Wsparcie Szpitala

Mapa kompetencji

Kto za co odpowiada przy decyzjach z udziałem AI w szpitalu

Sztuczna inteligencja nie ma osobowości prawnej. Każda decyzja kliniczna podejmowana przy wsparciu algorytmu musi mieć konkretnego autora — człowieka lub instytucję. Ten dokument porządkuje sześć kluczowych ról i obowiązków zgodnie z AI Act, Kodeksem Etyki Lekarskiej, MDR/IVDR, RODO i NIS2. To checklista referencyjna dla dyrektorów szpitali, IOD, działów IT oraz lekarzy, którzy chcą zorganizować placówkę tak, by każdą decyzję klinicznej z udziałem AI dało się prześledzić, zweryfikować i obronić.

1. LEKARZ

• Ostateczna decyzja diagnostyczna i terapeutyczna należy zawsze do lekarza.
• Obowiązek poinformowania pacjenta o użyciu AI w procesie diagnostycznym lub terapeutycznym.
• Uzyskanie świadomej zgody pacjenta — zaktualizuj standardowe formularze zgody.
• Weryfikacja rekomendacji algorytmu w świetle wiedzy klinicznej i kontekstu pacjenta.
• Dokumentowanie własnego rozumowania klinicznego w EDM — niezależnie od wyniku AI.

Podstawa prawna: Kodeks Etyki Lekarskiej art. 12 (od 1 stycznia 2025), RODO

2. DYREKTOR SZPITALA

• Wyznaczenie właściciela polityki AI governance na poziomie zarządu.
• Prowadzenie rejestru systemów AI używanych w placówce — z klasyfikacją ryzyka.
• Negocjowanie umów z dostawcami AI (prawa do logów, metadanych, modeli, SLA).
• Zapewnienie szkoleń AI literacy dla personelu medycznego, IT i zarządczego.
• Nadzór po wdrożeniu (post-market monitoring) i ścieżki zgłaszania incydentów.

Podstawa prawna: AI Act (2024/1689), ustawa o KSC (NIS2)

3. INSPEKTOR OCHRONY DANYCH (IOD)

• Weryfikacja podstaw prawnych przetwarzania danych pacjentów przez AI.
• Przeprowadzenie oceny skutków dla ochrony danych (DPIA) — krytyczne dla AI.
• Aktualizacja klauzul informacyjnych o przetwarzaniu danych przez AI.
• Nadzór nad mechanizmami anonimizacji i pseudonimizacji w treningu modeli.
• Współpraca z dostawcą przy ustaleniu współadministrowania lub powierzenia danych.

Podstawa prawna: RODO (Rozporządzenie 2016/679)

Mapa kompetencji — cd.

4. DZIAŁ IT / CISO

• Cyberbezpieczeństwo systemów AI — segmentacja sieci, kontrola dostępu, MFA.
• Integracja systemów AI z infrastrukturą szpitalną (HIS, LIS, RIS, PACS).
• Backup i procedury odtworzenia po incydencie.
• Automatyczne logowanie zdarzeń systemów wysokiego ryzyka (wymóg AI Act).
• Audyt cykliczny zgodności z normami ISO 27001, NIS2.

Podstawa prawna: Ustawa o KSC (NIS2), ISO 27001, AI Act

5. PRODUCENT OPROGRAMOWANIA AI

• Zgodność systemu z AI Act oraz MDR/IVDR (jeśli to wyrób medyczny).
• Pełna dokumentacja techniczna — dane treningowe, walidacja, czułość, swoistość.
• Ocena zgodności przed wprowadzeniem na rynek i rejestracja w bazie unijnej.
• Post-market monitoring i raportowanie poważnych incydentów do organów nadzoru.
• Zapewnienie wyjaśnialności (explainable AI) i mechanizmów human-in-the-loop.

Podstawa prawna: AI Act, MDR 2017/745, IVDR 2017/746

6. JEDNOSTKA NOTYFIKOWANA

• Niezależna ocena zgodności wyrobów medycznych klasy IIb/III.
• Certyfikacja przed wprowadzeniem na rynek — pełni rolę gatekeepera regulacyjnego.
• Audyt systemu zarządzania jakością producenta.
• Po wdrożeniu — okresowa weryfikacja zgodności w ramach surveillance audits.
• **Po wprowadzeniu na rynek** odpowiedzialność operacyjna wraca do producenta i użytkownika.

Podstawa prawna: MDR 2017/745, IVDR 2017/746

AI nie ma osobowości prawnej. Odpowiedzialność jest podzielona — nie scedowana na technologię. Każda decyzja kliniczna musi mieć konkretnego autora i ślad audytowy.

Checklista AI governance dla menedżera szpitala

Siedem kroków, które powinieneś wdrożyć przed 2 sierpnia 2026 r. — datą pełnego stosowania AI Act dla systemów wysokiego ryzyka.

- ☐ **Inwentaryzacja systemów AI**
  Zinwentaryzuj wszystkie systemy AI (również SaaS — np. ChatGPT Enterprise) i sklasyfikuj według ryzyka zgodnie z Załącznikiem III AI Act.
- ☐ **Właściciele i polityka governance**
  Wyznacz właściciela biznesowego każdego systemu oraz właściciela polityki AI governance na poziomie zarządu placówki.
- ☐ **Rewizja umów z dostawcami**
  Zrewiduj umowy z dostawcami AI — prawa do logów, metadanych, modeli, SLA na poprawki, procedury wycofania wersji modelu.
- ☐ **Rejestr decyzji wspieranych przez AI**
  Wdroż rejestr decyzji wspieranych przez AI: kto, kiedy, na podstawie jakiego modelu, jaką decyzję podjął. Wymóg AI Act dla systemów wysokiego ryzyka.
- ☐ **Aktualizacja formularzy zgody pacjenta**
  Zaktualizuj formularze świadomej zgody pacjenta o informację o użyciu AI (art. 12 KEL) oraz polityki RODO o nową kategorię przetwarzania.
- ☐ **Szkolenia AI literacy**
  Zaplanuj szkolenia kompetencyjne dla personelu medycznego, technicznego i zarządczego — obowiązek z 2 lutego 2025 r.
- ☐ **Integracja polityk: AI, cyber, RODO**
  Zintegruj politykę AI z politykami cyberbezpieczeństwa (NIS2) i RODO — tworzą wspólny kręgosłup compliance.

Kluczowe daty do pamiętania

Data	Wydarzenie regulacyjne
2 lutego 2025	AI literacy — obowiązek kompetencji personelu (AI Act)
1 stycznia 2025	KEL art. 12 — zgoda pacjenta na użycie AI (Polska)
26 marca 2025	EHDS — Europejska Przestrzeń Danych Zdrowotnych (start)
30 czerwca 2026	Deadline rozliczenia KPO D1.1.2 dla 359 szpitali
2 sierpnia 2026	Pełne stosowanie AI Act dla systemów wysokiego ryzyka
2 sierpnia 2027	Koniec okresu przejściowego dla AI w wyrobach medycznych (MDR/IVDR)

Materiał ma charakter informacyjny i edukacyjny. Nie stanowi porady prawnej. Stan informacji: maj 2026.