

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest **dostawa Systemu teleporad.**

I. **Termin realizacji zamówienia** – wdrożenie: **do 40 dni roboczych**, okres udostępnienia systemu: 24 miesiące od wdrożenia.

II. **Gwarancja.**

Gwarancja na system będzie świadczona przez okres 24 miesięcy od daty wdrożenia.

III. **Dokumentacja.**

Dostawca wytworzy i dostarczy Zamawiającemu:

1. Dokumentację użytkownika
2. Dokumentację analityczną
3. Dokumentację techniczną

IV. **Ogólny opis systemu.**

System ma umożliwiać przeprowadzenie telekonferencji pomiędzy pracownikiem medycznym, a pacjentem. System będzie zintegrowany z systemem informatycznym Zamawiającego, który będzie zarządzał grafikami / kalendarzami i inicjował udostępnienie danych do połączenia z systemu teleporad do pracownika medycznego i pacjenta. System teleporad ma umożliwiać jednoczesną pracę do maksymalnie 20 000 połączeń pracownik medyczny – pacjent. Zamawiający musi mieć możliwość zmiany osób do których przypisane są licencje. System teleporad musi obsługiwać połączenia audio/wideo i telefoniczne. Rozwiązanie musi dopuszczać możliwość dołączenia którejkolwiek ze stron (pracownik medyczny/pacjent) w trybie audio lub audio i video. System został podzielony na 3 obszary:

1. Moduł pracownika medycznego – interfejs udostępniony lekarzowi świadczącemu usługę telekonferencji.
2. Moduł pacjenta / osoby dołączającej – interfejs udostępniony pacjentowi lub osobie dołączającej do spotkania.
3. Moduł zarządzający – funkcjonalności przeznaczone dla administratora Systemu.

System zainstalowany będzie na infrastrukturze Dostawcy i udostępniony Zamawiającemu jako usługa typu SaaS. Komunikacja z systemem informatycznym Zamawiającego musi być zabezpieczona za pomocą dedykowanego kanału komunikacyjnego lub za pomocą odpowiednich reguł dostępowych. Zamawiający może wyrazić zgodę na instalację części Systemu na infrastrukturze Zamawiającego, jeśli taka potrzeba wyniknie z analizy przedwdrożeniowej i nie będzie znacząco wpływała na użycie infrastruktury Zamawiającego.

V. **Wdrożenie.**

Uruchomienie Systemu musi być poprzedzone pracami analitycznymi w ramach których doprecyzowane zostaną m.in. przypadki użycia, interfejsy z systemem informatycznym Zamawiającego, wymagania dotyczące interfejsu użytkownika.

VI. Wymagania funkcjonalne.

1. Moduł pracownika medycznego

- a. Aplikacja responsywna www pozwalająca na pracę zarówno na PC jak i na urządzeniach mobilnych (Android / iOS).
- b. Zalogowanie pracownika medycznego do aplikacji (identyfikacja).
- c. Obsługa komunikacji tekstowej (chat) – także z osobami znajdującymi się w poczekalni.
- d. Obsługa komunikacji głosowej.
- e. Obsługa komunikacji wideo.
- f. Możliwość przesyłania plików.
- g. Przełączenie się na użytkownika aktualnie zabierającego głos (widok aktywnego rozmówcy).
- h. Możliwość wyświetlania w jednym oknie wszystkich uczestników teleporady.
- i. Możliwość wyboru i konfiguracji urządzeń audio/wideo (mikrofon, kamera, głośniki urządzenia).
- j. Włączenie / wyłączenie kamery.
- k. Możliwość włączenia / wyłączenia mikrofonu.
- l. Możliwość regulacji głośności.
- m. Możliwość udostępnienia ekranu (możliwość wyboru ekranu przy zastosowaniu wielu ekranów) lub okna.
- n. Możliwość wyciszenia pacjenta.
- o. Możliwość usunięcia pacjenta.
- p. Możliwość zakończenia spotkania.
- q. Obsługa poczekalni - wpuszczenie oczekującego pacjenta do spotkania.
- r. Możliwość zawieszenia rozmowy.
- s. Sygnalizacja nowej wiadomości chat.
- t. Wyświetlanie informacji o jakości połączenia.
- u. Możliwość ustawienia wirtualnego tła.
- v. Możliwość zmiany hasła.

