SERWIS ZOZ.PL

ZARZĄDZANIE W OCHRONIE ZDROWIA

Nowe technologie, AI i cyberbezpieczeństwo w placówce medyczne

Niezbędna wiedza dla profesjonalistów w ochronie zdrowia

Zdobądź dostęp do najnowszych publikacji, które pomogą Ci efektywnie zarządzać placówką medyczną.

Sprawdź już dziś!

SERWIS ZOZ .PL
ZARZĄDZANIE W OCHRONIE ZDROWIA

Nowe technologie, AI i cyberbezpieczeństwo
Copyright © Warszawa 2026 by Wiedza i Praktyka sp. z o.o.

Autorzy: Marta Bogusiak, Maciej Lipka, Magdalena Pokrzycka-Walczak, Marzena Pytlarz-Pietraszko

Redakcja: Angelika Zdankiewicz-Staniszkis
Korekta: Zespół
Koordynator produkcji: Mariusz Jezierski
Koordynator projektów wydawniczych: Anna Jagodzińska
Content & Publishing Leader: Marta Grabowska-Peda

Projekt graficzny okładki: Agnieszka Makowska
Zdjęcie na okładce: Freepick
Skład i łamanie: Agnieszka Makowska

Wydanie I
Stan prawny: maj 2026 r. .
ISBN: 978-83-8409-788-5
Kod produktu: 1BV168

Wydawca:
Wiedza i Praktyka sp. z o.o.
03-918 Warszawa, ul. Łotewska 9a
tel. 22 518 29 29, faks 22 617 60 10
www.wip.pl

Publikacja uwzględnia stan prawny obowiązujący na dzień 1 maja 2026 r.

Niniejsza publikacja oraz wszystkie zawarte w niej teksty, grafiki i materiały są chronione prawem autorskim. Żadna część tego e-booka nie może być reprodukowana, przechowywana w systemach wyszukiwania lub transmitowana w jakiejkolwiek formie i jakimikolwiek środkami – elektronicznymi, mechanicznymi, kopiowania, nagrywania lub innymi – bez uprzedniej pisemnej zgody Redakcji.

Zakaz ten nie dotyczy cytowania ww. materiałów w granicach dozwolonego użytku, z powołaniem się na źródło.

Treści zawarte w niniejszej publikacji mają charakter wyłącznie informacyjny i edukacyjny. Publikacja została przygotowana z zachowaniem najwyższej staranności oraz z wykorzystaniem wysokich kwalifikacji, wiedzy i doświadczenia autorów oraz konsultantów. Niemniej jednak zawiera ona ogólne wskazówki i nie powinna być traktowana jako indywidualna porada prawna, finansowa, medyczna ani żadna inna forma profesjonalnej konsultacji.

Redakcja nie ponosi odpowiedzialności za decyzje podjęte na podstawie informacji zawartych w tej publikacji. W przypadku potrzeby uzyskania specjalistycznej porady zaleca się konsultację z odpowiednim ekspertem lub specjalistą w danej dziedzinie.

Spis treści

Nowe technologie, AI i cyberbezpieczeństwo 6

Cyfrowa transformacja w ochronie zdrowia 6
Diagnoza barier w cyfrowej transformacji ochrony zdrowia 6
Jak rozwijać kompetencje cyfrowe personelu medycznego? 7
Inwestycje w ludzi i zaufanie – fundament skutecznej cyfryzacji medycyny 8
Sukces cyfrowej transformacji zależy od ludzi, nie od technologii 9

Odpowiedzialne stosowanie AI w placówce medycznej 10

Kodeks Etyki Lekarskiej 11
Akt o AI 12
System Wysokiego Ryzyka od sierpnia 2026 13

Obrona przed cyberatakiem jako obowiązek zarządczy 17

Dlaczego ochrona zdrowia jest szczególnie narażona na cyberataki? 17
Co w praktyce oznacza „cyberatak" – najczęstsze scenariusze w placówkach 18
Najwrażliwsze obszary organizacji: od rejestracji po diagnostykę i rozliczenia 18
Zarządzanie incydentem jako zdarzeniem kryzysowym 19
Obowiązki formalne i odpowiedzialności: RODO,
bezpieczeństwo informacji, relacje z NFZ i kontrahentami 19
Koszty incydentu: finansowe, organizacyjne i wizerunkowe 20
Jak budować odporność placówki: governance,
umowy z dostawcami, standardy i testowanie gotowości 20
Wnioski dla zarządzających: jak przełożyć „cyberbezpieczeństwo"
na decyzje budżetowe i organizacyjne 21

Cyberbezpieczeństwo w ochronie zdrowia – co zmieniają nowe przepisy 22

Ochrona zdrowia jako sektor szczególnego znaczenia 22
Zakres podmiotowy – kto podlega nowym obowiązkom z NIS 2 23
Wspólna podstawa obowiązków – systemowe
podejście do cyberbezpieczeństwa 24

