

DOTYCZY: Dostawa licencji na oprogramowanie Portal Pracownika wraz z usługą dostępu do danych Zamawiającego poprzez chmurę prywatną

Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest Dostawa licencji na oprogramowanie Portal Pracownika zintegrowanego z systemem InfoMedica/AMMS Zamawiającego produkcji Asseco Poland (zwany dalej „ZSI”) wraz z usługą dostępu do tego portalu poprzez chmurę, spełniający minimalne wymagania opisane w dalszej części dokumentu .

PORTAL PRACOWNIKA	
Zamawiający wymaga dostawy systemu zgodnie z następującymi minimalnymi wymaganiami:	
I.	WYMAGANIA OGÓLNE
1)	Do obowiązków Wykonawcy w ramach niniejszego zadania należy: • Udzielenie bezterminowej, niewyłącznej, nieprzenoszalnej i niezbywalnej licencji na oprogramowanie Portal Pracownika zintegrowane z systemem InfoMedica Zamawiającego (zwanego dalej ZSI) spełniającą minimalne wymagania funkcjonalne określone poniżej. Udzielona licencja musi zapewnić uruchomienie oprogramowania na dowolnej liczbie urzędów oraz pozwalać na wykorzystanie w dowolnej jednostce organizacyjnej Zamawiającego • Wdrożenie dostarczonego oprogramowania Portalu Pracownika poprzez instalację oraz konfigurację (w tym stacje robocze o ile wymaga tego zaproponowane rozwiązanie) • Zintegrowanie dostarczonego Portalu Pracownika z systemem InfoMedica (moduły Kadrowo - Płacowe) • Dostarczenie wszystkich niezbędnych do prawidłowego działania Portalu Pracownika licencji w tym także licencji integracyjnych zapewniających współdziałanie oferowanego oprogramowania z oprogramowaniem InfoMedica Zamawiającego
2)	Portal Pracownika musi być kompatybilny i w sposób niezakłócony współdziałać z oprogramowaniem InfoMedica produkcji Asseco Poland funkcjonującym u Zamawiającego. Zamawiający zastrzega sobie prawo do potwierdzenia u producenta oprogramowania firmy Asseco Poland zgodności zaoferowanego systemu z posiadanym systemem.
3)	Współdziałanie z oprogramowaniem InfoMedica Zamawiającego należy rozumieć poprzez pełną dwukierunkową wymianę danych (nie dopuszcza się wymiany danych poprzez pliki, eksporty/importy danych, itp.);
4)	Dostarczony Portal Pracownika musi mieć zapewniony serwis gwarancyjny producenta. W ramach serwisu gwarancyjnego Zamawiający może zgłaszać błędy do producenta aplikacji oraz mieć dostęp do bazy wiedzy i aktualizacji zakupionego produktu zgodnie z opisem w pozycji „Warunki gwarancji”
5)	W przypadku, gdy zaoferowany przez Wykonawcę Portal Pracownika nie będzie właściwie współdziałać z oprogramowaniem InfoMedica Zamawiającego i/lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska produkcyjnego Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego. Dokona na własny koszt niezbędnych modyfikacji przywracających właściwe działanie środowiska produkcyjnego Zamawiającego również po odinstalowaniu oprogramowania.
6)	Wykonawca zobowiązany jest dostarczyć dokumentację techniczną w języku polskim ze wskazaniem poszczególnych wymaganych funkcjonalności (z dokładnością do punktu, strony w dokumentacji)
7)	Wykonawca dostarczy pełną dokumentację powdrożeniową zastosowanej/wdrożonej konfiguracji Portalu Pracownika zawierającą: • opis konfiguracji niezbędny do prawidłowego działania systemu • opis sposobu przeprowadzenia integracji oraz przepływu danych pomiędzy integrowanymi systemami zawierający schemat integracji dostarczonego oprogramowania z systemem ZSI • instrukcję postępowania w przypadku wystąpienia awarii – procedurę przywracania działania systemu
II.	MINIMALNE WYMAGANIA FUNKCJONALNE
1)	Dwukierunkowa integracja z ZSI w zakresie umożliwiającym pracownikowi tworzenie różnego rodzaju zdarzeń (np. wnioski urlopowe) i dostęp do informacji dotyczących danego pracownika
2)	Zabezpieczenie przed dostępem do danych dla niepowołanych osób (konieczność odrębnego logowania)