2. Moduł pacjenta / osoby dołączającej

- a. Aplikacja responsywna www pozwalająca na pracę zarówno na PC jak i na urządzeniach mobilnych (Android / iOS).
- b. Widok stanu konsultacji poczekalnia / teleporada.
- c. Obsługa komunikacji tekstowej (chat).
- d. Obsługa komunikacji głosowej.



- e. Obsługa komunikacji wideo.
- f. Możliwość przesyłania plików.
- g. Przełączenie się na użytkownika aktualnie zabierającego głos (widok aktywnego rozmówcy).
- h. Możliwość wyświetlania w jednym oknie wszystkich uczestników teleporady.
- i. Możliwość wyboru i konfiguracji urządzeń audio/wideo (mikrofon, kamera, głośniki urządzenia).
- j. Włączenie / wyłączenie kamery.
- k. Możliwość włączenia / wyłączenia mikrofonu.
- l. Możliwość regulacji głośności.
- m. Możliwość udostępnienia ekranu (możliwość wyboru ekranu przy zastosowaniu wielu ekranów) lub okna.
- n. Możliwość opuszczenia spotkania.
- o. Sygnalizacja nowej wiadomości chat.
- p. Możliwość udziału w telekonferencji za pomocą przeglądarki internetowej.
- q. Wyświetlanie informacji o jakości połączenia.
- r. Możliwość ustawienia wirtualnego tła.
- s. Przesłanie wiadomości o ocenie pracownika medycznego.
- t. Przesłanie wiadomości o jakości połączenia.

3. Moduł zarządzający

- a. Administrowanie rolami - pracownikami medycznymi. W tym m.in.: zarządzanie uprawnieniami, zarządzanie hasłami, blokowanie).
- b. Możliwość importu z pliku wielu kont pracowników medycznych jednocześnie.
- c. Moduł raportowania
 - i. Online – dostępność/zajętość pokoi w danym momencie oraz info historyczne z konkretnej daty - definiowalne interwały czasowe
 - ii. Billing, liczba teleporad w zadanym okresie z podziałem na odbyte/ nieodbyte.
 - iii. Czas trwania teleporad w zadanym okresie (czas sumaryczny, średni czas trwania teleporady, z podziałem na pracownika medycznego/pacjenta/placówka/obszar geograficzny itp.)
 - iv. liczba/czas teleporad z użyciem linku, z użyciem połączenia telefonicznego.
 - v. Czas oczekiwania pacjenta w poczekalni od momentu rozpoczęcia teleporady (oczekiwanie na pracownika medycznego).
 - vi. Czas oczekiwania pracownika medycznego w poczekalni od momentu rozpoczęcia teleporady (oczekiwanie na pacjenta).

4. Wymaganie ogólne:

- a. Teleporada będzie aktywna na 30 minut przed rozpoczęciem zaplanowanej teleporady. Możliwość zmiany parametru czasowego.
- b. Możliwość ustawienia komunikatu dla pacjenta po wejściu do poczekalni.
- c. Możliwość ustawienia komunikatu dla pacjenta po wejściu w link wcześniej niż 30 min przed rozpoczęciem teleporady.
- d. Zamknięcie teleporady po 8 godzinach od zakończenia teleporady.
- e. Możliwość ustawienia komunikatu dla użytkownika po wejściu w link teleporady, która już się zakończyła.
- f. Numer telefoniczny na który będzie możliwość wdzwonienia do teleporady będzie ustalony przez Zamawiającego (numer komórkowy, AUS – 19xyz).

5. Integracja z systemem Zamawiającego

5.1. System musi komunikować się z systemem informatycznym Zamawiającego za pomocą usług sieciowych (web service). System informatyczny Zamawiającego będzie co najmniej:

- a. Wysyłał żądania utworzenia / usunięcia / modyfikacji pokoju na potrzeby teleporady.
- b. Wysyłał żądania pobrania danych niezbędnych do połączenia się z teleporadą (link, nr. telefonu, pin itp.).
- c. Możliwość wykorzystania zewnętrznego katalogu użytkowników (pracowników medycznych).

