeprowadzi testy sprawdzające poprawność działania Platformy. 7. Potwierdzeniem wykonania prac będzie pisemne lub mailowe potwierdzenie realizacji przez uprawnionego pracownika Zamawiającego.

W przypadku braku realizacji przez Wykonawcę powyższych wymagań, związanych z obsługą gwarancyjną, Zamawiający może zastosować kary umowne określone w umowie.

12. Zasady asysty technicznej

W ramach realizacji przedmiotu zamówienia, po wykonanym wdrożeniu Platformy IP_CMC i jej odbiorze, odpowiedzialność za administrację Platformą IP_CMC przechodzi na GUMed dlatego też wymagane jest, aby Wykonawca zapewnił odpowiednią Asystę Techniczną spełniająca poniższe wymagania:

MODYFIKACJA 23.07.2024 **Załącznik 3 do SWZ**

Nr	Punkt kontrolny
AT.1	Wykonawca w ramach Asysty Technicznej zapewnia Zamawiającemu usługi konsultacyjne i porad w obszarze związanym z funkcjonowaniem platformy w zakresie/a w szczególności: 1. Informowanie w trybie pilnym do oprogramowania zmian i poprawek usuwających stwierdzone błędy i luki we wbudowanych mechanizmach i funkcjach zabezpieczeń. 2. Bezpośrednio odpowiadać na pytania dotyczące wydajności, funkcjonalności lub działania obsługiwanych programów. 3. Bezpośrednio odpowiadać na pytania dotyczące problemów z obsługiwanym Oprogramowaniem. 4. Wpierać w diagnozowaniu problemów w działaniu Oprogramowania. 5. Wspierać w rozwiązywaniu problemów w działaniu Oprogramowania. 6. Wspierać w zakresie wsparcia technicznego dotyczącego administrowania, konfiguracji, testowania czy odtwarzania Platformy IP_CMC. 7. Wspierać w zakresie projektowania i tworzenia nowych funkcjonalności Platformy IP_CMC. 8. Udzielać informacji w zakresie budowy i konfiguracji Platformy IP_CMC oraz chmury obliczeniowej. 9. Dawać rekomendacje dotyczące koniecznych zmian w zakresie dopasowania platformy do pojawiających się zmian prawnych.
AT.2	Wykonawca musi zapewniać świadczenie usług Asysty Technicznej, przez okres wskazany w Umowie.
AT.3	Zamawiający wymaga, aby Wykonawca posiadał aplikację internetową do przyjmowania i obsługi zgłoszeń, będącej podstawą komunikacji między Zamawiającym i Wykonawcą w zakresie zgłoszeń Asysty Technicznej. Aplikacja musi posiadać możliwość wysyłania powiadomień na temat zgłoszeń na podany adres e-mail oraz musi posiadać możliwość generowania raportów związanych ze zgłoszeniami.
AT.4	Zamawiający wymaga, aby Wykonawca świadczył usługi Asysty Technicznej minimalnie w Dni Robocze w Godzinach Roboczych.
AT.5	Wykonawca zapewni świadczenie usług Asysty Technicznej w miejscu użytkowania Platformy IP_CMC lub świadczenia usług Platformy IP_CMC. W szczególności Asysta Techniczna może być świadczona zdalnie, chyba że Zamawiający postanowi inaczej.
AT.6	Zgłaszanie zapotrzebowania na Asystę Techniczną przez Zamawiającego może następować w jednej z niżej wymienionych form: 1. Pierwszorzędnie przez dedykowany system zgłoszeń Zamawiającego zintegrowany z systemem zgłoszeń Wykonawcy; 2. Telefonicznie w sytuacjach nagłych.
AT. 7	W ramach Asysty Technicznej Wykonawca będzie dostarczał chmurę oraz dostarczał na bieżąco wymagane licencje na oprogramowanie lub usługi SaaS, co oznacza, że będzie ponosił również koszty cyklicznych opłat: 1. za licencje lub za usługi SaaS wymagane dla działania i utrzymania Platformy IP_CMC, 2. za usługi wymagane dla działania i utrzymania Platformy IP_CMC w chmurze obliczeniowej.

