Poradnik nabywcy

AI



Jesień 2026


AI
W ZDROWIU

Spis Treści

4. **Dlaczego powstał ten Poradnik?**
5. **Twórcy i Partnerzy Poradnika Nabywcy**
6. **O autorach**
8. **Komentarze ekspertów**
18. **Pytanie 1**
Czy na pewno AI jest najlepszym rozwiązaniem, czy też wystarczające jest inne narzędzie?
19. **Pytanie 2**
Czy AI spełnia wymagania prawne?
23. **Pytanie 3**
Czy AI jest skuteczna i jakie ma na to dowody?
28. **Pytanie 4**
Czy AI będzie działać w praktyce?
32. **Pytanie 5**
Czy Twój personel jest gotowy na AI?
35. **Pytanie 6**
Czy AI jest etyczna i wolna od dyskryminacji?
37. **Pytanie 7**
Czy dane medyczne będą przetwarzane zgodnie z prawem?
40. **Pytanie 8**
Czy rozwiązanie jest cyberbezpieczne?
43. **Pytanie 9**
Czy zapewnisz utrzymanie AI po wdrożeniu?
46. **Pytanie 10**
Czy znasz pełny koszt i długoterminową korzyść?
51. **Checklista Nabywcy AI,**
czyli 10 pytań przed podjęciem decyzji zakupowej
53. **Chcesz wiedzieć więcej**
bądź potrzebujesz wsparcia we wdrożeniu innowacji do swojej organizacji?
54. **Poznaj inne publikacje i inicjatywy**
współtworzone przez Koalicję AI i Innowacji w Zdrowiu oraz Polską Federację Szpitali.

Dlaczego powstał ten Poradnik?

Sztuczna inteligencja przestała być technologią przyszłości i stała się technologią teraźniejszości. Wspiera decyzje diagnostyczne lekarzy, pomaga przewidywać zapotrzebowanie na świadczenia, optymalizuje pracę personelu medycznego i przyspiesza odkrycia naukowe, które mogą zmienić życie pacjentów. Polska ochrona zdrowia stoi przed wyjątkową szansą: by nie tylko nadążyć za tym procesem, ale aktywnie go kształtować.

Jako Koalicja AI i innowacji w Zdrowiu obserwujemy, że warunki do masowego wdrożenia rozwiązań opartych na AI w polskim systemie ochrony zdrowia nigdy nie były bardziej sprzyjające. Rozwinięta infrastruktura e-zdrowia stanowi solidny fundament do budowania powszechnie dostępnych rozwiązań, a rodzimy sektor medtech wyróżnia się w skali Europy. Możliwości stwarzane przez te technologie są niezwykle ekscytujące, ale jednocześnie musimy być pewni, że produkty, które kupują nasze organizacje, spełniają najwyższe standardy bezpieczeństwa, jakości i skuteczności.

Rynek rozwiązań AI dla zdrowia rozwija się dynamicznie i nie zawsze w sposób przejrzysty. Wdrożenia, szczególnie gdy pochopnie realizowane, mogą nie przynieść oczekiwanych efektów, a w skrajnych przypadkach nieść ze sobą realne ryzyko dla pacjentów i organizacji. Dlatego tak ważne jest, by osoby odpowiedzialne za zakup i wdrożenie narzędzi AI wiedziały, jakie pytania zadawać i jak oceniać uzyskane odpowiedzi.

Ten poradnik powstał z myślą o każdym, kto uczestniczy w procesie podejmowania decyzji zakupowych dotyczących AI w ochronie zdrowia: dyrektorach szpitali i placówek POZ, liderach klinicznych, menedżerach transformacji cyfrowej, specjalistach ds. zamówień publicznych, a także decydentach po stronie płatnika i regulatora. Oferuje praktyczne wskazówki i konkretne pytania, które warto zadać przed i w trakcie każdego procesu zakupowego.

Wierzymy, że świadomy, dobrze przygotowany nabywca to najsilniejszy motor odpowiedzialnego rozwoju AI w polskiej ochronie zdrowia. Mamy nadzieję, że ten poradnik stanie się dla Państwa praktycznym narzędziem nie tylko przy pierwszym zakupie, ale przy każdej kolejnej decyzji dotyczącej AI[1].

