

AUDYT · HIS · EDM · DECYZJA CIO

Audyt HIS/EDM w 7 krokach

Praktyczny przewodnik dla dyrektorów IT, ABI/IOD i kadry zarządzającej - jak rzetelnie ocenić obecny system medyczny przed decyzją o modernizacji lub wymianie. Bez kosztownego audytu zewnętrznego.

7

KROKÓW METODY

14

KLUCZOWYCH PYTAŃ

3-6

TYGODNIE WYKONANIA

Po co audyt - i czemu wewnętrzny

Większość decyzji o wymianie systemu HIS/EDM podejmowana jest pod presją - kończy się umowa, dostawca podnosi ceny, system pada w piątek przed weekendem. To najgorszy moment na decyzję wartości 5-30 mln zł.

Ten dokument prowadzi Cię przez **7 kroków audytu wewnętrznego**, które wykonasz z własnym zespołem IT w 3-6 tygodni. Cel: zebrać twarde dane, zanim zaczniesz słuchać dostawców.

Komu się przyda

- Dyrektorowi IT - przygotowanie business case dla zarządu
- Inspektorowi ochrony danych (IOD) - mapowanie ryzyk RODO/NIS2
- Dyrektorowi szpitala - uzasadnienie decyzji inwestycyjnej
- Komitetowi przetargowemu - fakty do napisania OPZ

Czego unikamy

- Pytania „jaki system kupić” przed pytaniem „co naprawdę mamy”
- Decyzji opartej tylko na cenniku licencji (~30% rzeczywistego TCO)
- Listy 800 wymagań funkcjonalnych skopiowanych z innych przetargów
- Lock-inu z nowym dostawcą - przepisanego z poprzedniej umowy

Wynik audytu

Po przejściu 7 kroków zbierzesz materiał, na podstawie którego podejmiesz świadomie jedną z trzech decyzji:

Decyzja	Kiedy	Czas / koszt
Utrzymać	System spełnia $\geq 85\%$ potrzeb, niskie ryzyka	0 / koszt utrzymania
Zmodernizować	Architektura zdrowa, brakuje 2-4 modułów lub integracji	3-9 mies / 0,5-3 mln zł
Wymienić	Lock-in, brak rozwoju, ryzyka compliance, koszt utrzymania $\geq 40\%$ wartości projektu rocznie	9-18 mies / 5-30 mln zł

7 kroków audytu

KROK 1 Inwentaryzacja - co naprawdę mamy w użyciu

Wbrew pozorom większość szpitali nie ma aktualnej listy modułów, integracji i użytkowników HIS/EDM. Zacznij od faktów.

Pytania kontrolne:

- Ile modułów HIS jest faktycznie używanych (ostatnie 90 dni logów)?
- Ile aktywnych kont użytkowników, ile martwych?
- Z jakimi systemami zewnętrznymi mamy integracje (LIS, PACS, P1, NFZ, KSeF)?
- Jaka jest aktualna wersja systemu i kiedy ostatnia aktualizacja?

Sygnal ostrzegawczy: jeśli zespół IT nie potrafi odpowiedzieć w 3 dni - masz problem inwentaryzacyjny ważniejszy od wymiany systemu.

KROK 2 Mapa procesów - czy system pokrywa kluczowe scenariusze

Wybierz 5-7 najczęstszych scenariuszy klinicznych (np. przyjęcie pacjenta planowego, izba przyjęć, blok operacyjny, wypis z EDM, rozliczenie z NFZ). Przejdź każdy scenariusz krok po kroku w systemie.

Co mierzymy:

- Liczba kliknięć / ekranów na ukończenie zadania
- Ile danych personel wprowadza ręcznie, ile system zaciąga automatycznie
- Ile czynności wymaga przełączania między systemami (HIS → LIS → PACS)
- Co personel kompensuje przez Excel, papier, WhatsApp (workaround)

Sygnal ostrzegawczy: 3+ workarouny poza systemem = system de facto nie działa, mimo że formalnie „jest wdrożony”.

KROK 3**Wydajność i niezawodność - twarde liczby**

Bez metryk nie ma rozmowy o jakości. Zbierz dane z ostatnich 12 miesięcy.

Minimum, które trzeba znać:

- **Uptime** rzeczywisty (z monitoringu, nie z deklaracji dostawcy)
- Liczba **incydentów krytycznych** i czas ich rozwiązania (MTTR)
- Średni czas **response time** kluczowych ekranów (rejestracja, zlecenie, wynik)
- Ile razy w ciągu roku dostawca **przekroczył SLA** bez konsekwencji finansowych

Sygnał ostrzegawczy: jeśli dostawca nie raportuje uptime / SLA miesięcznie - masz lock-in informacyjny.

KROK 4**TCO rzeczywisty - pełny koszt posiadania**

Cennik licencji to zwykle 30-40% rzeczywistego kosztu. Reszta to ukryte pozycje, których szpital nie dostrzega rok do roku.

Co policzyć (rocznie):

- **Licencje** (per stanowisko, per moduł, per łóżko)
- **Utrzymanie / SLA** dostawcy (zwykle 18-25% wartości licencji rocznie)
- **Hosting i infrastruktura** (serwery, storage, backup, DR)
- **Integracje** - każda nowa integracja często osobno wyceniana
- **Szkolenia** przy rotacji personelu (15-25% rotacja w szpitalach)
- **Koszty przestoju** - utracone przyjęcia, ręczna rejestracja, nadgodziny
- **Wewnętrzny zespół IT** - etaty dedykowane do utrzymania systemu

Sygnał ostrzegawczy: jeśli $TCO \geq 40\%$ wartości projektu wdrożeniowego rocznie - system za drogo kosztuje. Standard rynkowy to 20-30%.