	Jednocześnie opłaty cykliczne będą prezentowane na dokumentach księgowych osobno, tj. na jednym dokumencie księgowym za dany okres zostaną wskazane rozdzielnie pozycje dotyczące: opłat subskrypcyjnych za chmurę, opłat za licencje oraz opłat za usługi SaaS.
AT.8	Obsługa zadań określonych w wymaganiu AT.1 musi być dostarczona w trybie ciągłym jednak dopuszczalne, jest za zgodą Zamawiającego, ustalenie, po odbiorze platformy IP_CMC, ograniczonego trybu udzielania usług konsultacyjnych i porad dopasowanego do bieżących wymagań Zamawiającego.

W przypadku braku realizacji przez Wykonawcę powyższych wymagań związanych z Asysty Technicznej, Zamawiający zastosuje kary umowne opisane w Umowie.

13. Wymagania w zakresie dokumentacji dla Platformy

Do realizowanego przedmiotu zamówienia Wykonawca dostarczy dokumentację pogrupowaną tematycznie i zawierającą spis oraz charakterystykę wszystkich składników dokumentacji.

13.1. Wymagania ogólne dot. dokumentacji

Dokumentacja Platformy IP_CMC powinna być dostarczona:

1. W postaci papierowej, jeśli taka potrzeba zostanie wskazana przez Zamawiającego, w formie spiętych, zszytych lub zbindowanych egzemplarzy,
2. W postaci elektronicznej – w formie plików w formacie PDF lub innego powszechnie dostępnego formatu dokumentów elektronicznych (MS Office, HTML itp.);
3. Każdy egzemplarz oprócz tytułu powinien posiadać oznaczenie wersji identycznej jak aktualna wersja aplikacji, którą opisuje (wraz z datą produkcji lub dostawy);
4. Suplementy do dokumentacji muszą być spisane w odrębnej liście (numer suplementu oraz datę wydania i wersję aplikacji).

Spis dokumentów zewnętrznych.

5. Jeżeli w dokumentacji występuje odwołanie do innych źródeł wymagany jest spis wszystkich użytych dokumentów zewnętrznych i miejsce publikowania;
6. Procedury nie mogą zawierać sformułowań typu „zgodnie ze standardową procedurą ...”;
7. W przypadku odniesień do zewnętrznej dokumentacji, zewnętrzna dokumentacja musi zostać dołączona lub zostać bardzo precyzyjnie wskazana (dostarczona w postaci trwałej kopii w przypadku dostępu do zasobów internetowych), a odwołanie musi wskazywać na konkretną stronę/fragment dokumentacji zewnętrznej;
8. W przypadku, jeśli procedura wymaga wykonywania specjalizowanych skryptów instalacyjnych (np. własne skrypty dostawcy systemu IT), skrypty muszą zostać dołączone do dokumentacji.

Aktualizacja dokumentacji:

9. Aktualizacja dokumentacji nie może być opóźniona w stosunku do odbieranego zakresu w ramach Faz.

Zasady licencjonowania i dot. praw autorskich:

10. Wykonawca przenosi na Zamawiającego pełne prawa autorskie do Dokumentacji na zasadach określonych w Umowie.

Polityka rozwoju Dokumentacji:

11. Wykonawca powinien zdefiniować swoją politykę w zakresie cyklicznego aktualizowania Dokumentacji w ramach realizacji Umowy.

13.2. Dokumentacja użytkowa

Zamawiający planuje po okresie Gwarancji samodzielnie administrować i utrzymywać Platformę IP_CMC. Wymaga to pozyskania od Wykonawcy odpowiedniej wiedzy i dokumentacji. W związku z tym Wykonawca przygotuje dokumentację użytkową, którą minimalnie składać się będzie z:

1. Przewodnika dla użytkownika.
2. Instrukcji dla administratora i służb technicznych, w tym instrukcja instalacji i konfiguracji.
3. Opisu sprzęgu, w tym integracji synchronicznych i asynchronicznych.
4. Opisu Konfiguracji.
5. Dokumentacji powdrożeniowej.