3)	Możliwość modyfikacji wyglądu pulpitu dostępnego po zalogowaniu przez użytkownika
4)	Funkcjonalność powiadomień wysyłanych na wskazane adresy e-mail pracowników min. o: • Zmianie statusu wniosku urlopowego • Powiadomienie o wniosku oczekującym na zatwierdzenie • Powiadomienie o nowym komunikacie /zarządzeniu
5)	Funkcjonalność konfiguracji kont użytkowników wraz z ich uprawnieniami do poszczególnych funkcji bądź grup funkcji
6)	Zapewnienie możliwości włączenia autoryzacji użytkowników poprzez usługę Active Directory
7)	Zapewnienie tworzenia odpowiednich zgodnych z polityką szpitala zasad dotyczących haseł (m.in. okres ważności, ilość powtórzeń, długość hasła).
8)	Panel konfiguracyjny dostępny tylko dla administratora umożliwiający zarządzanie kontami użytkowników oraz parametrami systemu (m.in. widocznością poszczególnych części składowych menu) oraz parametrami synchronizacji danych
9)	Funkcjonalność zmiany hasła oraz automatyczne przekazanie uprawnień stanowiskowych w przypadku nieobecności, w ramach konta użytkownika.
10)	Zarządzanie widocznością danych kontaktowych pracowników poprzez możliwość wyłączenia/włączenia tych danych dla wybranej grupy pracowników lub dla wszystkich pracowników
11)	Funkcjonalność konfiguracji obiegu dokumentów dla wniosków urlopowych i delegacji
12)	Funkcjonalność parametryzacji struktury organizacyjnej, w tym: • informacji o podległościach komórek • informacji o przełożonych • informacji o poziomach obiegu wniosku urlopowego
13)	Przeglądanie przez pracownika swoich danych w zakresie kadrowym, w tym co najmniej: • danych personalnych • informacji o nieobecnościach • wymiarów i stanów urlopów • danych dotyczących badań lekarskich wraz z informacją o dacie wygaśnięcia badań • wyświetlanie zastępstw urlopowych • obsługę akceptacji zastępstw urlopowych • obsługę wniosków do korekty
14)	Przeglądanie przez pracownika swoich danych w zakresie płacowym, w tym co najmniej: • przeglądanie pasków płacowych • miesięczne i narastające zestawienie dochodów wraz z informacją o przekroczeniu progu podatkowego • informacje o zadłużeniach i składkach na KZP
15)	Przeglądanie przez pracownika swoich danych o odbytych szkoleniach oraz podpisanych umowach szkoleniowych
16)	Przeglądanie przez pracownika swoich danych dotyczących wyposażenia na stanie oraz poszczególnych komponentów tego wyposażenia
17)	Przeglądanie przez pracownika grafików planowanych
18)	Funkcjonalność elektronicznego obiegu wniosków urlopowych zapewniająca min.: • możliwość złożenia przez pracownika wniosku urlopowego • możliwość zatwierdzenia wniosku przez wskazanego zastępcę, a następnie przez bezpośredniego przełożonego • powiadomienia mailowe informujące o oczekującym wniosku do zatwierdzenia lub o zmianie statusu danego wniosku urlopowego • podgląd informacji o wymiarze i stanie danego typu urlopu • przeglądanie danych o urlopach, w ramach określonego zakresu czasowego • przekazywanie informacji o wnioskowanych nieobecnościach do systemu kadrowo-płacowego
19)	Funkcjonalność wyszukiwania danych kontaktowych pracowników poprzez: • wyszukanie pracowników zatrudnionych w danej komórce organizacyjnej • wyszukanie pracowników podlegających danemu przełożonemu • wyszukanie pracownika według imienia lub nazwiska
20)	Funkcjonalność zapewniająca dedykowany panel dla przełożonego, zapewniający min.: • wyświetlanie aktywności pracownika (rejestracja wniosku urlopowego, delegacji) • zatwierdzanie urlopów • zatwierdzanie delegacji • przeglądanie informacji o nieobecnościach

	• przeglądanie informacji o wygasających badaniach lekarskich • przeglądanie informacji o ilości dni zaległego urlopu wypoczynkowego • przeglądanie wyposażenia • przekazywanie uprawnień do obsługi wniosków urlopowych i delegacji podległych pracowników • w przypadku kiedy przełożonym jest Dyrektor lub jego Zastępca zapewnienie wyświetlania aktywności dla wszystkich pracowników podległego działu, nie tylko kierownika tego działu
21)	Funkcjonalność zapewniająca dedykowany panel usprawniający obsługę dostępnych informacji przez kadry, pozwalający na: • obsługę listy błędnie wyeksportowanych wniosków urlopowych • obsługę wniosków urlopowych oczekujących na akceptację • przeglądanie wniosków urlopowych wraz z możliwością rejestracji rezygnacji lub modyfikacji daty zakończenia w przypadku zachorowania pracownika • obsługę wniosków delegacyjnych oczekujących na akceptację
22)	Funkcjonalność zapewniająca pobieranie deklaracji podatkowych przez pracownika
23)	Funkcjonalność zapewniająca dedykowany umożliwiający obsługę dostępnych danych przez płace, pozwalający na: • zainicjowanie procesu dystrybucji deklaracji podatkowych • przeglądanie informacji o odebranych i nieodebranych deklaracjach • wysyłanie przypomnienia o deklaracjach oczekujących na odbiór • przekazywanie informacji o odebranych i nieodebranych deklaracjach do systemu kadrowo-płacowego • zainicjowanie procesu dystrybucji ZUS IMIR na podstawie plików XML pobranych z programu Płatnik • wyrażenie przez pracownika zgody lub sprzeciwu na elektroniczną dystrybucję ZUS IMIR • przeglądanie informacji o odebranych i nieodebranych ZUS IMIR • wysyłanie przypomnienia o ZUS IMIR oczekujących na odbiór
24)	Funkcjonalność zapewniająca dedykowany panel umożliwiający obsługę zarządzeń i komunikatów przez pracownika poprzez: • przeglądanie wszystkich dostępnych publikacji • wyróżnienie publikacji wymagających potwierdzenia odczytu
25)	Funkcjonalność zapewniająca publikację zarządzeń i komunikatów poprzez: • możliwość wprowadzenia nowej publikacji • możliwość wprowadzenia załącznika w formacie: Word, PDF, JPG, Excel, tekst • możliwość określania grupy odbiorców • możliwość określania poziomu ważności publikacji • możliwość określania wymagalności potwierdzenia zapoznania się z treścią oraz terminu potwierdzenia • wysyłanie powiadomienia o nowych publikacjach do odczytania przez wskazaną grupę pracowników • przeglądanie informacji o odczytanych i nieodczytanych publikacjach • wysyłanie przypomnienia o publikacjach oczekujących na odczyt • przeglądanie wszystkich wprowadzonych publikacji

