Załącznik nr 2 - Wymagania bezpieczeństwa systemu interaktywnej bazy wiedzy wspierającej pracę lekarza

Spis treści

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37NIP: 5251575309
biuro@cez.gov.pl | www.cez.gov.pl
REGON: 001377706

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU
Ministerstwo Zdrowia

Wymagania regulacyjne

Kod wymagania	Opis wymagania
NFUN-B-REG-01	Zapewnienie zgodności z zapisami Data Protection Impact Assessment (DPIA). Przed wdrożeniem rozwiązania Wykonawca jest zobowiązany do dostarczenia informacji niezbędnych do przeprowadzenia oceny skutków dla ochrony danych (art. 35 RODO), w tym szczegółowego opisu operacji przetwarzania, planowanych środków bezpieczeństwa oraz analizy ryzyka dla praw i wolności osób fizycznych.
NFUN-B-REG-02	Wykonawca musi posiadać certyfikat ISO 27001 lub równoważny dokument potwierdzający funkcjonowanie systemu zarządzania bezpieczeństwem informacji adekwatnego do zakresu świadczonej usługi. Za równoważny dokument Zamawiający uzna dokument potwierdzający wdrożenie i stosowanie u Wykonawcy systemu zarządzania bezpieczeństwem informacji obejmującego co najmniej: • politykę bezpieczeństwa informacji, • zarządzanie ryzykiem w obszarze bezpieczeństwa informacji, • zarządzanie incydentami bezpieczeństwa, • kontrolę dostępu do informacji i systemów, • zarządzanie ciągłością działania, • okresowy przegląd i doskonalenie stosowanych środków bezpieczeństwa. • Dokument potwierdzający spełnienie wymagania musi zostać dołączony do oferty Wykonawcy.
NFUN-B-REG-03	System, w zakresie w jakim wykorzystuje komponenty AI/LLM, musi być zgodny z przepisami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1689 (AI Act) w zakresie adekwatnym do funkcji realizowanych przez System oraz do jego faktycznej klasyfikacji prawnej. Zastosowane komponenty AI nie mogą być wykorzystywane w sposób wykraczający poza funkcję informacyjno-edukacyjną Systemu określoną w OPZ.
NFUN-B-REG-04	W zakresie, w jakim System przetwarza dane osobowe, w szczególności dane użytkowników, administratorów, identyfikatory techniczne, dane związane z uwierzytelnianiem, autoryzacją, bezpieczeństwem i rozliczalnością działania Systemu, Wykonawca musi zapewnić zgodność działania rozwiązania z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO).

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37NIP: 5251575309
biuro@cez.gov.pl | www.cez.gov.pl
REGON: 001377706

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU
Ministerstwo Zdrowia

NFUN-B-REG-05	Na żądanie Zamawiającego Wykonawca przekaże dokumentację opisującą zasady działania komponentów AI/LLM zastosowanych w Systemie, w szczególności: opis architektury rozwiązania, zakres wykorzystania modeli, ograniczenia funkcjonalne, sposób ochrony danych, mechanizmy zapewniające powtarzalność i weryfikowalność odpowiedzi, sposób powiązania odpowiedzi ze źródłami wiedzy oraz środki ograniczające ryzyko generowania treści niezgodnych z OPZ. Zakres dokumentacji musi być adekwatny do faktycznej klasyfikacji prawnej rozwiązania.
NFUN-B-REG-06	System musi spełniać minimalne wymagania technicznoorganizacyjne dla systemów usługodawców ezdrowia (CeZ) określone w Załączniku ZSZ_SZBI_ISO_P_A_15._Polityka-bezpieczeństwa-informacji-dla-wykonawcow_IP_v.1. 2.pdf. https://www.cez.gov.pl/sites/default/files/paragraph.attachments.field_attachments/2024-11/Polityka-Bezpieczenstwa-Informacji-dla-wykonawcow_IP_v.1.2.pdf - organizacyjne dla systemów usługodawców e-zdrowia (CeZ)
NFUN-B-REG-07	Wykonawca musi zapewnić i utrzymywać zgodność Systemu z wymaganiami prawnymi i regulacyjnymi mającymi zastosowanie do oferowanego rozwiązania przez cały okres trwania umowy.