5.2. Dostarczony System będzie miał możliwość:

- a. Utworzenie teleporady i wysyłania informacji niezbędnych do połączenia się z teleporadą pracownika medycznego (link, pin, identyfikator itp.). Przesłany link może być wykorzystany przez kilka osób (maksymalnie 5).
- b. Utworzenie teleporady i wysyłania informacji niezbędnych do połączenia się z teleporadą pacjenta (link, pin, itp.). Przesłany link może być wykorzystany przez kilka osób (maksymalnie 5).
- c. Wysyłania wygenerowanego raportu.
- d. Modyfikacji teleporady.
- e. Odwołania teleporady za pomocą linku przesłanego do systemu Zamawiającego

5.3. Szczegółowa lista oraz specyfikacja interfejsów zostanie ustalona na etapie analizy przedwdrożeniowej.

6. Wymagania niefunkcjonalne

- a. Dostarczone rozwiązanie musi być oparte o silnik, który działa jako usługa zewnętrzna i jest wykorzystywane przez co najmniej 100 000 użytkowników i organizowane jest za jego pomocą co najmniej 200 000 spotkań rocznie.
- b. Wysoka dostępność i skalowalność rozwiązania musi być zapewniona poprzez rozproszoną globalnie infrastrukturę.
- c. Platforma na której będzie działał system musi być zgodna z certyfikatami: ISO 27001, ISO 27017, ISO 27018.

- d. Możliwość udziału w telekonferencji za pomocą komputera, telefonu stacjonarnego, urządzeń mobilnych poprzez sieci WLAN, 3G/4G oraz LTE.
- e. Możliwość przeprowadzania do maksymalnie 20 000 jednoczesnych połączeń audio/wideo lub telefonicznych. Zastosowane zostaną następujące progi:
 - i. Max. 2000 jednoczesnych połączeń – od startu systemu
 - ii. Max. 5000 jednoczesnych połączeń – od dnia wskazanego przez Zamawiającego
 - iii. Max. 10000 jednoczesnych połączeń – od dnia wskazanego przez Zamawiającego
 - iv. Max. 15000 jednoczesnych połączeń – od dnia wskazanego przez Zamawiającego
 - v. Max. 20000 jednoczesnych połączeń – od dnia wskazanego przez Zamawiającego

W oparciu o dotychczasowe doświadczenia Zamawiający szacuje rozkład ruchu: 60% połączenia telefoniczne, 40% połączenia internetowe w przypadku połączeń pacjentów. Pracownicy medyczni będą wykorzystywali tylko połączenia internetowe.

- f. System nie będzie przechowywał żadnych danych wymienianych pomiędzy pracownikiem medycznym a pacjentem. Historia wiadomości tekstowych oraz przesłanych plików będzie usuwana po wygaśnięciu pokoju.
- g. Możliwość założenia nieograniczonej liczby kont pracowników medycznych.
- h. Dostępność systemu na poziomie **min.** 99,5% w skali miesiąca.
- i. Realizacja połączeń klient – klient z jakością 720p oraz 30 klatkach na sekundę (fps), przy połączeniu sieciowym 2 Mbps.
- j. Automatyczne dostosowywanie jakości wideo do jakości połączenia sieciowego.
- k. System musi zapewnić szyfrowanie połączenia odbywającego się za pomocą sieci Internet zgodnie ze standardami: TLS 1.2, AES 128, AES 256.
- l. Dostępność systemu na urządzeniach mobilnych: Android 10 lub nowszymi, iOS 14 lub nowszymi.
- m. Obsługa przez przeglądarki Google Chrome 65 lub nowsze, Firefox 48 lub nowsza, Microsoft Edge 25 lub nowsza, Safari 11 lub nowsza w wersjach stacjonarnych i mobilnych.
- n. Organizacja spotkania wirtualnego może się odbyć poprzez zestawienie konferencji webowej na bazie aplikacji lub przeglądarki internetowej w trybie, który umożliwi uczestnictwo osobom nie posiadającym dostępu administratora do swojego komputera bez konieczności instalacji żadnych aplikacji lub wtyczek wymagających uprawnień administratora do komputera.
- o. System musi być dostępny przynajmniej w języku polskim oraz angielskim.
- p. Możliwość nagrania przedzapowiedzi w systemie audio/video i IVR: o RODO, Instrukcji postępowania, regulaminów/warunków korzystania, oświadczeń, spotów informacyjnych itp.

