SERWIS ZOZ.PL

ZARZĄDZANIE W OCHRONIE ZDROWIA



NIS2 w placówce medycznej

Praktyczny przewodnik dla szpitali, przychodni, laboratoriów i podwykonawców ochrony zdrowia

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

NIS2 w placówce medycznej
Praktyczny przewodnik dla szpitali, przychodni, laboratoriów i podwykonawców ochrony zdrowia
Copyright © Warszawa 2026 by Wiedza i Praktyka sp. z o.o.

Autorzy: Magdalena Pokrzycka-Walczak, Maciej Lipka
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: kwiecień 2026 r. .
ISBN: 978-83-8409-685-7
Kod produktu: 1BV0159

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 kwietnia 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

Wstęp 6

Rozdział 1. NIS2 w ochronie zdrowia – co weszło w życie 3 kwietnia 2026 r. 7

Rozdział 2. Kogo dotyczą nowe obowiązki 8

- Podmioty kluczowe i ważne w ochronie zdrowia 8
- Podmiot kluczowy a podmiot ważny – co to zmienia 9
- Szybki test: czy Twoja placówka może być PKW 9
- Najczęstsze błędy przy kwalifikacji 10

Rozdział 3. Wpis do wykazu PKW 11

- Obowiązek samoidentyfikacji 11
- Jakie dane przygotować do wniosku 11
- Jakie dokumenty warto mieć przygotowane 12
- Najczęstsze błędy przy wpisie 13

Rozdział 4. Jakie obowiązki trzeba wdrożyć w placówce 14

- SZBI i dokumentacja bezpieczeństwa 14
- KRK i wymagania wobec osób wykonujących zadania 15
- Zapewnienie przepływu informacji 15
- Obowiązki kierownika PKW 16
- Audyt 16

Rozdział 5. Zgłaszanie incydentów i sprawozdawczość 17

- Co to jest incydent poważny 17
- Terminy zgłoszeń: 24 h/72 h/1 miesiąc 18
- Co powinno zawierać zgłoszenie 18
- Co zgłaszać, a co tylko rejestrować 19
- Usuwanie podatności i dostęp do informacji o incydentach 19

Rozdział 6. NIS2 i RODO w jednym procesie 20

Jeden proces obsługi incydentu 20
Wspólny zespół i „teczka sprawy” 20
Komunikacja z pacjentami 21
Od kiedy trzeba realizować nowe obowiązki 22
Kary pieniężne dla placówki 22
Odpowiedzialność kierownika 23
Od kiedy grożą kary 24

Podsumowanie 25

Podstawa prawna 25

Wstęp

Placówka medyczna może otrzymać bardzo wysokie kary, jeśli nie dostosuje się do nowych wymogów cyberbezpieczeństwa. Dyrektywa NIS2, wdrożona do polskiego porządku prawnego przez nowelizację ustawy o krajowym systemie cyberbezpieczeństwa, zaostrza przepisy i nakłada nowe obowiązki na podmioty uznane za kluczowe i ważne. W ochronie zdrowia oznacza to konieczność ustalenia własnego statusu, uporządkowania dokumentacji, wdrożenia systemu zarządzania bezpieczeństwem informacji oraz przygotowania procedur zgłaszania incydentów.

Ten e-book został przygotowany z myślą o szpitalach, przychodniach, laboratoriach i podwykonawcach działających w sektorze ochrony zdrowia. Pokazuje, jak przeanalizować status placówki, kiedy trzeba wpisać się do wykazu podmiotów kluczowych i ważnych, jakie obowiązki należy wdrożyć oraz jak zorganizować obsługę incydentu, aby równolegle spełnić wymagania NIS2 i RODO.

W dalszej części:

- ustawę o krajowym systemie cyberbezpieczeństwa określamy skrótem **uksc**,
- ustawę z 23 stycznia 2026 r. zmieniającą uksc – jako **nowelizację**.

Rozdział 1. NIS2 w ochronie zdrowia – co weszło w życie 3 kwietnia 2026 r.

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa miała na celu wdrożenie dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555, czyli dyrektywy NIS2. Od 3 kwietnia 2026 r. w polskim systemie prawnym obowiązują zaktualizowane przepisy, które podnoszą standardy cyberbezpieczeństwa i nakładają nowe obowiązki na podmioty uznane za kluczowe i ważne.

W ochronie zdrowia temat ma szczególne znaczenie, ponieważ cyberatak może oznaczać nie tylko problem techniczny, lecz także realne zagrożenie dla ciągłości świadczeń, bezpieczeństwa danych i zdrowia pacjentów. Dlatego placówki medyczne muszą znać zasady kwalifikacji do kategorii PKW, obowiązki związane z organizacją cyberbezpieczeństwa, reguły raportowania incydentów oraz konsekwencje niewdrożenia wymaganych rozwiązań.

Dyrektywa NIS2 i wdrażające ją przepisy krajowe nie dotyczą wyłącznie największych podmiotów. Kwestia zaliczenia do kategorii podmiotów kluczowych i ważnych wymaga odrębnej analizy, a w praktyce nawet mała placówka powinna taką analizę przeprowadzić.

Rozdział 2.
Kogo dotyczą nowe obowiązki

Podmioty kluczowe i ważne w ochronie zdrowia

Uksc kieruje nowe obowiązki do podmiotów zaliczonych do kategorii podmiotów kluczowych lub ważnych, a także do ich kierowników. Przepisy przewidują złożone zasady klasyfikacji, wymagające analizy samej ustawy, jej załączników oraz innych przepisów sektorowych.

W przypadku podmiotów wykonujących działalność leczniczą najczęściej do kategorii PKW będą zaliczać się:

- podmioty lecznicze będące średnimi lub dużymi przedsiębiorstwami,
- inne podmioty udzielające świadczeń opieki zdrowotnej będące podwykonawcą dla PKW w sektorze ochrona zdrowia,
- świadczeniodawcy posiadający w swojej strukturze organizacyjnej Szpitalny Oddział Ratunkowy, Centrum Urazowe lub Centrum Urazowe dla Dzieci.

Przedsiębiorstwo zatrudniające mniej niż 50 pracowników i którego roczny obrót lub roczna suma bilansowa nie przekracza 10 mln euro, co do zasady nie będzie PKW. Nie oznacza to jednak, że mniejsza placówka może automatycznie wykluczyć taki status. W rzadszych przypadkach, ze względu na charakter działalności, właściwe organy mogą zakwalifikować do tej kategorii także inny podmiot wykonujący działalność leczniczą, np. gdy zostanie on zidentyfikowany jako podmiot krytyczny albo uznany za PKW przez organ właściwy do spraw cyberbezpieczeństwa.