Wymagania ogólne bezpieczeństwa

Kod wymagania	Wymaganie
NFUN-B-O-01	Wszystkie połączenia pomiędzy modułami Systemu i modułami a systemami CeZ muszą używać TLS 1.3 z HSTS, cert pinning.
NFUN-B-O-02	System musi być wolny od wszelkich ryzyk/podatności opisanych w OWASP Top10:2025 i OWASP API Security Project odpowiednio dla części aplikacyjnej i API. System musi być wolny od potwierdzonych podatności w bazie programu CVE™, który kataloguje publicznie ujawnione podatności cyberbezpieczeństwa. System nie może zawierać podatności sklasyfikowanych jako L1 OWASP ASVS v5.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37NIP: 5251575309
biuro@cez.gov.pl | www.cez.gov.pl
REGON: 001377706

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU
Ministerstwo Zdrowia

NFUN-B-O-03	Interfejs graficzny Systemu, jeśli jest dostarczany przez Wykonawcę, musi spełniać wymagania dostępności cyfrowej zgodnie z WCAG 2.1 na poziomie co najmniej AA, zgodnie z wymaganiami OPZ.

Wymagania bezpieczeństwa dotyczące architektury

Niezależne od modelu oferowanej usługi

Kod wymagania	Opis wymagania
NFUN-B-A-05	przypadku oferowania Systemu w modelu SaaS, System musi być utrzymywany w architekturze wysokiej dostępności (HA), adekwatnej do wymagań SLA określonych w dokumentacji zamówienia. Szczegółowy model realizacji wysokiej dostępności zostanie opisany przez Wykonawcę w ofercie lub na etapie Analizy Przedwdrożeniowej.
NFUN-B-A-07	W przypadku oferowania Systemu w modelu SaaS Wykonawca musi zapewnić skuteczną izolację danych, konfiguracji oraz uprawnień Zamawiającego od innych klientów, uniemożliwiając dostęp pomiędzy środowiskami klientów. Zastosowany model izolacji musi być opisany przez Wykonawcę i podlega akceptacji Zamawiającego.

Wymagania bezpieczeństwa w zakresie infrastruktury

Kod wymagania	Opis wymagania
NFUN-B-I-01	W przypadku utrzymywania przez Wykonawcę Systemu w chmurze, infrastruktura chmurowa powinna spełniać wymagania SCCO adekwatne do charakteru przetwarzania oraz modelu świadczenia usługi, zgodnie z wymaganiami Zamawiającego uzgodnionymi na etapie Analizy Przedwdrożeniowej.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37NIP: 5251575309
biuro@cez.gov.pl | www.cez.gov.pl
REGON: 001377706

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU
Ministerstwo Zdrowia

Wymagania w stosunku do komponentów LM/LLM/A

Kod wymagania	Wymaganie
NFUN-B-ML-01	System nie może wykorzystywać danych pochodzących z zapytań użytkowników Zamawiającego do retrainingu, fine-tuningu, budowy dodatkowych zasobów wiedzy ani tworzenia mechanizmów RAG wykraczających poza zakres usługi świadczonej na rzecz Zamawiającego. Dopuszczalne jest wykorzystywanie zagregowanych danych technicznych wyłącznie w zakresie niezbędnym do zapewnienia bezpieczeństwa, monitoringu, rozliczalności i utrzymania usługi, bez możliwości identyfikacji użytkownika lub odtworzenia treści zapytań.
NFUN-B-ML-02	W przypadku świadczenia usługi w modelu SaaS Wykonawca musi zapewnić, że dane pochodzące z zapytań użytkowników oraz techniczne dane sesyjne są przechowywane wyłącznie przez okres niezbędny do realizacji usługi, bezpieczeństwa i rozliczalności, zgodnie z uzgodnioną polityką retencji. Dane te nie mogą być wykorzystywane do trenowania, dostrajania ani rozwijania modeli poza zakresem świadczenia usługi na rzecz Zamawiającego. Dane wejściowe, pośrednie i wyjściowe nie mogą być odkładane w logach ani backupach systemu Wykonawcy w sposób wykraczający poza uzgodniony zakres logowania i rozliczalności.
NFUN-B-ML-03	System musi realizować sanityzację wejścia i wyjścia dla modułu konwersacyjnego AI. Parametry sanityzacji muszą być konfigurowalne przez Zamawiającego w zakresie uzgodnionym na etapie Analizy Przedwdrożeniowej. Sanityzacja powinna obejmować co najmniej: wykrywanie prób prompt injection/jailbreak, ograniczanie zapytań niezwiązanych z funkcją Systemu, blokowanie generowania treści wykraczających poza zakres bazy wiedzy, blokowanie generowania indywidualnych zaleceń terapeutycznych dla konkretnego lub hipotetycznego pacjenta oraz kontrolę długości zapytań i odpowiedzi.
NFUN-B-ML-04	System musi eksportować do systemu logów Zamawiającego metadane techniczne dotyczące działania modułu AI, w szczególności: identyfikator lub wersję użytego modelu, czas odpowiedzi, identyfikator sesji, identyfikator zapytania, informacje o wykorzystanych mechanizmach bezpieczeństwa oraz status wykonania operacji. Zakres eksportowanych danych nie może obejmować danych pacjentów ani treści wykraczających poza uzgodniony zakres logowania.
NFUN-B-ML-05	Moduły Systemu zawierające komponenty LLM muszą być przetestowane pod kątem podatności opisanych w OWASP Top 10 for LLM Applications lub równoważnym aktualnym standardzie bezpieczeństwa dla systemów opartych o modele języków.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37NIP: 5251575309
biuro@cez.gov.pl | www.cez.gov.pl
REGON: 001377706