[1] Poradnik został opracowany na bazie NHS AI Buying Guide (NHSx), uzupełniony o wymogi AI Act (UE 2024/1689), rozporządzenie Parlamentu Europejskiego Rady (UE) 2017/745 (MDR), dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 (NIS2) i rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO).
Poradnik został przygotowany w stanie prawnym na: Październik 2026 r.

Twórcy i Partnerzy Poradnika Nabywcy

TWÓRCY PORADNIKA NABYWCY

AI W ZDROWIU

WZDROWIU

PFSz Polska Federacja Szpitali

PARTNER PRAWNY

sotlaw

PARTNER WSPIERAJĄCY

Teleradiologia 24 Grupa Diagnostyka

KOORDYNACJA PROJEKTU



Lek. Ligia Kornowska
Liderka Koalicji AI
i innowacji w Zdrowiu



Karolina Kornowska
Dyrektor Operacyjna wZdrowiu,
Dyrektor ds. Organizacyjnych Polskiej Federacji Szpitali, Liaison Officer na Polskę w Europejskiej Federacji Szpitali HOPE



Prof. Jarosław J. Fedorowski
Prezes Polskiej Federacji Szpitali,
Gubernator na Polskę w Europejskiej Federacji Szpitali HOPE,
Skarbnik i członek Komitetu Wykonawczego Zarządu Światowej Federacji Szpitali
Profesor University of Vermont College of Medicine,
Profesor Akademii Zamojskiej

O autorach

Koalicja AI i innowacji w zdrowiu – inicjatywa mająca na celu wykorzystanie pełnego potencjału innowacji i sztucznej inteligencji w zdrowiu oraz wspieranie cyfrowej transformacji. Koalicja stawia sobie za cel kształtowanie polityki rozwoju sztucznej inteligencji i innowacji w polskim systemie ochrony zdrowia oraz stworzenie środowiska umożliwiającego szybkie i powszechne korzystanie przez polski system ochrony zdrowia z najnowszych osiągnięć AI. Koalicja AI i innowacji w zdrowiu podejmuje liczne działania mające na celu popularyzację innowacji w polskim systemie ochrony zdrowia. Działania te mają charakter wszechstronny, zarówno po stronie regulacyjnej – tworzenie sektorowych polityk publicznych, jak i po stronie technologicznej – wykorzystywanie oraz wspieranie prac badawczo-rozwojowych nad technologiami umożliwiającymi zastosowanie innowacji w opiece medycznej. Do Koalicji należy ponad 150 wiodących krajowych i globalnych podmiotów zaangażowanych w tworzenie i wdrażanie algorytmów AI. Koalicja ma charakter grupy roboczej. Koalicja prowadzi merytoryczny dialog ze stroną publiczną. Więcej informacji: http://aiwzdrowiu.pl

Polska Federacja Szpitali (PFSz) - ogólnopolska organizacja pracodawców zrzeszająca Szpitale niezależnie od ich struktury własnościowej, wielkości, profilu specjalistycznego, lokalizacji czy modelu działania. Polska Federacja Szpitali (PFSz) zrzesza bezpośrednio ponad 250 Szpitali, a poprzez porozumienia z lokalnymi i sektorowymi związkami Szpitali funkcjonuje jako organizacja parasolowa w sumie dla ponad 500 Szpitali. Atut PFSz stanowi także spora grupa członków wspierających: liczących się firm krajowych i międzynarodowych, ekspertów systemu ochrony zdrowia oraz ambasadorów PFSz. PFSz jest pełnoprawnym członkiem Europejskiej Federacji Szpitali HOPE z siedzibą w Brukseli, która zrzesza prawie 80% zasobów szpitalnych w Unii Europejskiej, a także Światowej Federacji Szpitali IHF – jedynej globalnej organizacji szpitali – z siedzibą w Genewie. PFSz jest głosem polskich szpitali na forum krajowym, europejskim oraz światowym. Więcej informacji: http://www.pfsz.org/

O autorach

wZdrowiu - zespół ekspertów, zajmujących się wspieraniem wdrażania innowacji w ochronie zdrowia, doradztwem technologicznym, prawnym oraz marketingowym, organizacją eventów z zakresu healthcare oraz publikowaniem dokumentów dotyczących innowacji w sektorze ochrony zdrowia. Kontakt: Karolina Kornowska, COO, karolina.kornowska@wzdrowiu.com

dotlaw - w dotlaw projektujemy architekturę prawną dla firm technologicznych i podmiotów sektora ochrony zdrowia. Prowadzimy firmy przez regulacje AI Act, ochronę danych medycznych i wymagania regulacyjne dot. rejestracji wyrobów medycznych. Zamiast prawniczego żargonu dostarczamy konkretne rekomendacje biznesowe: co zrobić, w jakim terminie i z jakim skutkiem. Działamy blisko technologii i blisko biznesu, żeby przełomowe rozwiązania trafiały do gabinetów lekarskich i placówek medycznych szybko i bezpiecznie.