USŁUGA DOSTĘPU DO DANYCH POPRZEC CHMURĘ PRYWATNĄ

Zamawiający wymaga dostarczenia subskrypcji systemu zapewniającego dostęp pracowników Zamawiającego do danych wskazanych poniżej poprzez chmurę prywatną zgodnie z następującymi minimalnymi wymaganiami:

Przez chmurę prywatną Zamawiający rozumie środowisko obliczeniowe dostarczane przez dostawcę usług w chmurze z uwzględnieniem wymagań RODO oraz zgodnych z przepisami prawa dotyczących ochrony wrażliwych danych medycznych i finansowych, w którym zasoby obliczeniowe są przydzielane i zarządzane tylko i wyłącznie przez jedną organizację

I.	WYMAGANIA OGÓLNE
1)	Usługa dostępu do danych poprzez chmurę prywatną musi obejmować następujące obszary: • dane zawarte w Portalu Pracownika • dostęp do Zdalnego Repozytorium Elektronicznej Dokumentacji Medycznej dla pracowników medycznych Zamawiającego • dostęp do oprogramowania umożliwiającego przechowywanie Elektronicznej Dokumentacji Medycznej (EDM) w lokalizacji zdalnej (repozytorium Wykonawcy) wraz z możliwością jej

	indeksowania i wymiany pomiędzy placówkami ochrony zdrowia przy wykorzystaniu infrastruktury P1 oraz platformy eCareMed
2)	Wykonawca dokona wdrożenia, instalacji oraz konfiguracji wszystkich elementów (w tym stacje robocze o ile wymaga tego zaproponowane rozwiązanie) składających się na całość dostarczanej usługi
3)	Usługa musi być kompatybilna i w sposób niezakłócony współdziałać z oprogramowaniem ZSI funkcjonującym u Zamawiającego. Zamawiający zastrzega sobie prawo do potwierdzenia u producenta oprogramowania firmy Asseco Poland zgodności zaoferowanej usługi z posiadanym systemem ZSI.
4)	Wszystkie niezbędne licencje do prawidłowego działania usługi oraz licencje integracyjne do prawidłowego współdziałania oferowanej usługi z oprogramowaniem ZSI Zamawiającego dostarczy Wykonawca.
5)	Dostarczona usługa musi zapewnić dostęp do danych na dowolnej liczbie urządzeń
6)	W przypadku, gdy zaoferowana przez Wykonawcę usługa nie będzie właściwie współdziałać z oprogramowaniem ZSI Zamawiającego i/lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska produkcyjnego Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego. Dokona na własny koszt niezbędnych modyfikacji przywracających właściwe działanie środowiska produkcyjnego Zamawiającego również po odinstalowaniu oprogramowania.
7)	Wykonawca wraz z usługą dostarczy pełną dokumentację powdrożeniową zastosowanej/wdrożonej konfiguracji zawierającą: • opis konfiguracji usługi, • opis sposobu przeprowadzenia integracji oraz przepływu danych (z podziałem na szczegółowy opis wszystkich możliwych do przesłania danych) pomiędzy systemem ZSI a dostarczoną usługą • instrukcje stanowiskowe dla użytkowników końcowych • instrukcje administrowania nowym środowiskiem.
8)	Łańcuch dostaw Łańcuch dostaw stanowi sieć dostawców i usługodawców, którzy prowadzą współpracę od pozyskiwania przedmiotu umowy. • Wykonawca dołączy do umowy opis łańcucha dostaw dla przedmiotu umowy, • Wykonawca zapewni propagację odpowiednich praktyk w zakresie bezpieczeństwa w całym łańcuchu dostaw, jeżeli jakiegokolwiek komponent przedmiotu umowy został zakupiony lub nabyte od innych dostawców lub innych podmiotów (np. podwykonawców zajmujących się tworzeniem oprogramowania i dostawców komponentów sprzętowych);
9)	Usługa powinna zostać dostarczona w modelu SaaS (Software as a Service).
10)	Dostawca skonfiguruje i uruchomi usługę do komunikacji z użytkowanym przez Zamawiającego ZSI
11)	Wykonawca udostępni infrastrukturę sprzętową w chmurze w trybie 24h/7 dni spełniającą wszystkie obowiązujące przepisy prawa w zakresie przechowywania i przetwarzania danych osobowych oraz danych medycznych pacjenta.
12)	Dostawca zobowiązany jest wskazać lokalizację Centrów Przetwarzania Danych wykorzystywanych na potrzeby usługi.
13)	Wykonawca w zakresie udostępnionej w chmurze infrastruktury sprzętowej przekaże Zamawiającemu pełną informację o wszystkich fizycznych lokalizacjach serwerów , na których przetwarzane będą dane zawarte z zastrzeżeniem, że żadne z tych miejsc nie może być zlokalizowane poza granicami Unii Europejskiej.
14)	Wykonawca w zakresie udostępnionej w chmurze infrastruktury sprzętowej będzie zobowiązany do każdorazowego przekazania Zamawiającemu informacji o planowanej zmianie lokalizacji udostępnionej w chmurze infrastruktury sprzętowej w terminie umożliwiającym podjęcie decyzji o ewentualnym rozwiązaniu umowy, tj. nie później niż 2 miesiące przed dniem planowanej zmiany lokalizacji.
15)	Wykonawca w zakresie udostępnionej w chmurze infrastruktury sprzętowej umożliwi Zamawiającemu pełny dostęp do dokumentacji dotyczącej zasad bezpieczeństwa oraz środków technicznych przyjmowanych w poszczególnych centrach przetwarzania danych.
16)	Okres świadczenia usługi 24 / 36 miesięcy od daty zawarcia umowy.
17)	Oferowana usługa w środowisku chmurowym musi zapewniać uwierzytelnianie dwuskładnikowe (2FA)