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU
Ministerstwo Zdrowia

Wymagania dotyczące procesu uwierzytelniania i dostępu

Kod Wymagania	Opis wymagania
NFUN-B-S-01	System musi umożliwiać zarządzanie dostępem do kont administracyjnych, w szczególności nadawanie, zmianę oraz odbieranie uprawnień przez Zamawiającego lub na jego zlecenie. W przypadku modelu wdrożenia wymagającego integracji z mechanizmami tożsamości Zamawiającego, szczegółowy sposób realizacji zostanie uzgodniony na etapie Analizy Przedwdrożeniowej.
NFUN-B-S-02	System musi umożliwiać zarządzanie rolami i uprawnieniami użytkowników zgodnie z modelem RBAC

Wymagania dotyczące procesu wdrożenia

Kod Wymagania	Opis wymagania
NFUN-B-P-01	Przed wdrożeniem Wykonawca opracuje model zagrożeń zgodnie z metodyką PASTA lub STRIDE oraz na tej podstawie zaproponuje zmiany ograniczające zagrożenia do poziomu Niski (CVSS < 3.0). Sposób oceny podatności powinien być zgodny z CVSS Common Vulnerability Scoring System.
NFUN-B-P-02	Komponenty użyte do opracowania systemu na dzień odbioru Systemu nie mogą posiadać znanych podatności na poziomie wyższym niż Niski CVSS ver 4.0 < 3.0).
NFUN-B-P-03	Sposób realizacji zadań oraz zabezpieczenia dostarczonych systemów muszą spełniać wymagania opisane w Załączniku ZSZ_SZBI_ISO_P_A_15._Polityka-bezpieczeństwa-informacji-dla-wykonawcow_IP_v.1. 2.pdf.
NFUN-B-P-04	Wykonawca przed odbiorem przetestuje System w sposób opisany OWASP Application Security Verification Standard (ASVS) | OWASP Foundation. Level 2 Wersja 5 . Podatności na poziomie średnim i wyższym wykryte podczas testów Wykonawca musi usunąć na własny koszt a następnie powtórzyć procedurę testów.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37NIP: 5251575309
biuro@cez.gov.pl | www.cez.gov.pl
REGON: 001377706

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU
Ministerstwo Zdrowia

Wymagania dotyczące wprowadzania zmian

Kod Wymagania	Wymaganie
NFUN-B-Z-01	Wykonawca jest zobowiązany do aktualizacji modułów wnioskowania, analizy, ML, LLM przez cały czas trwania Umowy. tak aby ich wersje odzwierciedlały postępy w nauce w tych obszarach. Aktualizacje powinny być realizowane co najmniej raz w roku
NFUN-B-Z-02	System musi realizować proces zatwierdzania zmian obejmujący co najmniej: zgłoszenie zmiany, ocenę wpływu na bezpieczeństwo, funkcjonalność, integralność i dostępność Systemu, wdrożenie testowe, testy regresji, zatwierdzenie przez Zamawiającego oraz wdrożenie produkcyjne. Wymaganie dotyczy wszystkich komponentów Systemu, niezależnie od modelu świadczenia usługi, w tym komponentów AI/LLM, jeżeli są wykorzystywane. Wszelkie zmiany wymagają akceptacji Zamawiającego w zakresie uzgodnionym w Umowie.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37NIP: 5251575309
biuro@cez.gov.pl | www.cez.gov.pl
REGON: 001377706

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU
Ministerstwo Zdrowia