Obowiązki podmiotów ważnych 25
Obowiązki podmiotów kluczowych 26
System zarządzania bezpieczeństwem informacji (SZBI)
– szerszy zakres i realne funkcjonowanie 26
Bezpieczeństwo łańcucha dostaw – wyraźnie wzmocnione wymagania 26
Incydenty – te same terminy, większa gotowość organizacyjna 27
Jaki incydent trzeba zgłaszać 28
Jak wygląda raportowanie incydentów w praktyce? 29
Odpowiedzialność kierownictwa i charakter zmian 30

Dojrzałość cyfrowa placówki medycznej – jak ją ocenić i co naprawdę pokazuje 32

Czym jest dojrzałość cyfrowa placówki medycznej 32
Ocena dojrzałości cyfrowej placówki medycznej – podejście praktyczne 33
Przykłady praktyczne oceny dojrzałości cyfrowej 34
Wnioski dla dyrektora placówki medycznej 35
Ocena dojrzałości cyfrowej dla dyrektora – najważniejsze obszary 35
Podsumowania 36
Lista kontrolna: co wchodzi w skład dojrzałości cyfrowej placówki medycznej 38

Cyfrowa transformacja w ochronie zdrowia

Cyfrowa transformacja w ochronie zdrowia nabiera tempa, ale bez kompetentnego personelu technologia pozostaje jedynie gadżetem. Sprawdź, jak budować zaufanie do innowacji, rozwijać umiejętności cyfrowe zespołu i skutecznie wdrażać nowoczesne rozwiązania w swojej placówce.

Diagnoza barier w cyfrowej transformacji ochrony zdrowia

Cyfrowa transformacja w ochronie zdrowia to proces, który obejmuje nie tylko wdrażanie technologii, ale także zmianę podejścia do organizacji pracy i zarządzania personelem. Placówki medyczne coraz częściej wykorzystują narzędzia oparte na sztucznej inteligencji i analizie danych, jednak sukces tych rozwiązań zależy od gotowości całego zespołu do ich stosowania.

Na drodze do pełnej cyfryzacji medycyny wciąż pojawia się wiele barier. WHO w raporcie „Przyspieszenie wdrażania rozwiązań cyfrowych w Europejskim Regionie WHO" zwraca uwagę na problemy infrastrukturalne, ograniczony dostęp do szkoleń i nadmierne obciążenie pracowników administracyjnych oraz klinicznych. W polskich realiach dodatkowym wyzwaniem jest fragmentaryczność systemów informatycznych, brak interoperacyjności i niejednolite standardy dokumentacji.

Dyrektorzy i właściciele placówek, którzy planują inwestycje w technologie, powinni rozpocząć od analizy zasobów i kompetencji zespołu. Warto także ocenić, które obszary działalności placówki mogą realnie zyskać na cyfryzacji – diagnostyka obrazowa, rejestracja, raportowanie, a może zarządzanie danymi medycznymi. Takie rozpoznanie pozwala uniknąć sytuacji, w której technologia staje się kosztownym, lecz mało użytecznym dodatkiem.

Jak rozwijać kompetencje cyfrowe personelu medycznego?

Rozwój kompetencji cyfrowych personelu medycznego to kluczowy element skutecznej transformacji technologicznej w placówkach ochrony zdrowia. Nawet najlepiej zaprojektowane rozwiązania informatyczne nie przyniosą oczekiwanych efektów, jeśli użytkownicy nie potrafią ich obsługiwać lub nie rozumieją ich potencjału.

Budowanie umiejętności cyfrowych powinno rozpocząć się od diagnozy potrzeb szkoleniowych. Dyrektorzy i kierownicy placówek powinni ustalić, które grupy zawodowe – lekarze, pielęgniarki, rejestratorki, pracownicy administracyjni – wymagają wsparcia w zakresie obsługi systemów IT, analizy danych czy cyberbezpieczeństwa. Dopiero na tej podstawie można zaplanować program edukacyjny dopasowany do poziomu doświadczenia uczestników i specyfiki danej jednostki.

Eksperci WHO podkreślają, że skuteczność szkoleń zależy od ich personalizacji i praktycznego charakteru. Programy ogólne, realizowane bez uwzględnienia realnych potrzeb, nie tylko nie przynoszą efektów, ale także mogą wzbudzać opór wobec cyfryzacji. Warto więc angażować uczestników w planowanie tematów i włączać do procesu wewnętrznych ambasadorów zmian – pracowników, którzy już dobrze znają narzędzia cyfrowe i mogą wspierać kolegów w nauce.

Stałe monitorowanie wyników szkoleń i analiza poziomu satysfakcji uczestników pozwalają utrzymać ich skuteczność. Placówki, które regularnie aktualizują programy edukacyjne i łączą je z oceną jakości pracy, szybciej osiągają dojrzałość cyfrową i zwiększają efektywność funkcjonowania całego zespołu.