18)	Wykonawca zapewni wysoki poziom bezpieczeństwa dla komunikacji pomiędzy usługą a infrastrukturą Zamawiającego. W przypadku wykorzystania komunikacji SSL w ramach usługi Wykonawca dostarczy niezbędne certyfikaty WSS, TLS. na okres zgodny z okresem udostępniania usługi Zamawiającemu
19)	W celu zapewnienia wysokiego poziomu bezpieczeństwa Dostawca zapewni objęcie usługi monitoringiem prowadzonym przez Security Operation Center (SOC) działającym w trybie 24/7/365 i bieżące informowanie Zamawiającego o wszystkich zauważonych incydentach.
20)	W ramach usługi Wykonawca zapewni kopie zapasowe danych z minimum 3 dni wstecz .
21)	Dostawca dostarczy komplet dokumentów opisujących szczegółowo zasady korzystania z usługi z uwzględnieniem wymagań RODO (w tym Regulamin, Opis usługi).
22)	Wykonawca podpisze umowę powierzenia przetwarzania danych osobowych
23)	Przerwy techniczne w ciągu miesiąca kalendarzowego nie mogą trwać dłużej niż 48 godzin i nie powinny rozpoczynać się przed godziną 19:00. O planowanych przerwach technicznych Wykonawca zobowiązany jest informować Zamawiającego z minimum 2 dniowym wyprzedzeniem.
24)	W przypadku rezygnacji przez Zamawiającego z usługi Dostawca przekaze całość zdeponowanej w usłudze dokumentacji w formacie umożliwiającym zaimportowanie dokumentów i odtworzenie w innym systemie teleinformatycznym.
II.	MINIMALNE WYMAGANIA FUNKCJONALNE
1)	Minimalne wymagania funkcjonalne w zakresie usługi dostępu do danych zawartych w Portalu Pracownika
a)	Dostępność na komputery stacjonarne oraz urządzenia mobilne
b)	Wywołanie Portalu Pracownika w środowisku chmurowym.
c)	Usługa musi zapewnić zarządzanie rejestrem użytkowników wraz z możliwością zarządzania uprawnieniami użytkowników.
d)	Funkcjonalność umożliwiająca wysyłanie zaproszeń dostępowych do systemu dla nowych użytkowników poprzez pocztę e-mail dostępną z poziomu administratora systemu.
e)	Funkcjonalność zapewniająca powiązanie użytkowników z użytkownikami systemu Portal Pracownika.
f)	Usługa musi weryfikować dostęp użytkowników Portalu Pracownika. W przypadku braku dostępu lub braku konta powinien wyświetlić właściwy komunikat.
g)	Po zalogowaniu do usługi wywołanie Portalu Pracownika nie może wymagać dodatkowego uwierzytelniania. Dopuszcza się pierwszorazowe logowanie weryfikujące.
h)	Portal Pracownika dostępny w środowisku chmurowym musi posiadać pełny zakres funkcjonalności Portalu Pracownika działającego w sieci szpitalnej.
i)	Po zalogowaniu użytkownika do Portalu Pracownika w środowisku chmurowym muszą być weryfikowane uprawnienia użytkownika nadane w systemie Portal Pracownika działającym w sieci szpitalnej.
2)	Minimalne wymagania funkcjonalne w zakresie dostępu do Zdalnego Repozytorium EDM dla pracowników medycznych Zamawiającego
a)	Usługa musi zapewniać zdalny dostęp do wybranych dokumentów EDM wytwarzanych w ramach podmiotu.
b)	Usługa musi udostępniać przeglądarkę dokumentów EDM
c)	Zdalny dostęp do dokumentacji EDM musi być zapewniony także w przypadku zatrzymania działania całego systemu łącznie z bazą danych – w związku z tym należy zapewnić stałą dostępność kont zdefiniowanych w środowisku chmurowym niezależnie od działania systemu ZSI.
d)	Dostęp do repozytorium EDM w środowisku chmurowym musi być ograniczony tylko z wskazanych przez Zamawiającego publicznych adresów IP. <u>Uwaga:</u> Zamawiający dopuści także ograniczenie polegające na możliwości czasowego włączenia /wyłączenia dostępu w zależności od potrzeb użytkowników Zamawiającego. Dostęp do repozytorium EDM musi być ograniczony tylko dla wybranych przez Zamawiającego użytkowników identyfikowanych adresem e-mail, za pomocą kont zdefiniowanych w usłudze zdalnego repozytorium. Autentykacja w systemie musi być zgodna z najwyższymi standardami bezpieczeństwa
e)	Usługa musi być zintegrowana z wykorzystywanym systemem ZSI w taki sposób, aby Elektroniczna Dokumentacja Medyczna generowana przez ten system mogła być udostępniana zdalnie.