7. Wymagania bezpieczeństwa

- a. System, ze względu na fakt, że będzie przetwarzał wrażliwe dane medyczne, musi spełniać wymagania dla aplikacji www zdefiniowane w standardzie OWASP (Open Web Application Security Project) Application Security Verification Standard (ASVS) w wersji 4.0.2 na poziomie 3.
- b. System musi zapewniać poufność, integralność oraz dostępność wszystkich przesyłanych danych „in-transit” z wykorzystaniem mocnych algorytmów i funkcji kryptograficznych, tj., min. TLS 1.2+, funkcje haszujące z rodziny SHA2 i być zgodny z wymaganiami ASVS.
- c. Przechowywane dane „at-rest” muszą być szyfrowane z wykorzystaniem algorytmu AES-256 lub równie mocnego. Dotyczy to jakichkolwiek danych przechowywanych po stronie Zamawiającego i danych u Dostawcy usługi (SaaS).
- d. System musi wykorzystywać szyfrowanie przy komunikacji pomiędzy wszystkimi komponentami.
- e. Poszczególne komponenty Systemu muszą być wyizolowane od siebie minimum na poziomie logicznym.
- f. Wszystkie zależne komponenty niezbędne do działania Systemu (np. system operacyjny, serwer www, biblioteki itp.) powinny być skonfigurowane zgodnie z najlepszymi praktykami bezpieczeństwa oraz uszczelnione w zakresie konfiguracji (hardening usługi, serwerów).
- g. Wszystkie dodatkowe komponenty użyte w Systemie nie będące utworem dostawcy (np. biblioteki open source, wtyczki, pluginy) powinny być sprawdzone pod kątem bezpieczeństwa, w zakresie potencjalnej eksfiltracji danych,
- h. System musi zapewnić proces uwierzytelnienia oraz autoryzacji w dostępie do danych. W szczególności każdy dostęp użytkownika do danych osobowych lub wrażliwych będzie wymagał uwierzytelnienia.
- i. System powinien zapewniać integrację w zakresie uwierzytelnienia z systemem po stronie Zamawiającego, tj. Active Directory.
- j. Proces uwierzytelnienia dla kont uprzywilejowanych/wysokich uprawnień powinien wspierać MFA (Multi Factor Authentication).
- k. System powinien posiadać mechanizm uprawnień oparty na rolach (tzw. Role Base Access Control – RBAC).
- l. System powinien zapewniać mechanizmy zarządzania sesją zgodne z ASVS.
- m. Role nie powinny być przypisywane bezpośrednio konkretnym osobom lecz uprawnienia powinny być grupowane w zbiory przypisane do ról w systemie.
- n. Baza danych powinna zapewniać separację danych – podział danych na dwie części – odseparowanie danych wrażliwych (niosących w sobie informacje identyfikujące) od pozostałych danych.
- o. System musi umożliwiać wielu użytkownikom równoległy dostęp do tych samych danych lub obszarów funkcjonalnych bez utraty integralności danych
- p. System musi zapewnić mechanizmy bezpiecznego usuwania danych wrażliwych.

- q. Jeśli System będzie umożliwiał zdalne wgranie plików (upload) przez użytkownika, to takie pliki należy wcześniej sprawdzić pod kątem akceptowalnego formatu danych, występowania wirusów, malware, złośliwego kodu w załączanych plikach.
- r. System musi tworzyć i utrzymywać log systemu, rejestrujący historię logowania do systemu wszystkich użytkowników (w tym użytkowników uprzywilejowanych) oraz wykonane przez nich czynności wprowadzania, modyfikacji i usuwania danych. Zakres danych, które powinny podlegać takiemu audytowi/logowaniu zostanie określony na etapie analizy przedwdrożeniowej.
- s. Interfejsy integracyjne pomiędzy infrastrukturą Zamawiającego a infrastrukturą Dostawcy (np. API) muszą zapewnić proces wzajemnego uwierzytelnienia stron (mTLS) wykorzystując silną kryptografię.
- t. Aplikacja powinna wykazywać ochronę przed atakami typu XSS (Cross Site Scripting), SQL Injection, CSRF (Cross-Site Request Forgery), zafiksowanie sesji (Session Fixation).
- u. Powinny być skonfigurowane nagłówki bezpieczeństwa HTTP, w szczególności (X Frame Options, X XXS Protection, X Content Type Options, X Permitted Cross Domain Policies, Strict Transport Security, Content Security Policy, Rererrer Policy) w zakresie oczekiwanej funkcjonalności.
- v. Powinien istnieć mechanizm współdzielenia zasobów między źródłami (CORS),
- w. Dostawca powinien dostarczyć raport z testów bezpieczeństwa Systemu oraz aplikacji www i mobilnych zgodnie z wytycznymi OWASP ASVS L3 w zakresie funkcjonalnym Systemu.