Szczegółowe wymagania dotyczące poszczególnych dokumentów zostały wskazane w następujących wymaganiach Zamawiającego:

Nr	Punkt kontrolny
DOK.1	Dostawca dostarczy instrukcję instalacji Platformy IP_CMC zawierającą opis jak zainstalować oprogramowanie lub skonfigurować komponenty Platformy IP_CMC na chmurze obliczeniowej.
DOK.2	Dostawca dostarczy przewodnik użytkownika, który zawiera opis jak korzystać z dostarczonego rozwiązania IP_CMC mogą operatorzy Platformy IP_CMC oraz członkowie Laboratoriów Wirtualnych.
DOK.3	Dostawca dostarczy Opis konfiguracji zawierający listę komponentów Platformy IP_CMC i ich opis, a także opis jak komponenty zostały dostosowane do środowiska docelowego.
DOK.4	Wykonawca przygotuje dokumentację sprzęgu i integracji opisującą działanie metod i funkcji oraz opis konfiguracji dostępów do sprzęgu Platformy IP_CMC.
DOK.5	Dostawca dostarczy dokumentację projektową zgodnie z zakresem określonym w części "Zarządzanie projektem", m.in. przygotuje i dostarczy dokumentację powdrożeniową, techniczną zapewniającą zrozumienie struktury, funkcji oraz opis budowy komponentów Platformy IP_CMC.
DOK.6	W szczególności Wykonawca sporządzi i dostarczy dokumentację powdrożeniową zawierającą minimalnie: 1. Rejestry zmian i wersji dokumentacji wdrożeniowej. 2. Dokumentację dotyczącą historii projektu. 3. Dokumentację wprowadzonych zmian, aktualizacji i wersji Platformy CMC. 4. Architekturę systemu, w tym szczegółowy opis struktury systemu, warstw aplikacji, komponentów, baz danych, integracji z innymi systemami, informacji o użytych technologiach, frameworkach i bibliotekach. 5. Instrukcje instalacji z opisem krok po kroku instalacji wszystkich niezbędnych składników Platformy IP_CMC i skryptów automatyzujących procesy DevSecOps. 6. Instrukcje konfiguracji, w tym ustawień aplikacji, parametrów serwerów, ustawień bazy danych, konfiguracji sieciowej, konfiguracji zabezpieczeń, firewalli, itp.

	7. Procedury aktualizacji po wykryciu błędów, potencjalnych zagrożeń czy po pojawieniu się łatek od dostawców. 8. Informacje na temat danych testowych, które mogą być wykorzystane do testowania Platformy IP_CMC w czasie wdrożenia. 9. Zaktualizowane instrukcje użytkowania. 10. Dokumentację zawierającą opisy procedur i procesów, które należy przestrzegać podczas korzystania z Platformy CMC. 11. Opis sposobu raportowania błędów i usterek wraz z instrukcjami dotyczącymi sposobu zgłaszania problemów i śledzenia ich statusu. 12. Informacje kontaktowe do zespołu wsparcia technicznego, wraz z procedurami zgłaszania pytań, problemów lub żądań pomocy. 13. Szczegółowe informacje techniczne dotyczące kodu źródłowego, struktury baz danych, sprzęgu, integracji zewnętrznych systemów, w tym opisy endpointów, metod i przykłady użycia. 14. Opis przyjętych polityk bezpieczeństwa, w tym zabezpieczeń, uwierzytelniania, kontroli dostępu, szyfrowania danych. 15. Plan awaryjny i procedury odzyskiwania danych, szczegółowe procedury na wypadek awarii systemu, w tym plany odzyskiwania po katastrofie i kopie zapasowe. 16. Informacje kontaktowe: Dane kontaktowe osób odpowiedzialnych za projekt, wsparcie techniczne i utrzymanie systemu. 17. Informacje na temat licencji oprogramowania, zewnętrznych bibliotek, użytych grafik itd. 18. Glosariusz: Wyjaśnienia terminów technicznych i skrótów używanych w dokumencie.
DOK.7	Wykonawca zapewni, że powdrożeniowa dokumentacja projektu IT będzie dokładna, aktualna i łatwo dostępna dla wszystkich zainteresowanych stron.
DOK.8	Wykonawca przygotuje dokumentację opisującą możliwości wykorzystania zasobów chmury przez naukowców do celów naukowych w laboratoriach.
DOK.9	Dokumentacja użytkownika (tj. przewodnik użytkownika) powinna zawierać szczegółowy opis wszelkich funkcjonalności i właściwości dostarczonego rozwiązania informatycznego, pozwalający na poprawną konfigurację i eksploatację Oprogramowania zgodnie z jej przeznaczeniem. W szczególności dokumentacja powinna zawierać: 1. opis podstawowych ról użytkowników i zasad ich kreowania; 2. opis zarządzania uprawnieniami użytkownika i tworzenia profili; 3. opis zarządzania autoryzacją i autentykacją użytkowników; 4. opis interfejsu użytkownika oraz opis zasad budowy dialogu z użytkownikiem 5. opis specyficznych elementów konfiguracji interfejsu użytkownika; (personalizacja interfejsu, zasad dialogu) - jeśli takie występują; 6. instrukcje obsługi dla wszystkich zasadniczych funkcjonalności biznesowych; 7. opis procedur przetwarzania danych dostępnych dla użytkownika (opis procesów lub diagramy procesów); Przewodnik użytkownika może być podzielony wg zasadniczych grup ról wykorzystujących Oprogramowanie w procesach biznesowych. Jeśli przewodnik składa się z kilku elementów to w każdym z nich powinno znaleźć się ich wyszczególnienie i istotne odnośniki do powiązanych elementów.