Diagnostyka Teleradiologia24 - od 2008 roku tworzymy teleradiologię opartą na jakości, bezpieczeństwie i odpowiedzialności medycznej. Łączymy placówki medyczne z siecią radiologów, zapewniając zdalną diagnostykę obrazową niezależnie od miejsca i trybu pilności badania. Rozwijamy autorski system RADONE, który integruje i wspiera cały proces diagnostyczny – od przesłania badania po diagnozę radiologiczną. Działamy zgodnie ze standardami ISO 9001 i ISO 27001 poddając proces teleradiologii niezależnej zewnętrznej certyfikacji. Technologię traktujemy jako narzędzie – naszym celem jest bezpieczna, sprawna i dostępna diagnostyka obrazowa dla pacjentów i placówek w całej Polsce.

Komentarze ekspertów

Agencja Oceny Technologii Medycznych i Taryfikacji

Najpierw ramy, potem zakup – doświadczenia instytucji publicznej

„Poradnik Nabywcy" słusznie rozpoczyna się od pytania, czy sztuczna inteligencja (AI) jest właściwym rozwiązaniem. Z perspektywy Agencji Oceny Technologii Medycznych i Taryfikacji warto jednak postawić jeszcze jedno, wcześniejsze pytanie: czy organizacja jest gotowa na korzystanie z AI? W praktyce pracownicy często sięgają po modele językowe, korzystając z prywatnych kont. Brak jasno określonych zasad nie eliminuje takiego zjawiska, lecz sprawia, że wykorzystywanie AI odbywa się poza kontrolą organizacji (tzw. shadow AI). Choć poradnik koncentruje się przede wszystkim na rozwiązaniach klinicznych, warto pamiętać, że w instytucjach publicznych, w tym również w szpitalach, pierwszym wdrażanym narzędziem AI bywa rozwiązanie ogólnego przeznaczenia.

W AOTMiT wdrażanie sztucznej inteligencji rozpoczęliśmy od stworzenia odpowiednich ram organizacyjnych i prawnych, które pozwalają korzystać z nowych technologii w sposób bezpieczny, świadomy i zgodny z obowiązującymi przepisami. Pierwszym krokiem było przyjęcie zarządzenia określającego politykę korzystania z narzędzi AI, uwzględniającą wymagania AI Act oraz RODO. Zgodnie z art. 4 AI Act obowiązek zapewnienia odpowiedniego poziomu kompetencji w zakresie AI spoczywa na podmiotach stosujących te systemy od 2 lutego 2025 r., niezależnie od tego, czy dane narzędzie jest wyrobem medycznym.

Powołaliśmy również interdyscyplinarny zespół, w którego skład wchodzą prawnicy, analitycy, specjaliści IT oraz Inspektor Ochrony Danych. Każde narzędzie przechodzi określoną ścieżkę oceny, obejmującą wpis do rejestru, analizę warunków licencyjnych i umowy powierzenia przetwarzania danych, ocenę ryzyka oraz DPIA. Na tej podstawie zespół przygotowuje rekomendację wskazującą sposób i warunki korzystania z narzędzia, w tym dopuszczalny zakres przetwarzania danych.

W ten sposób dopuściliśmy do użytku asystenta AI zintegrowanego z pakietem biurowym w wersji enerprise oraz modele językowe kilku innych dostawców, również w wersjach przeznaczonych dla firm. Wybrane rozwiązania zapewniają, że przekazywane im dane nie są wykorzystywane do trenowania modeli, a z dostawcami możliwe jest zawarcie umów powierzenia przetwarzania danych. Obecnie rozwijamy te działania, pracując nad tworzeniem agentów AI oraz automatyzację procesów (workflow).