f)	Zapewnienie konfiguracji systemu ZSI w taki sposób, aby system mógł automatycznie , w określonych przez Zamawiającego interwałach czasowych generował raport zbiorczy na temat każdego pacjenta przebywającego na oddziale (np. dokument „Tymczasowa Historia Choroby”), który byłby składowany w zdalnym repozytorium EDM . Intencją przechowywania wybranych danych w ramach usługi jest wykorzystanie tych danych w celu kontynuacji leczenia pacjenta na wypadek czasowej niedostępności systemu HIS . Tymczasowa Historia Choroby po zakończeniu pobytu musi zostać automatycznie usunięta i zastąpiona ostateczną wersją Historii Choroby .
3)	Minimalne wymagania funkcjonalne – w zakresie usługi dostępu do oprogramowania umożliwiającego przechowywanie Elektronicznej Dokumentacji Medycznej (EDM) w lokalizacji zdalnej wraz z możliwością jej indeksowania i wymiany pomiędzy placówkami ochrony zdrowia przy wykorzystaniu infrastruktury P1 oraz platformy eCareMed
a)	Usługa musi umożliwiać składowanie wybranej lub pełnej Elektronicznej Dokumentacji Medycznej w prywatnej chmurze EDM poza infrastrukturą Zamawiającego, dając możliwość indeksowania dokumentacji medycznej i jej wymiany z innymi świadczeniodawcami za pomocą systemu P1 oraz platformy eCareMed.
b)	Zapewnienie konfiguracji posiadanego przez Zamawiającego systemu ZSI w taki sposób aby zapewnić indeksację dokumentów na platformę P1 oraz platformę eCareMed poprzez repozytorium w usłudze chmurowej i tym samym aby dokumenty, o które będą wnioskować świadczeniodawcy i pacjenci, były pobierane z repozytorium dostępnego w chmurze prywatnej
c)	Możliwość składowania i udostępniania dokumentów wytworzonych w oparciu o standard HL7 CDA, w tym Polską Implementację Krajową (PIK) HL7 CDA.
d)	Usługa musi umożliwiać przechowywanie całości dokumentacji EDM wytwarzanej w jednostce ze szczególnym uwzględnieniem tej, która jest wymagana prawem do indeksowania w ramach P1.
e)	Dostarczona usługa do komunikacji z systemem ZSI musi wykorzystywać standard IHE (zgodnie z wytycznymi przygotowanymi do komunikacji z systemem P1).
f)	Usługa będzie zapewniać minimum 1 TB przestrzeni na składowane dokumenty (ok 450 000 dokumentów miesięcznie) oraz będzie zapewniać możliwość jej rozbudowy.
g)	Każdy odpowiednio zdefiniowany, nowoutworzony w systemie HIS Zamawiającego dokument EDM zostanie automatycznie przesłany do przedmiotu usługi oraz zostanie utworzony na platformie P1 indeks dla tego dokumentu wskazujący jego lokalizację (dotyczy dokumentów, których indeksowanie na Platformie P1 jest wymagane prawnie)
h)	Każdy odpowiednio zdefiniowany, nowoutworzony w systemie HIS Zamawiającego dokument EDM zostanie automatycznie przesłany do przedmiotu usługi oraz zostanie utworzony na platformie eCareMed indeks dla tego dokumentu wskazujący jego lokalizację (dotyczy dokumentów zdefiniowanych do indeksacji na platformę eCareMed)
i)	Wykonawca dokona migracji do przedmiotu usługi wskazanych dokumentów EDM dotychczas przechowywanych w lokalnym repozytorium EDM Szpitala oraz ustawi na platformie P1/eCareMed indeksy wskazujące na repozytorium Wykonawcy jako aktualne położenie dla tych dokumentów.
j)	Dokumentacja, o której mowa w ppkt. g i h pozwoli na dostęp do dokumentów EDM pacjentów Szpitala za pośrednictwem platformy P1/ eCareMed z pominięciem lokalnego repozytorium Zamawiającego.
k)	Wykonawca udostępni Zamawiającemu nieodpłatne i w formacie umożliwiającym import dokumentów do lokalnego repozytorium EDM Zamawiającego kopie wszystkich dokumentów Elektronicznej Dokumentacji Medycznej Zamawiającego przechowywanych w repozytorium Wykonawcy, w terminie do 30 dni kalendarzowych od daty zakończenia umowy.

