

Rekomendacje
dla zgodności Platformy Medycznej z przepisami Prawa Medycznego
(wymagają indywidualnego dostosowania)

1. Podstawy prawne, które należy uwzględnić

OBSZAR	AKT PRAWNY
Ochrona danych osobowych	RODO, ustawa o ochronie danych osobowych
Dokumentacja medyczna	Ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta
Działalność medyczna	Ustawa o działalności leczniczej
Systemy IT w zdrowiu	Ustawa o systemie informacji w ochronie zdrowia
Telekomunikacja	Prawo telekomunikacyjne, ustawa o świadczeniu usług drogą elektroniczną
Kwalifikacje personelu	Ustawa o zawodach lekarza i pielęgniarzy

2. Wymagania dotyczące danych medycznych

Dane osobowe medyczne

Dane medyczne są danymi wrażliwymi. Do ich przetwarzania wymagana jest:

- wyraźna zgoda pacjenta, lub
- przetwarzanie w ramach realizacji świadczenia zdrowotnego (np. art. 9 ust. 2 lit. h RODO).

Dokumentacja medyczna (Ustawa o prawach pacjenta, art. 24-30):

- Musi być prowadzona w formie elektronicznej od 2021 r.
- Musi zawierać m.in. dane identyfikacyjne, diagnozy, wyniki badań, zalecenia.
- Musi być przechowywana przez 20 lat (lub 30 lat w przypadku zgonu pacjenta z powodu przemocy).

3. Wymogi dla Platformy jako systemu teleinformatycznego

Musi spełniać:

- Wymogi interoperacyjności i standardów HL7 / FHIR (integracja z P1, eWUŚ, RPWDL).
- Zabezpieczenia techniczne zgodnie z art. 13 ustawy o systemie informacji w ochronie zdrowia:
 - identyfikacja i uwierzytelnienie użytkowników,
 - rejestrowanie dostępu do danych,
 - mechanizmy szyfrowania i integralności danych.

Jeśli platforma oferuje e-rejestrację lub e-wizyty:

- Musi zapewniać autoryzację pacjenta (np. Profil Zaufany, SMS, hasło + e-mail).

- Musi umożliwiać potwierdzenie tożsamości lekarza (np. podpis kwalifikowany, ZUS, P1).
- Konsultacje online muszą spełniać warunki świadczenia zdrowotnego (diagnoza, zalecenia, dokumentacja).

4. Obowiązki administratora danych i podmiotu medycznego

- Zawarcie umowy powierzenia przetwarzania danych (np. z hostingiem, podwykonawcą).
- Prowadzenie Rejestru czynności przetwarzania danych (art. 30 RODO).
- Wyznaczenie Inspektora Ochrony Danych (IOD) (obowiązkowe dla placówek medycznych).
- Procedury w przypadku naruszenia ochrony danych – zgłoszenie do UODO w ciągu 72h.

5. Zgody, klauzule i regulaminy

Należy:

- Zgodę pacjenta na przetwarzanie danych osobowych w określonym celu (np. rejestracja, kontakt).
- Klauzulę informacyjną RODO (administrator, cel, podstawa, prawa pacjenta).
- Regulamin korzystania z platformy – jasno określa zasady świadczenia usług (np. teleporad).
- Politykę prywatności – opisuje jak dane są zbierane, przetwarzane, przechowywane.

6. Rekomendowane certyfikaty i standardy bezpieczeństwa

Obszar Rekomendacja

Zarządzanie bezpieczeństwem ISO 27001

Dane zdrowotne ISO 27799

Systemy medyczne ISO 13485 (jeśli sprzęt/oprogramowanie medyczne)

Interoperacyjność HL7, FHIR

Przetwarzanie w chmurze Certyfikowana chmura (np. zlokalizowana w UE)

7. Dodatkowe narzędzia i systemy krajowe

- P1 – system informacji medycznej (e-recepty, e-skierowania, EDM).
- eWUŚ – weryfikacja ubezpieczenia pacjenta.
- RPWDL – Rejestr Podmiotów Wykonujących Działalność Leczniczą.

- SMK – System Monitorowania Kształcenia pracowników medycznych (dla szkoleń i uprawnień).