DOK.10	Dokumentacja eksploatacyjna oraz techniczna dla służb technicznych i administratorów (Instrukcji dla administratora i służb technicznych) powinna zawierać opisy wszelkich cech, właściwości i funkcjonalności pozwalających na poprawną z punktu widzenia technicznego eksploatację Platformy IP_CMC. W szczególności dokumentacja ta powinna zawierać: 1. Wyszczególnienie oraz opis powiązań wszystkich komponentów sprzętowych, systemowych i aplikacyjnych występujących lub wymaganych do poprawnej pracy aplikacji zgodnie z wymaganiami wydajności, funkcjonalności i bezpieczeństwa (minimalny, maksymalny, rekomendowany), dla komponentów innych dostawców, należy dokładnie określić wykorzystywane i dopuszczalne wersje; 2. Konfigurację dla wszystkich urządzeń i usług wdrożonych/zainstalowanych w ramach budowy Platformy IP_CMC. 3. Opis konfiguracji komponentów Oprogramowania, w tym wersję oprogramowania, narzędzia, użytkowników i grupy systemowe, katalog instalacyjny, położenie plików konfiguracyjnych, pierwotne parametry konfiguracyjne i zmodyfikowane w procesie instalacji, położenie plików logów, położenie i opis innych kluczowych plików i katalogów, parametry instancji, itp. 4. Opis architektury logicznej i technicznej wymaganej do zrozumienia powiązań logicznych poszczególnych komponentów i ich roli w architekturze Platformy IP_CMC. 5. Opis struktur danych. Opis wykorzystywanych struktur danych musi w szczególności zawierać: listę tabel bazy danych wraz z opisem pól, formaty danych, itp., kryteria walidacji danych wejściowych, opis zmiennych konfiguracyjnych. 6. Procedury tworzenia środowisk pomocniczych. Zasady i procedury tworzenia środowisk (testowych, rozwojowych, raportowych) oraz metod klonowania i animizacji (depersonifikacji) danych przenoszonych pomiędzy środowiskami; 7. Procedury eksploatacji. W szczególności dokumentacja zawiera procedury: a) tworzenia/odtwarzania kopii bezpieczeństwa operacyjnego i kopii zapasowych oraz odtwarzania/kreowania z kopii wszystkich komponentów aplikacji i środowiska (bazy danych, komponenty serwera aplikacji, klienta itp.), b) odtworzenia systemu po katastrofie (disaster recovery). Procedury muszą opisywać kolejne kroki pozwalające na bezpieczne zatrzymanie/uruchomienie elementu infrastruktury chmurowej oraz Oprogramowania. 8. Procedury lub instrukcje instalacji, reinstalacji, deinstalacji oraz aktualizacji. Szczegółowy opis postępowania w przypadku tworzenia lub zmian w środowisku; jeśli wykorzystywane są procedury innych dostawców dla standardowych komponentów (np. baz danych) wystarczy wskazać w dokumentacji szczegółowe odniesienie do procedur standardowych właściwych dla tych komponentów. 9. Opis rutynowych czynności administracyjnych (dziennych, tygodniowych, miesięcznych itp.) oraz działań pozwalających na utrzymanie wymaganej dostępności, wydajności i bezpieczeństwa. Wymagane jest dostarczenie poprawnych inicjalnych sekwencji realizowanych czynności administracyjnych i utrzymaniowych i zasad ich aktualizacji i budowy; opis zasad pielęgnacji i utrzymania aplikacji. Procedury administracyjne powinny w szczególności zawierać informacje o

