Rekomendacje

dotyczące zabezpieczenia danych medycznych i transmisji danych przez platformę.

1. Zgodność z przepisami prawa

Proszę zwrócić uwagę na to czy platforma spełnia obowiązujące regulacje:

- RODO (GDPR) – w UE ochrona danych osobowych, w tym wrażliwych (np. dane medyczne).
- Ustawa o systemie informacji w ochronie zdrowia (Polska) – np. art. 5 i 13.
- ISO 27001 / ISO 27799 – standardy zarządzania bezpieczeństwem informacji i danych zdrowotnych.
- HIPAA (jeśli działasz w USA) – dla danych medycznych i transmisji elektronicznej.

2. Zabezpieczenia techniczne danych

W czasie spoczynku (storage):

- Szyfrowanie danych: AES-256 dla danych w bazach (np. PostgreSQL, MongoDB).
- Segmentacja danych pacjentów: logiczna separacja danych różnych użytkowników.
- Kontrola dostępu: tylko autoryzowany personel ma dostęp do danych – przez RBAC (Role-Based Access Control).
- Backupy i disaster recovery: automatyczne backupy z szyfrowaniem i testowanymi procedurami odzyskiwania.

W czasie transmisji:

- TLS 1.2+ / HTTPS – obowiązkowe szyfrowanie komunikacji (np. z przeglądarką lub aplikacją mobilną).
- VPN lub dedykowane tunele (IPSec/SSL VPN) – do komunikacji między serwerami wrażliwymi.
- Certyfikaty cyfrowe i podpisywanie danych – dla integralności dokumentów medycznych (np. e-recepty).

3. Autoryzacja i uwierzytelnianie użytkowników

- MFA (Multi-Factor Authentication) – dla personelu medycznego i administratorów.
- SSO (Single Sign-On) – integracja np. z systemami szpitalnymi (LDAP, Active Directory).
- Monitorowanie logów logowania i operacji na danych – audytowalność działań.

4. Testowanie i bezpieczeństwo aplikacji

- Regularne testy penetracyjne – niezależni specjaliści sprawdzający odporność systemu.
- WAF (Web Application Firewall) – ochrona przed atakami typu SQLi, XSS itd.
- Zasada najmniejszych uprawnień (PoLP) – każda rola ma tylko absolutnie niezbędne prawa.

5. Transmisja danych między systemami (np. HL7 / FHIR)

- Protokół FHIR (REST + JSON/XML) z TLS – nowoczesny standard interoperacyjności.
- Bezpieczna wymiana danych HL7 v2 – z szyfrowanym transportem (np. MLLP przez VPN).
- Integracje z P1, eWUŚ, RPWDL – tylko przez autoryzowane kanały i po audycie.

6. Dokumentacja, audyty i polityki

- Polityka bezpieczeństwa informacji.
- Rejestr czynności przetwarzania danych (RODO art. 30).
- Umowy powierzenia przetwarzania danych (z hostingiem, chmurą, partnerami).
- Szkolenia pracowników z ochrony danych.

7. Bezpieczeństwo infrastruktury chmurowej (jeśli stosowana)

- Chmury z certyfikatami ISO 27001, HDS (Francja), ENS (Hiszpania), HIPAA.
- Strefy geograficzne zgodne z RODO (np. EU West).
- Ograniczenie dostępu do zasobów przez IAM (Identity and Access Management).

Rekomendowane narzędzia / technologie

Obszar	Narzędzie / Protokół
Szyfrowanie	AES-256, TLS 1.3
Przechowywanie danych	PostgreSQL, MongoDB z at-rest encryption
Monitoring	ELK Stack, Grafana + Prometheus
Firewall / WAF	Cloudflare, AWS WAF, ModSecurity
Transmisja HL7 / FHIR	HAPI FHIR, Mirth Connect
Backup i DR	Veeam, AWS Backup, Google

Obszar	Narzędzie / Protokół
	Backup