Dotychczasowe doświadczenia AOTMiT związane z wdrażaniem narzędzi AI pozwoliły nam sformułować trzy ważne wnioski, na które warto zwrócić uwagę przed podjęciem decyzji o ich wykorzystaniu:

Agencja Oceny Technologii Medycznych i Taryfikacji

1. Czytaj licencję, a nie tylko materiały handlowe

W przypadku jednego z analizowanych narzędzi okazało się, że zapytania kierowane do wyszukiwarki internetowej wykraczają poza zakres umowy powierzenia przetwarzania danych. Dlatego warto dokładnie sprawdzić, jak działają poszczególne komponenty rozwiązania, w tym funkcje wyszukiwania, modele dostarczane przez podwykonawców, usługi dalszych podmiotów przetwarzających dane (subprocesorów) czy funkcje udostępniane w wersjach testowych. Należy również zwrócić uwagę na możliwość przekazywania danych poza UE. Ryzyko związane z lokalizacją danych oraz ciągłością ich ochrony prywatnej to dwie odrębne kwestie, które powinny zostać uwzględnione w ocenie skutków dla ochrony danych (DPIA) oraz ocenie skutków transferu danych (TIA).

2. Dopuszczenie narzędzia do użytku nie musi być decyzją ostateczną

W AOTMiT rekomendacje dot. korzystania z narzędzi AI mają charakter warunkowy i podlegają okresowym przeglądom. Gdy pojawiły się nowe informacje wpływające na ocenę ryzyka, zdecydowaliśmy się ponownie przeanalizować warunki korzystania z jednego z rozwiązań. Po przeprowadzeniu testów na fikcyjnych danych oraz wdrożeniu etykiet poufności i mechanizmów zapobiegania utracie danych (DLP) wydaliśmy nową rekomendację, zawężającą zakres dopuszczalnego wykorzystania narzędzia. Takie podejście nie oznacza niepowodzenia wdrożenia. Przeciwnie – pokazuje, że możliwość weryfikacji i zmiany wcześniejszych decyzji, jest ważnym elementem bezpiecznego korzystania z AI.

3. AI to element systemu bezpieczeństwa, a nie osobny zakup

W Agencji narzędzia AI włączamy w istniejący system zarządzania bezpieczeństwem informacji i ciągłością działania. Obejmuje on m.in. mechanizmy zapobiegania utracie danych, które kontrolują dane wprowadzane do asystenta AI, oraz monitorowanie bezpieczeństwa. Wdrożenie AI bez odpowiednich zabezpieczeń może bowiem zwiększyć ryzyko cyberataków.
Doświadczenia związane z awariami dużych dostawców pokazują również, jak ważne jest zapewnienie ciągłości pracy. Dlatego warto rozważyć korzystanie z więcej niż jednego narzędzia AI. Takie podejście nie tylko ogranicza skutki ewentualnych awarii, ale także zmniejsza zależność od jednego dostawcy.

Z kolei podczas przygotowywania zapytania ofertowego na agenta AI oceniliśmy również opracowany przez nas prototyp, stosując wobec niego te same kryteria co w przypadku ofert zewnętrznych. Okazało się, że jego możliwości były niewiele mniejsze niż proponowanych rozwiązań. Takie porównanie pozwala lepiej ocenić, za jakie funkcjonalności i korzyści organizacja rzeczywiście płaci.

Świadomy nabywca AI to nie tylko organizacja, która potrafi zadawać dostawcom właściwe pytania, ale przede wszystkim taka, która ma jasno określone zasady podejmowania decyzji o korzystaniu z AI i wie, jak skutecznie nadzorować jej działanie.



dr n. med. Przemysław Rzodkiewicz
Zastępca Prezesa wykonującego zadania Prezesa AOTMiT.

Centrum e-Zdrowia

Poradnik przygotowany przez Koalicję AI i Innowacji w Zdrowiu, Polską Federację Szpitali oraz wZdrowiu trafia w bardzo ważny moment rozwoju polskiej ochrony zdrowia. Pokazuje, że wdrażanie sztucznej inteligencji staje się rzeczywistością. Potwierdzają to również wyniki badań, które od kilku lat prowadzą Centrum e-Zdrowia wraz z Ministerstwem Zdrowia. Tegoroczna IX edycja "Badania stopnia informatyzacji podmiotów wykonujących działalność leczniczą" pokazuje, że obecnie narzędzia wykorzystujące sztuczną inteligencję stosuje 7,3% placówek w diagnostyce i leczeniu, 5,9% w zarządzaniu oraz 4,7% w obsłudze pacjenta. Najczęściej AI wspiera diagnostykę obrazową RTG i tomografii komputerowej. Jednocześnie aż 40,9% badanych szpitali planuje wdrożenie rozwiązań AI w ciągu najbliższych 12 miesięcy.