KROK 5**Audyt zgodności - NIS2, RODO, P1, EDM**

System HIS/EDM jest centralnym punktem bezpieczeństwa danych medycznych. Sprawdź faktyczny, nie deklaracyjny stan zgodności.

Co zweryfikować:

- **NIS2** - czy mamy [checklistę gotowości](#) wypełnioną z wynikiem $\geq 16/22$?
- **RODO** - kontrola dostępu, audit log, anonimizacja, prawo do bycia zapomnianym
- **P1 / EDM** - czy wymiana dokumentów medycznych z P1 działa (e-Recepta, e-Skierowanie, EDM, IKP)?
- **KSeF** - fakturowanie z fakturami strukturyzowanymi (od 01.04.2026 obowiązkowe)
- **Backup i DR** - testowe odtworzenie wykonane w ostatnich 12 miesiącach (z dowodem)

Sygnal ostrzegawczy: brak audit log w systemie produkcyjnym = ryzyko prawne (art. 32 RODO + NIS2 art. 21).

KROK 6**Architektura - otwartość, lock-in, możliwość rozwoju**

To jeden z najważniejszych kroków, a najczęściej pomijany. Architektura przesądza o kosztach kolejnych 5-10 lat.

Pytania techniczne (do zespołu IT i dostawcy):

- Czy mamy dostęp do **schematu bazy danych** i bezpośrednio do danych w bazie?
- Czy są **otwarte API** z udokumentowanymi endpointami (REST/HL7 FHIR)?
- Czy możemy **eksportować dane** w standardowych formatach bez asysty dostawcy?
- Czy umowa pozwala na **integracje przez podmioty trzecie** bez zgody dostawcy?
- Co się stanie, jeśli dostawca **zniknie z rynku**? Czy mamy dostęp do kodu źródłowego (escrow)?
- Czy system jest oparty na **otwartych technologiach** (PostgreSQL, Linux) czy zamkniętych (Oracle, MSSQL bez licencji)?

Sygnal ostrzegawczy: jeśli odpowiedź na 3+ pytania to „nie wiemy” lub „dostawca powiedział że tego nie udostępni” - masz hard lock-in. Wymiana będzie kosztowna ale konieczna.

KROK 7**Decyzja i rekomendacja dla zarządu**

Zsumuj wnioski z kroków 1-6 w jednostronicowej rekomendacji dla zarządu/dyrekcji.

Struktura rekomendacji (1 strona A4):

- **Stan obecny** - 3 kluczowe metryki (uptime, TCO/rok, % luk funkcjonalnych)
- **3 największe ryzyka** - z oszacowaniem kosztu materializacji
- **3 scenariusze** (utrzymać / zmodernizować / wymienić) z TCO 5-letnim
- **Rekomendacja** - jeden scenariusz z uzasadnieniem w 3 zdaniach
- **Plan działania** w pierwszych 90 dniach

Sygnal ostrzegawczy: jeśli rekomendacja nie mieści się na 1 stronie - zarząd jej nie przeczyta. Skróć.

Co dalej

Audyt to początek, nie koniec. Niezależnie od decyzji (utrzymać/zmodernizować/wymienić) - masz teraz **twarde dane do rozmów z dostawcami i zarządem**.

Częste błędy po audycie

- Wykorzystanie audytu jako narzędzia walki z dostawcą zamiast bazy decyzyjnej
- Pisanie OPZ do nowego przetargu na podstawie wymagań starego dostawcy (utrwała lock-in)
- Pominięcie kosztów migracji danych przy wycenie nowego systemu
- Brak komunikacji z personelem klinicznym - opór przy wdrożeniu

Co warto zrobić w tym samym czasie

1. Wypełnij checklistę gotowości NIS2 - równoległy proces, te same dane wejściowe
2. Zorganizuj dialog techniczny z 3-5 dostawcami przed pisaniem OPZ (legalna procedura PZP)
3. Sprawdź klauzule równoważności w OPZ - żeby naprawdę dopuścić konkurencję
4. Zaplanuj budżet z rezerwą 20-30% na pozycje nieprzewidziane w pierwszym kosztorysie

Pomoc OneCare

OneCare jest dostawcą systemu OpenCARE i potencjalnym wykonawcą w postępowaniach na HIS/EDM. Nie pełniemy roli doradcy zamawiającego w przygotowaniu postępowania (art. 56 ust. 1 pkt 4 PZP). To, co możemy zaoferować:

- **Materiały edukacyjne** - kolejne lead magnety, webinary i artykuły o cyfryzacji szpitali
- **Demo OpenCARE** - 30-minutowa prezentacja systemu na realnych przepływach klinicznych
- **Wizyta referencyjna** - możliwość zobaczenia OpenCARE w pracującym szpitalu
- **Złożenie oferty** - w postępowaniu otwartym, jako jeden z wykonawców na warunkach jednakowych dla wszystkich

kontakt@onecare.com.pl · +48 601 821 612 · onecare.com.pl

Zastrzeżenie. Niniejszy materiał ma charakter edukacyjny i nie stanowi porady prawnej, technicznej ani inwestycyjnej. Decyzje o wymianie systemu medycznego wymagają indywidualnej oceny stanu placówki,

środowiska technicznego i kontraktowego. OneCare Sp. z o.o. nie ponosi odpowiedzialności za decyzje podjęte wyłącznie na podstawie tego dokumentu.

© 2026 OneCare Sp. z o.o. · ul. Pokrzywy 4, 05-850 Kręczki · NIP 1182322364 · KRS 0001221324 · Sąd Rejonowy dla m.st. Warszawy, XIV Wydział Gospodarczy KRS

Wersja 1.0 · 4 maja 2026 · Dokument do swobodnej dystrybucji w pełnej, niezmienionej formie