	okresowych zadaniach, które muszą być wykonane przez administratora, np. weryfikacja zajętości przestrzeni tabel, konieczność wykonywania analizy tabel, czyszczenia logów, itp. 10. Opis zasad i zaleceń strojenia aplikacji. 11. Dokumentacja administratora bezpieczeństwa. 12. Zestaw dokumentacji szczegółowo opisujących zastosowane rozwiązania dotyczących spełniania wymagań ogólnych (zgodnie z wymaganiami prawa) oraz specyficznych zamawiającego dot. bezpiecznej eksploatacji. Dokumentacja, w szczególności, powinna zawierać: • opis zastosowanych mechanizmów ochrony przed naruszeniem zasad dostępu (poufności), integralności, niezaprzeczalności, wiarygodności oraz opis mechanizmów udostępniania, autoryzacji w tym autoryzacji operacji szczególnych; • opis zastosowanych mechanizmów logowania zdarzeń, śladu audytowego oraz kontroli i monitorowania działań w aplikacji/systemie w tym wszelkich prób naruszenia zasad bezpieczeństwa; • dokumentacja administratora aplikacji i administratora środowiska systemu opisująca szczegółowo funkcjonalności, interfejs oraz zasady zarządzania kontami (użytkownikami) oraz uprawnieniami poszczególnych ról, profili, użytkowników itp.; • dokumentacja opisująca sposób realizacji wymagań wynikających z przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U.2002 Nr 101, poz. 926 z późn. zm.), w tym sposób realizacji wymagań wynikających z rozporządzania Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r., w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024, z późn. zm.), jeśli aplikacja przetwarza dane osobowe; w sprawie cyberbezpieczeństwa uwzględniająca zapisy dyrektywy NIS-2. • opis zabezpieczeń interfejsów oraz opis metod zapewnienia poufności i kontrolowalności tych kanałów przepływu informacji, jeśli aplikacja wykorzystuje jakiekolwiek mechanizmy wymiany informacji z innymi systemami; • dokumentacja z testów bezpieczeństwa aplikacji wykonanych przez dostawcę lub wykonanych przez niezależną firmę specjalistyczną. • wyszczególnienie wszystkich parametryzowanych elementów systemu wraz z opisem ich znaczenia i dopuszczalnych wartości oraz stosowanych wartości domyślnych
DOK.11	Dokumentacja będzie zawierać opis podejścia do jej wersjonowania, w tym będzie zawierać opis zasad: • wersjonowania. • zarządzania dokumentami historycznymi i archiwalnymi

MODYFIKACJA 23.07.2024 **Załącznik 3 do SWZ**

14. Wymagania w zakresie zgodności z prawem i regulacjami

Całość prac związanych z tworzeniem Platformy IP_CMC oraz jej późniejszym utrzymaniem powinna być prowadzona w sposób profesjonalny i zgodny z obowiązującym prawem. W szczególności Wykonawca powinien zapewnić zgodność z następującymi wymaganiami:

Nr	Punkt kontrolny
CO.1	Platforma IP_CMC musi być zgodna z aktualnymi przepisami prawa, na podstawie których funkcjonuje Zamawiający.
CO.2	Zamawiający wymaga, aby Platforma IP_CMC była aktualizowana i modyfikowana na bieżąco, co do zgodności z obowiązującym powszechnie prawem oraz wewnętrznymi aktami prawnymi i regulaminami.
CO.3	W przypadku zmian w aktach prawa powszechnie obowiązującego, Wykonawca ma obowiązek dokonać aktualizacji/modyfikacji Platformy IP_CMC w terminie do 7 dni kalendarzowych przed wejściem w życie nowych przepisów lub przepisów w zmienionym brzmieniu, a gdy vacatio legis jest krótszy niż 7 dni kalendarzowych– w dniu ich wejścia w życie.
CO.4	W przypadku zmian w aktach prawa i regulaminach wewnętrznie obowiązujących Zamawiający udostępni Wykonawcy treść zmienionego aktu prawnego lub regulaminu. W takim wypadku Wykonawca ma obowiązek dokonać aktualizacji/modyfikacji Platformy IP_CMC w terminie do 7 dni od otrzymania treści aktu prawnego lub regulaminu.
CO.5	Wykonawca wskaże fizyczne miejsce przechowywania danych IP_CMC, w tym danych konfiguracyjnych i technicznych, oraz kopii danych.
CO.6	Wykonawca gwarantuje, że żadne dane Platformy IP_CMC, w tym dane konfiguracyjne i techniczne, nie będą transferowane przez łącza w sposób jawny oraz nie będą przekazywane przed urządzenia poza terenem EU.
CO.7	Wykonawca gwarantuje, że będą one przechowywane wyłącznie na terenie Polski lub Unii Europejskiej.
CO.8	Platforma IP_CMC musi posiadać historię ścieżek analizy (pipeline) danych medycznych: sekwencyjnych, obrazowych oraz klinicznych. Ścieżki analizy powinny być udokumentowane.
CO.9	Platformy IP_CMC ma możliwość wyeksportowania ścieżek analizy z poziomu wiersza poleceń (command linę interface) do plików zewnętrznych.
CO.10	Wykonawca zapewnia zgodność Platformy IP_CMC z obowiązującymi regulacjami ochrony danych osobowych, takimi jak RODO oraz cyberbezpieczeństwa, takimi jak NIS2. Platforma IP_CMC spełnia wymagania regulacji dotyczących bezpieczeństwa norm 27001:22 i prywatności przechowywanych danych. Wykonawca udokumentuje zgodność z przepisami i politykami RODO oraz z przepisami prawa.

15. Wymagania w zakresie opcji

Zamawiający przewiduje możliwość zamówienia dodatkowych usług związanych z Platformą IP_CMC w ramach prawa Opcji. Zamówienie prac w ramach Opcji będzie możliwe w ramach ustalonego w Umowie limitu i może dotyczyć dowolnych prac rozwojowych w ramach platformy, których Zamawiający nie przewidział na etapie zamówienia, a które wynikać mogą z pojawiających nowych

możliwości technicznych, zmian w procesach Zamawiającego, zmian wynikających z nowych wymagań Agencji Badań Medycznych, konieczności dopasowania działania Platformy IP_CMC z nowymi Partnerami czy ośrodkami badawczymi. Zasady korzystania z Opcji zostały wskazane w Umowie, jednocześnie Wykonawca będzie stosował się do następujących wymagań szczegółowych:

Nr	Punkt kontrolny
OP.1	Zamawiający wymaga, aby Wykonawca przyjmował zgłoszenia dotyczące zlecenia Opcji w Godzinach Roboczych.
OP.2	Zlecenie i realizacja prac w ramach Opcji będzie realizowane w następującym trybie: 1. Prace zleca Zamawiający. 2. Przed przystąpieniem do wykonania prac przez Wykonawcę, Strony uzgodnią wstępnie zakres prac tj. termin wykonania oraz przewidywaną pracochłonność. 3. Zamawiający każdorazowo będzie zgłaszać Wykonawcy potrzebę wykonania prac w formie pisemnej lub mailowej. 4. Wykonawca wykona prace w uzgodnionym terminie. 5. Wykonawca przystąpi do wykonania prac zgodnie z zakresem określonym w zleceniu, po jego przyjęciu. W przypadku odmowy przyjęcia zlecenia, Wykonawca prześle Zamawiającemu pisemne lub mailowe uzasadnienie odmowy ze wskazaniem rozbieżności pomiędzy zleceniem a wcześniejszymi ustaleniami. 6. Po wykonaniu prac Wykonawca przeprowadzi testy sprawdzające poprawność działania Platformy. 7. Potwierdzeniem wykonania prac będzie pisemne lub mailowe potwierdzenie realizacji przez uprawnionego pracownika Zamawiającego. 8. Wykonawca wykona w terminie wykonania prac uzupełnienie dokumentacji. Wykonawca dochowa profesjonalnej staranności, aby dokonane w ramach Opcji prace nie wpływały na stabilną i wydajną pracę Platformy IP_CMC. W przypadku ryzyka negatywnego wpływu na wydajność Wykonawca poinformuje o tym przed przyjęciem zlecenia.
OP.3	Dla prac wykonanych w ramach Opcji Wykonawca zapewni gwarancję do końca trwania Gwarancji, ale nie krócej niż przez okres minimum 2 miesięcy, na zasadach określonych w OPZ w rozdziale 11.
OP.4	Dla prac wykonanych w ramach Opcji Wykonawca zapewni asystę techniczną do końca trwania Asysty Technicznej, ale nie krócej niż przez okres minimum 2 miesięcy, na zasadach określonych w OPZ w rozdziale 12.
OP.5	Opłaty za prace w ramach prawa Opcji będą prezentowane na dokumentach księgowych osobno dla każdego zadania, tj. na jednym dokumencie księgowym za dany okres zostaną wskazane rozdzielnie pozycje dotyczące każdego ze zleceń w ramach Opcji.