WARUNKI GWARANCJI DLA OPRGORAMOWANIA PORTAL PRACOWNIKA	
Zamawiający wymaga zapewnienia usługi serwisu gwarancyjnego zgodnie z następującymi minimalnymi wymaganiami:	
1)	Wykonawca zapewni serwis gwarancyjny producenta dostarczonego oprogramowania przez okres minimum 24/36 miesięcy , który rozpoczyna się w dniu podpisania protokołu końcowego odbioru przedmiotu zamówienia bez zastrzeżeń.
2)	Wykonawca zapewni serwis gwarancyjny producenta dostarczonych systemów w dni robocze od poniedziałku do piątku w godzinach 8.00-16.00 z wyjątkiem dni ustawowo wolnych od pracy.
3)	Wymagany zakres serwisu gwarancyjnego dla dostarczonego oprogramowania: • Usuwanie wszelkich błędów dostarczonego oprogramowania • Instalowanie i wdrożenia nowych wersji dostarczonego oprogramowania • Usuwanie wszelkich awarii dostarczonego oprogramowania • Zapewnienie prawidłowego współdziałania dostarczonego oprogramowania z ZSI

	- Weryfikacja integralności baz danych. - Bieżące optymalizowanie konfiguracji dostarczonego oprogramowania z uwzględnieniem potrzeb Zamawiającego. - Pomoc w awaryjnym odtwarzaniu na wniosek zamawiającego, stanu oprogramowania i zgromadzonych danych archiwalnych, poprawnie zabezpieczonych na odpowiednich nośnikach. - Weryfikacja integralności baz danych. - Bieżące optymalizowanie konfiguracji dostarczonego oprogramowania z uwzględnieniem potrzeb Zamawiającego. - Bieżące sprawdzenia poprawności działania całego systemu, oraz w razie wystąpienia takiej potrzeby, przeprowadzenie dodatkowych szkoleń dla personelu.								
4)	Możliwość zgłaszania przez Zamawiającego błędów oraz modyfikacji dotyczących funkcjonowania dostarczonego oprogramowania przy czym Zamawiający może zgłaszać następujące typy błędów: - BŁĄD KRYTYCZNY – taki, który uniemożliwia użytkowanie oprogramowania (w zakresie jego podstawowej funkcjonalności wskazanej w dokumentacji użytkownika) i prowadzi do zatrzymania jego eksploatacji, utraty danych lub naruszenia ich spójności, w wyniku, których niemożliwe jest prowadzenie działalności. - BŁĄD ZWYKŁY – taki, który nie wpływa na pracę całego systemu - MODYFIKACJA – zapewniająca możliwość zgłaszania uwag i propozycji modyfikacji oprogramowania								
5)	Zgłaszanie awarii przez Zamawiającego odbywać się będzie poprzez: - witrynę internetową Wykonawcy oraz telefonicznie - za pomocą poczty elektronicznej na adres oraz telefonicznie W przypadku, gdy zgłoszenie zostanie przyjęte przez Wykonawcę: - w godzinach pomiędzy 16.00 a 24.00 dnia roboczego – traktowane jest jak przyjęte o godz. 8.00 następnego dnia roboczego, - w godzinach pomiędzy 0.00 a 8.00 dnia roboczego - traktowane jest jak przyjęte o godz. 8.00 danego dnia roboczego, - w dniu ustawowo lub dodatkowo wolnym od pracy - traktowane jest jak przyjęte o godz. 8.00 najbliższego dnia roboczego.								
6)	Usługi serwisu gwarancyjnego w okresie obowiązywania gwarancji będą polegać na: - usuwaniu błędów (krytycznych, zwykłych) wykrytych w dostarczonym oprogramowaniu w wymaganych terminach, określonych w tabeli poniżej <table border="1"> <thead> <tr> <th>Status zgłoszenia</th><th>Maksymalny czas naprawy</th></tr> </thead> <tbody> <tr> <td>Błąd krytyczny</td><td>4 dni robocze od momentu zarejestrowania zgłoszenia błędu</td></tr> <tr> <td>Błąd zwykły</td><td>21 dni roboczych od momentu zarejestrowania zgłoszenia błędu.</td></tr> <tr> <td>Modyfikacja</td><td>czas dokonania i udostępnienia Zamawiającemu modyfikacji będzie każdorazowo uzgadniany pomiędzy Wykonawcą i Zamawiającym.