(261511)

# Wymagania bezpieczeństwa systemu/Aplikacji typu Interpreter Badań Laboratoryjnych

## Spis treści





Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

# Wymagania regulacyjne

| Kod wymagania | Opis wymagania |
|---|---|
| NFUN-B-REG-1 | System musi posiadać aktualną certyfikację CE jako wyrobu medycznego klasy IIa/IIb zgodnie z MDR (EU) 2017/745, w tym Dokumentację techniczną potwierdzającą bezpieczeństwo Systemu. |
| NFUN-B-REG-2 | API systemu musi być zgodne ze standardami HL7 FHIR R4 (https://ezdrowie.gov.pl/portal/home/dla-dostawcow/interfejsy) dla wymiany danych medycznych w e-zdrowiu Polska, z profilem bezpieczeństwa . |
| NFUN-B-REG-3 | System musi spełniać wymagania IEC 62304 klasa B/C (software jako significant risk) dla cyklu życia oprogramowania medycznego,<br>Wynik analizy musi zostać dołączony do oferty Wykonawcy. |
| NFUN-B-REG-4 | System musi być zgodny z ISO 14971:2019 (zarządzanie ryzykiem wyrobów medycznych), w tym analiza ryzyka cyberbezpieczeństwa zintegrowana z ryzykiem klinicznym. Wynik analizy musi zostać dołączony do oferty Wykonawcy. |
| NFUN-B-REG-5 | 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-6 | Wykonawca musi posiadać certyfikat ISO 27001 lub równoważny w zakresie obejmującym tworzenie i wdrażanie oprogramowania. Certyfikat musi zostać dołączony do oferty Wykonawcy. |
| NFUN-B-REG-7 | Wykonawca musi posiada certyfikat ISO 13485 lub równoważny w zakresie obejmującym tworzenie i wdrażanie oprogramowania . Certyfikat musi zostać dołączony do oferty Wykonawcy. |
| NFUN-B-REG-8 | System musi spełniać wymagania Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie zharmonizowanych przepisów dotyczących sztucznej inteligencji (tzw. Akt o sztucznej inteligencji – AI Act), jako system wysokiego ryzyka w rozumieniu tego aktu. |
| NFUN-B-REG-9 | Wykonawca jest zobowiązany do współpracy z Zamawiającym w zakresie zgłaszania poważnych incydentów związanych z działaniem systemu, zgodnie z procedurami opisanymi w art. 62 AI Act. |
| NFUN-B-REG-10 | System oraz wszystkie procesy związane z jego działaniem i utrzymaniem muszą być w pełni zgodne z Rozporządzeniem Parlamentu Europejskiego i Radu (UE) 2016/679 (RODO). |
| NFUN-B-REG-11 | Wykonawca jest zobowiązany dostarczenia następujących elementów potwierdzających zgodność z AI Act (poziom 2a):<br>• deklaracji zgodności UE (art. 47),<br>• kompletnej dokumentacji technicznej (art. 11 i załącznik IV),<br>• instrukcji użytkowania dla użytkowników końcowych (art. 13),<br>• potwierdzenia wykonania testów ex-ante (art. 19),<br>• planu i systemu monitorowania po wprowadzeniu do użytku (art. 61), |
| NFUN-B-REG-12 | System musi spełniać minimalne wymagania technicznoorganizacyjne dla systemów usługodawców ezdrowia (CeZ) określone w Załączniku ZSZ_SZBI_ISO_P_A_15._Polityka-bezpieczeństwa-informacji-dla- |



Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

| | |
|---|---|
| | wykonawcow_IP_v.1. 2.pdf - organizacyjne dla systemów usługodawców e-zdrowia (CeZ) |
| NFUN-B-REG-13 | Wykonawca musi zapewnić i aktywnie utrzymywać zgodność modelu ze wszystkimi wymienionymi regulacjami prawnymi przez cały okres trwania umowy. |



Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

# Wymagania ogólne bezpieczeństwa

| ID | Wymaganie |
|---|---|
| NFUN-B-O-01 | System musi realizować pseudonimizację danych wejściowych (wyniki badań, dane uzyskane podczas wywiadu), po stronie infrastruktury CeZ uniemożliwiając re-identyfikację |
| NFUN-B-O-02 | Wszystkie połączenia pomiędzy modułami Systemu i modułami a systemami CeZ muszą używać TLS 1.3 z HSTS, cert pinning i mutual TLS . |
| NFUN-B-O-03 | Dane wejściowe (wyniki badań) i wyjściowe (interpretacje) muszą być szyfrowane w spoczynku (AES-256 GCM) z kluczami zarządzanymi przez Zamawiającego niezależnie od modelu oferowania usługi ( onpremis lub SaaS). |
| NFUN-B-O-04 | System musi walidować integralność wyników interpretacji (cyfrowy podpis/hasz z sygnaturą modelu/version), uniemożliwiając modyfikację bez detekcji. |
| NFUN-B-O-05 | System musi być wolny od wszelkich ryzyk/podatności opisanych w OWASP Top10:2025 i OWASP API Security Project odpowiednio dla części aplikacyjnej i API. |
| NFUN-B-O-06 | Interfejs graficzny (RWD) musi spełniać WCAG 2.1 AA w zakresie bezpieczeństwa (brak client-side vulnerabilities). |
| NFUN-B-O-07 | W przypadku wykorzystania przez Wykonawcę komponentów stron trzecich (w tym open source), Wykonawca jest zobowiązany do dostarczanie pełnej listy użytych komponentów (SBOM – Software Bill of Materials) wraz z ich nazwami, wersjami, licencjami. |
| NFUN-B-O-08 | Wykonawca zapewnia wsparcie do wszystkich komponentów Systemu oraz ich aktualizacje przez cały okres trwania umowy. |



Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

# Wymagania bezpieczeństwa dotyczące architektury

Niezależne od modelu oferowanej usługi

| Kod wymagania | Opis wymagania |
|---|---|
| NFUN-B-A-03 | System musi posiadać moduł umożliwiający ewidencję i statystykę Interpretacji |
| NFUN-B-A-06 | System musi umożliwiać jego odtworzenie w czasie <4h. |
| NFUN-B-A-07 | W przypadku oferowanie przez Wykonawcę systemu SaaS system musi być wdrożony z całkowitą izolacją tenantów (bez części wspólnych dla różnych klientów), uniemożliwiając dostęp do danych pomiędzy klientami klientów. |
| NFUN-B-A-08 | System musi realizować segmentację komponentów (UI/API/LLM/ML/storage/Voice2text/text2Voice) z osobnym skalowaniem horyzontalnym i zerowym zaufaniem między nimi. |

# Wymagania bezpieczeństwa w zakresie infrastruktury

| Kod wymagania | Opis wymagania |
|---|---|
| NFUN-B-I-04 | Moduł musi umożliwiać przywrócenie stanu konfiguracji oraz danych operacyjnych na podstawie ostatnio wykonanych kopii zapasowych w czasie określonym w tabeli SLA. |
| NFUN-B-I-06 | Dostawca musi dostarczyć mechanizmy i instrukcje umożliwiające:<br>• Monitorowania bezpieczeństwa,<br>• Utrzymania aktualności systemów i oprogramowania,<br>• Ciągłości działania,<br>• Zarządzania uprawnieniami,<br>• Doskonalenia systemu bezpieczeństwa,<br>• Raportowania stanu bezpieczeństwa infrastruktury, |
| NFUN-B-I-07 | W przypadku utrzymywania przez Wykonawcę Systemu w chmurze, Infrastruktura chmurowa musi spełniać wymagania SCCO na poziomie 2 |



Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

# Wymagania w stosunku do komponentów LM/LLM/A

| ID | Wymaganie |
|---|---|
| NFUN-B-ML-1 | System musi zapewniać wyjaśnialność (explainability) wyników interpretacji: dla każdej generowanej interpretacji musi dostarczać zrozumiałe wyjaśnienie (np. "Na podstawie podwyższonego poziomu X i historii Y, zalecane Z"), z odniesieniem do reguł/wzorów modelu, zrozumiałe dla laika medycznego, zgodne z MDCG 2023-5 i wymogami transparentności AI Act. |
| NFUN-B-ML-2 | System nie może uczyć się na przesłanych danych użytkownika w szczególności:<br>• brak mechanizmów retrainingu, fine-tuningu<br>• aktualizacji modeli na podstawie danych wejściowych,<br>• tworzenia RAG na bazie danych wejściowych lub wejściowych<br>• zbierania danych zagregowanych |
| NFUN-B-ML-3 | W przypadku oferty w modelu SaaS:<br>System musi automatycznie usuwać wszystkie dane wejściowe (wyniki badań, pseudonimy, metadane interakcji) po wykonaniu analizy i generowaniu interpretacji, w czasie <1h, z potwierdzeniem usunięcia w logach (data privacy by design, art. 5.1.e RODO).,<br><br>Dane wejściowe pośrednie i wyjściowe nie mogą być odkładane w logach lub backupach systemu Wykonawcy w przypadku udostępnienia usługi w Modelu SaaS |
| NFUN-B-ML-4 | System musi realizować sanityzację wejścia i wyjścia do modelu LLM w module "Zebranie wywiadu medycznego":<br>Poniższe parametry sanityzacji muszą być konfigurowalne przez Zamawiającego w panelu administracyjnym z walidacją i możliwością testowania.<br>Wejście i Wyjście:<br>• filtrowanie/blocklista słów/tematów (np., seks, przemoc, finanse,<br>• polityka, tematy nie związane z wywiadem),<br>• długość promptu,<br>• blokada danych osobowych (PESEL, adres, imię/nazwisko),<br>• detekcja prompt injection/jailbreak<br>Wyjście:<br>• blokada zaleceń terapeutycznych/diagnostycznych ("skonsultuj z lekarzem"),<br>• limit długości odpowiedzi,<br>• system musi mieć możliwość definiowania kategorii stwierdzeń medycznych<br>• filtrowanie medycznych stwierdzeń wysokiego ryzyka (np. "rak", "zawał") bez poniżej sterowalnego dla każdej kategorii poziomu |



Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

| | |
|---|---|
| | ufności |
| NFUN-B-ML-5 | Jeśli w systemie zastosowane są komponenty AI/ML/LLM muszą być udokumentowane zgodnie z MDCG 2023-5 (guidance on AI/ML w MDR), z walidacją modeli i monitoringiem performance. |
| NFUN-B-ML-6 | System musi eksportować do systemu Logów Zamawiającego, metadane dotyczące użytego w interpretacji badania modelu(model version, confidence score, bias check) |
| NFUN-B-ML-7 | Moduły system zawierając elementy LMM musza być przetestowane pod kątem OWASP Top 10 for LLM |



Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

# Wymagania dotyczące monitoringu i logowania

| Kod wymagania | Opis wymagania |
|---|---|
| NFUN-B-L-01 | System musi rejestrować wszystkie operacje systemowe i użytkowe w dzienniku zdarzeń, w tym:<br>• zdarzenia administracyjne,<br>• zmiany konfiguracji,<br>• błędy przetwarzania,<br>• zmiany w ustawieniach użytkowników. |
| NFUN-B-L-02 | System musi dla każdego wpisu w dzienniku zdarzeń zapisywać co najmniej:<br>• identyfikator użytkownika,<br>• czas operacji,<br>• typ operacji,<br>• identyfikator obiektu (np. zlecenia, modelu SI),<br>• rezultat (sukces, błąd). |
| NFUN-B-L-03 | System musi rejestrować wszystkie operacje na danych osobowych i medycznych (pseudonimizacja, odczyt, zmiana, udostępnienie, usunięcie) w dzienniku audytowym zawierającym co najmniej:<br>• identyfikator użytkownika lub obiektu,<br>• czas operacji,<br>• zakres danych,<br>• typ operacji. |
| NFUN-B-L-04 | System powinien umożliwiać przegląd dziennika zdarzeń z poziomu interfejsu graficznego (GUI) przez użytkowników posiadających odpowiednie uprawnienia. |
| NFUN-B-L-05 | System musi rejestrować każde użycie interfejsów API zewnętrznych, w tym co najmniej:<br>• żądanie,<br>• nadawca,<br>• kod odpowiedzi,<br>• czas realizacji. |
| NFUN-B-L-05 | System musi umożliwiać generowanie powiadomień w przypadku wystąpienia określonych zdarzeń zdefiniowanych przez Zamawiającego. |
| NFUN-B-L-06 | System powinien zapewniać, że:<br>• Powiadomienia muszą być dostępne w formie wiadomości e-mail,<br>• Powiadomienia mogą być generowane z wykorzystaniem API. |
| NFUN-B-L-07 | System musi umożliwiać rejestrowanie operacji użytkowników (logi audytowe), w tym:<br>• logowania,<br>• uruchamiania procesów,<br>• edycji konfiguracji,<br>• zmian uprawnień. |



Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

| | |
|---|---|
| NFUN-B-L-08 | Logi audytowe muszą być dostępne dla administratorów i możliwe do eksportu i integracji z zewnętrznymi systemami SIEM (Security Information and Event Management). |
| NFUN-B-L-09 | Logi audytu nie mogą zawierać danych osobowych w otwartej formie. W przypadku umieszczania tych informacji dane te muszą być zaszyfrowane kluczem określanym przez Zamawiającego |
| NFUN-B-L-10 | System musi umożliwiać konfigurację poziomu szczegółowości logowania operacji (np. tylko błędy, wszystkie działania administracyjne). |
| NFUN-B-L-11 | System zapewnia możliwość utrwalenia dowodu interakcji Użytkownika |
| NFUN-B-L-12 | System musi logować dla każdej interpretacji wyników badań jej wyjaśnienie zgodnie z NFUN-B-ML-1. |
| NFUN-B-L-13 | System musi monitorować skuteczność modeli ML/LLM w tym:<br>• accuracy, F1-Score,<br>• drift detection,<br>• confidence distribution<br>i automatycznie alarmować przy przekroczeniu zdefiniowanych przez Zamawiającego progów. W wymaganych przypadkach może być to realizowane w sposób ciągły na podstawie danych testowych dostarczonych przez Zamawiającego włączonych do strumienia danych interpretowanych. |
| NFUN-B-L-14 | System musi rejestrować niepożądane zdarzenia z interpretacji w tym:<br>• confidence level poniżej zdefiniowanego dla kategorii przez Zamawiającego,<br>• oznaczanie przez człowieka jako "błędna interpretacja"<br>• wykryty drift modelu,<br>• późnienie powyżej zdefiniowanego przez Zamawiającego<br>Wysyłać alerty do administratorów Systemu oraz wysyłać alerty związane z cyber-incydentami do SIEM. |
| NFUN-B-L-16 | System musi posiadać moduł wykrywający anomalie (np. w wolumenie zapytań) i wysyłać alerty via email/webhook/SIEM. |
| NFUN-B-L-17 | W przypadku oferty w modelu SaaS:<br>System musi automatycznie usuwać wszystkie dane wejściowe (wyniki badań, pseudonimy, metadane interakcji) po wykonaniu analizy i generowaniu interpretacji, w czasie <1h, z potwierdzeniem usunięcia w logach.<br>Dane wejściowe pośrednie i wyjściowe nie mogą być odkładane w logach lub backupach systemu Wykonawcy w przypadku udostępnienia usługi w modelu SaaS |
| NFUN-B-L-18 | Niezależnie od oferowanego przez Wykonawcę modelu dostępu do usługi wszystkie logi musza być składowane na infrastrukturze Zamawiającego |