16. Zasady odbioru

W celu zapewnienia transparentności działania Wykonawcy w czasie odbioru wyników jego prac Wykonawca spełni następujące wymagania obligatoryjne:

Nr	Punkt kontrolny
ODB.1	Wykonawca zapewni przeprowadzenie procedury odbiorów dla wykonanych prac i dostarczonych produktów oraz usług zgodnie z zasadami określonymi w umowie między Wykonawcą a Zamawiającym.

ODB.2	Wykonawca przystąpi do odbiorów komponentów technicznych Platformy IP_CMC pod kątem poprawności i zgodności z Dokumentem Analizy wdrożeniowej, Projektem Technicznym oraz OPZ, po przygotowaniu i przetestowaniu wcześniej samodzielnie przez Wykonawcę.
ODB.3	Wykonawca przystąpi do odbiorów produktów i usług dostarczonych w ramach kamieni milowych zgodnie z harmonogramem.

17. Podstawy prawne

Dostarczana Platforma musi być zgodna z następującymi aktami prawnymi:

Nr	Akty prawne
AP.1	Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. z 2023 r. poz. 2465.)
AP.2	Rozporządzenie Parlamentu Europejskiego I Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
AP.3	Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzecznika Praw Pacjenta (Dz. U. z 2024 r. poz. 581.)
AP.4	Rozporządzenie Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (t.j. Dz. U. z 2022 r. poz. 1304 z późn. zm.).
AP.5	Rozporządzenie Ministra Zdrowia z dnia 7 lipca 2017 r. w sprawie minimalnej funkcjonalności dla systemów teleinformatycznych umożliwiających realizację usług związanych z prowadzeniem przez świadczeniodawcę list oczekujących na udzielenie świadczenia opieki zdrowotnej (Dz. U. z 2017 r. poz. 1404)
AP.6	Rozporządzenie Ministra Zdrowia z dnia 26 września 2005 r. w sprawie kryteriów medycznych, jakimi powinni kierować się świadczeniodawcy, umieszczając świadczeniobiorców na listach oczekujących na udzielenie świadczenia opieki zdrowotnej (Dz.U. z 2005 r., nr 200, poz. 1661)
AP.7	Ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (Dz. U. z 2023 r. poz. 1516 z późn. zm.)
AP.8	Ustawa z dnia 15 lipca 2011 r. o zawodach pielęgniarki i położnej (Dz. U. 2023 r. poz. 185, 1234)
AP.9	Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz. U. Dz. U. z 2023 r. poz. 991 z późn. zm.)
AP.10	Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781.)
AP.11	Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 307)
AP.12	Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344.)

AP.13	Ustawa z dnia 5 września 2016 r. o usługach zaufania, identyfikacji elektronicznej (Dz. U. z 2024 r. poz. 422.)
AP.14	Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. Urz. UE C z 2014 r.);
AP.15	Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r., poz. 2247);
AP.16	Rozporządzenie Ministra Zdrowia z dnia 26 czerwca 2020 r. w sprawie szczegółowego zakresu danych zdarzenia medycznego przetwarzanego w systemie informacji oraz sposobu i terminów przekazywania tych danych do Systemu Informacji Medycznej (Dz.U. 2020 poz. 1253)