</td></tr> </tbody> </table> - jeżeli naprawa błędu nie jest możliwa w czasie naprawy określonym w tabeli powyżej, dopuszcza się możliwość zastosowania obejścia, przy czym zastosowanie obejścia nie wyłącza zobowiązania Wykonawcy do naprawy błędu, zastosowanie obejścia powoduje zmniejszenie priorytetu błędu do niższej kategorii błędu, z tym że czas naprawy takiego błędu po zastosowaniu obejścia liczony jest od chwili dokonania zgłoszenia tego błędu; - dostarczanie i instalacja uaktualnień, poprawek i nowych wersji dostarczonych systemów w terminach uzgodnionych z Zamawiającym	Status zgłoszenia	Maksymalny czas naprawy	Błąd krytyczny	4 dni robocze od momentu zarejestrowania zgłoszenia błędu	Błąd zwykły	21 dni roboczych od momentu zarejestrowania zgłoszenia błędu.	Modyfikacja	czas dokonania i udostępnienia Zamawiającemu modyfikacji będzie każdorazowo uzgadniany pomiędzy Wykonawcą i Zamawiającym.
Status zgłoszenia	Maksymalny czas naprawy								
Błąd krytyczny	4 dni robocze od momentu zarejestrowania zgłoszenia błędu								
Błąd zwykły	21 dni roboczych od momentu zarejestrowania zgłoszenia błędu.								
Modyfikacja	czas dokonania i udostępnienia Zamawiającemu modyfikacji będzie każdorazowo uzgadniany pomiędzy Wykonawcą i Zamawiającym.								
7)	Usługi serwisu gwarancyjnego świadczone będą w siedzibie Zamawiającego lub zdalnie po podpisaniu zasad zdalnego dostępu								
8)	W przypadku realizacji wsparcia gwarancyjnego w formie dostępu zdalnego realizowane może być wyłącznie przez osoby upoważnione przez Wykonawcę. Osoby te otrzymają możliwość zdalnego dostępu do zasobów informatycznych Zamawiającego zgodnie z zasadami określonymi poniżej: § 1. Udostępnienie - W celu realizacji usług o których mowa w § Umowy, zdalny dostęp zostanie udostępniony Wykonawcy przez Zamawiającego w terminie uzgodnionym przez Strony. - Dostęp zdalny ustanawiany jest tylko i wyłącznie do systemów Zamawiającego stanowiących przedmiot umowy.								

	3. Dostęp zdalny jest możliwy tylko i wyłącznie za pośrednictwem danych autoryzacyjnych udostępnionych Wykonawcy przez Zamawiającego. 4. Zamawiający zobowiązuje się do zapewnienia sprawnego kanału komunikacji. 5. Zamawiający ogranicza zasoby dostępne dla sesji zdalnej do niezbędnego minimum § 2. Zasady korzystania 1. Korzystając ze Zdalnego Dostępu Wykonawca: a. będzie wykorzystywał Zdalny Dostęp wyłącznie w celu realizacji przedmiotu umowy; b. nie będzie pozyskiwał ani przetwarzał żadnych innych danych, za wyjątkiem danych niezbędnych do realizacji przedmiotu umowy; 2. Wykonawca może wnioskować o dane autoryzacyjne tylko i wyłącznie dla osób wykazanych w imiennym wykazie osób upoważnionych do zdalnego dostępu. 3. Zabrania się Wykonawcy przekazywania danych autoryzacyjnych innym osobom niż osoby wskazane w imiennym wykazie osób upoważnionych. 4. Wykonawca jest zobowiązany do niezwłocznego poinformowania Zamawiającego o zaprzestaniu wykonywania usług będących przedmiotem umowy przez pracownika posiadającego dostęp zdalny § 3. Warunki Techniczne do uzyskania Zdalnego Dostępu 1. Zamawiający zapewni bezpieczny kanał VPN; 2. Jeżeli zdalny dostęp przez Wykonawcę musi być realizowany z wykorzystaniem oprogramowania nie będącego w posiadaniu Zamawiającego. Wykonawca na własny koszt dostarczy legalne oprogramowanie Zamawiającemu. Oprogramowanie to musi działać tylko i wyłącznie poprzez udostępniony przez Zamawiającego kanał VPN. 3. Zamawiający nie dopuszcza oprogramowania wykorzystującego obce serwery pośredniczące do komunikacji pomiędzy stronami Umowy 4. Zamawiający przekaze osobie realizującej prace wynikające z zapisów Umowy dane autoryzacyjne a. identyfikator użytkownika (login) b. hasło dostępu c. parametry niezbędne do zestawienia zdalnego połączenia. 5. Użytkownicy po stronie Wykonawcy zobowiązują się do nieudostępniania danych autoryzacyjnych innym osobom oraz wykorzystywania dostępu wyłącznie w celu realizacji niniejszej Umowy. 6. Instalacja oraz konfiguracja przekazanego oprogramowania leży po stronie pracowników Wykonawcy.
--	--