# Wymagania dotyczące procesu uwierzytelniania i dostępu

| Kod Wymagania | Opis wymagania |
|---|---|



Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

| | |
|---|---|
| NFUN-B-S-01 | System musi wykorzystywać mechanizmy uwierzytelniania Administratorów systemu zapewnione przez Zamawiającego zgodne Azure Entra |
| NFUN-B-S-02 | System musi umożliwiać zarządzanie rolami i uprawnieniami użytkowników zgodnie z modelem RBAC |
| NFUN-B-S-03 | Zarządzane wszystkimi danymi do uwierzytelnienia (a w szczególności dostępów do baz danych, interfejsów API) – tzw. „Secrety” - musi być zrealizowane w oparciu o system Secret management dostarczony przez Zamawiającego zgodny z Hashicorp Vault |

# Wymagania dotyczące procesu wdrożenia

| Kod Wymagania | Opis wymagania |
|---|---|
| NFUN-B-P-01 | Wykonawca w fazie analizy dostarczy do akceptacji Zamawiającego projekt architektury zawierający co najmniej: diagram kontekstu, diagram komponentów, diagram wdrożenia, diagram przepływu danych wraz z określeniem protokołów portów, standardów szyfrowania, uwierzytelniania i autoryzacji oraz pełen wykaz zastosowanych zabezpieczeń na wszystkich warstwach systemu |
| NFUN-B-P-02 | Przed wdrożeniem Wykonawca opracuje model zagrożeń zgodnie z metodyką PASTA lub tożsamą oraz na tej podstawie zaproponuje zmiany ograniczające zagrożenia do poziomu Niski (CVSS ver 4.0 < 3.0). |
| NFUN-B-P-03 | Przed wdrożeniem Wykonawca przedstawi Software Bill of Material (dalej SBOM). Wraz z określeniem podatności użytych komponentów. |
| NFUN-B-P-04 | 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-05 | 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-06 | 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. |
| NFUN-B-P-07 | Wykonawca dostarczy i przetestuję procedurę odtwarzania Systemu po awarii rozległej (katastrofie) z użyciem skryptów IaC |
| NFUN-B-P-08 | Sposób dostępu do poszczególnych środowisk Systemu/Modułu przez pracowników wykonawcy: DEV, TEST, ACC, PROD – za pośrednictwem system PAM dostarczonego przez Zamawiającego |



Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

# Wymagania dotyczące wprowadzania zmian

| ID | Wymaganie |
|---|---|
| NFUN-B-Z-01 | Wykonawca jest zobowiązany do aktualizacji komponentów systemu przez cały czas trwania Umowy tak aby ich wersja była posiadała wsparcie ich producenta oraz była pozbawiona podatności wysokich (CVSS ver 4.0 >7.0) |
| NFUN-B-Z-02 | 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-03 | System musi realizować proces zatwierdzania zmian z etapami: zgłoszenie, ocena wpływu bezpieczeństwa/klinicznego, wdrożenie testowe, testy regresji, zatwierdzenie przez Zamawiającego, wdrożenie produkcyjne.<br>Wymaganie dotyczy wszystkich komponentów systemu niezależnie od oferowanego modelu (on-premis, SaaS) i obejmuje wszystkie elementy systemu w tym modele ML/LLM, reguły interpretacji Wszelkie zmiany wymagają akceptacji CeZ. |
| NFUN-B-Z-04 | Wykonawca musi dostarczyć raport skanowania systemu przed każdym wdrożeniem zmiany pod kątem nowych podatności i wstrzymywać wdrożenia przy podatnościach (CVSS ver 4.0 >7.0) |
| NFUN-B-Z-05 | Wykonawca przed każdą planowaną zmianą musi dostarczyć listę wszystkich aktualizacji/patchy/zmiany w SBOM. |
| NFUN-B-Z-06 | Wykonawca musi weryfikować integralność aktualizacji (podpis cyfrowy) przed wdrożeniem oraz dostarczać wynik tej weryfikacji przed wdrożeniem produkcyjnym. |



Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706