WARUNKI REALIZACJI USŁUGI DOSTĘPU DO DANYCH POPRZECZ CHMURĘ PRYWATNĄ	
Zamawiający wymaga zapewnienia usługi dostępu do danych poprzez chmurę prywatną zgodnie z następującymi minimalnymi wymaganiami:	
1)	Wykonawca zapewni dostęp do usługi przez okres minimum 24/36 miesięcy , który rozpoczyna się w dniu podpisania protokołu końcowego udostępnienia usługi
2)	Wykonawca zapewni Zamawiającemu wsparcie techniczne dla udostępnionej usługi w dni robocze od poniedziałku do piątku w godzinach 8.00-16.00 z wyjątkiem dni ustawowo wolnych od pracy.
3)	Wymagany zakres wsparcia technicznego dla dostarczonej usługi: • Usuwanie wszelkich błędów udostępnionego w ramach usługi oprogramowania • Instalowanie i wdrożenia nowych wersji udostępnionego w ramach usługi oprogramowania • Usuwanie wszelkich awarii udostępnionego w ramach usługi oprogramowania • Zapewnienie prawidłowego współdziałania udostępnionego w ramach usługi oprogramowania z ZSI • Bieżące optymalizowanie konfiguracji udostępnionego w ramach usługi oprogramowania z uwzględnieniem potrzeb Zamawiającego.
4)	Wykonawca gwarantuje funkcjonowanie usługi w trybie 24/7/365 oraz jej dostępność na poziomie 99,5% w skali miesiąca kalendarzowego.
5)	Możliwość zgłaszania przez Zamawiającego błędów dotyczących funkcjonowania udostępnionego w ramach usługi oprogramowania, przy czym Zamawiający może zgłaszać następujące typy błędów:

	• BŁĄD/AWARIA KRYTYCZNA – taka, która uniemożliwia użytkowanie udostępnionego w ramach usługi oprogramowania (w zakresie jego podstawowej funkcjonalności wskazanej w dokumentacji użytkownika) i prowadzi do zatrzymania jego eksploatacji, utraty danych lub naruszenia ich spójności. • BŁĄD ZWYKŁY – taki, który nie wpływa na pracę całego systemu								
6)	Zgłaszanie awarii/błędów przez Zamawiającego odbywać się będzie poprzez: • witrynę internetową Wykonawcy oraz telefonicznie • za pomocą poczty elektronicznej na adres oraz telefonicznie W przypadku, gdy zgłoszenie zostanie przyjęte przez Wykonawcę: • w godzinach pomiędzy 16.00 a 24.00 dnia roboczego – traktowane jest jak przyjęte o godz. 8.00 następnego dnia roboczego, • w godzinach pomiędzy 0.00 a 8.00 dnia roboczego - traktowane jest jak przyjęte o godz. 8.00 danego dnia roboczego, • w dniu ustawowo lub dodatkowo wolnym od pracy - traktowane jest jak przyjęte o godz. 8.00 najbliższego dnia roboczego.								
7)	Czasy usunięcia błędów/awarii (krytycznych, zwykłych) wykrytych w udostępnionego w ramach usługi oprogramowaniu określono w tabeli poniżej: <table border="1"> <thead> <tr> <th>Status zgłoszenia</th><th>Maksymalny czas naprawy</th></tr> </thead> <tbody> <tr> <td>Awaria /Błąd krytyczny</td><td>1 dzień roboczy od momentu zarejestrowania zgłoszenia błędu</td></tr> <tr> <td>Błąd zwykły</td><td>7 dni roboczych od momentu zarejestrowania zgłoszenia błędu.</td></tr> <tr> <td>Inne</td><td>dostarczanie i instalacja uaktualnień, poprawek i nowych wersji dostarczonych systemów w terminach uzgodnionych z Zamawiającym</td></tr> </tbody> </table>	Status zgłoszenia	Maksymalny czas naprawy	Awaria /Błąd krytyczny	1 dzień roboczy od momentu zarejestrowania zgłoszenia błędu	Błąd zwykły	7 dni roboczych od momentu zarejestrowania zgłoszenia błędu.	Inne	dostarczanie i instalacja uaktualnień, poprawek i nowych wersji dostarczonych systemów w terminach uzgodnionych z Zamawiającym
Status zgłoszenia	Maksymalny czas naprawy								
Awaria /Błąd krytyczny	1 dzień roboczy od momentu zarejestrowania zgłoszenia błędu								
Błąd zwykły	7 dni roboczych od momentu zarejestrowania zgłoszenia błędu.								
Inne	dostarczanie i instalacja uaktualnień, poprawek i nowych wersji dostarczonych systemów w terminach uzgodnionych z Zamawiającym								