Najnowsze wyniki raportu „Granice zaufania. AI w ochronie zdrowia z perspektywy pacjentów i lekarzy" opracował z kolei Instytut Badań Pollster w ramach inicjatywy AI Health Horizons, pod patronatem Okręgowej Izby Lekarskiej w Warszawie. Badanie przeprowadzono w lipcu i sierpniu 2026 roku na próbie 1039 dorosłych Polaków oraz 288 lekarzy. Pokazało ono, że wobec sztucznej inteligencji w ochronie zdrowia zarówno pacjenci, jak i lekarze mają tyle samo obaw, co nadziei. Społecznym oczekiwaniem pozostaje możliwość kontaktowania się z drugim człowiekiem, rozmowa z nim, a nie wyłącznie z maszyną. Badania pokazują również, że bardziej niż AI ufamy słowom i decyzjom lekarza. Gdyby diagnoza AI i lekarza była sprzeczna, 62% pacjentów zaufałoby lekarzowi, a tylko 4% sztucznej inteligencji. Jednocześnie badani nie mają wątpliwości, że AI może pewne procesy ułatwić i przyspieszyć. Jak pokazały te same badania, 62% pacjentów i 66% lekarzy uważa, że technologia może pomóc medykom poświęcić więcej czasu na wizytę. Aż 90% lekarzy i 73% pacjentów wskazuje natomiast, że wdrażaniu AI muszą towarzyszyć jasno określone standardy, nadzór i określenie odpowiedzialności.

Doświadczenia Centrum e-Zdrowia we wdrażaniu rozwiązań opartych na AI pokazują, że każdy świadomy nabywca tego typu narzędzi powinien zadać sobie szereg istotnych pytań. Odpowiedzialne wykorzystanie sztucznej inteligencji wymaga bowiem nie tylko zgodności z przepisami, ale również odpowiedniego przygotowania organizacyjnego, kompetencji cyfrowych personelu i zdolności do oceny skuteczności wdrażanych narzędzi.

Te założenia są też fundamentem szkoleń z podstaw AI, które prowadzimy dla pracowników ochrony zdrowia w ramach Akademii Centrum e-Zdrowia. Dotyczą one nie tylko obsługi konkretnych narzędzi, ale też kwestii prawnych i etycznych. W szkoleniach wzięło udział już 1656 osób, głównie personel szpitali, jak i POZ oraz AOS, a kolejne terminy planowane są na styczeń i luty 2027 roku. Ogromna popularność tych szkoleń pokazuje, jak duża jest potrzeba wiedzy wśród pracowników ochrony zdrowia i jak bardzo potrzebne są inicjatywy, które dostarczają sprawdzonych, rzetelnych informacji na temat AI.

Dlatego właśnie „Poradnik Nabywcy AI" to wartościowe narzędzie dla kadry zarządzającej, specjalistów ds. zamówień publicznych, zespołów IT oraz wszystkich osób odpowiedzialnych za rozwój cyfrowy placówek medycznych. Im bardziej świadome będą decyzje dotyczące zakupu i wdrażania rozwiązań AI, tym większa szansa, że technologie te przełożą się na poprawę jakości opieki zdrowotnej, efektywne wykorzystanie zasobów i lepsze doświadczenia pacjentów.



Jarosław Sot
Dyrektor Centrum
e-Zdrowia

Ministerstwo Zdrowia

Jak ocenia Pan potrzebę praktycznych, usystematyzowanych narzędzi wspierających placówki medyczne w świadomych decyzjach zakupowych dotyczących AI?

Szpitale coraz aktywniej sięgają po rozwiązania oparte na AI i budują własne doświadczenie w ich wdrażaniu. Wraz z dojrzewaniem rynku zmienia się jednak charakter decyzji, które należy podejmować. Dziś coraz ważniejsze jest nie tylko to, jak działa dane rozwiązanie, ale dla jakiego problemu klinicznego zostało stworzone, na jakich danych potwierdzono jego skuteczność i czy rzeczywiście sprawdzi się w konkretnym środowisku placówki medycznej.

Wspólne, praktyczne narzędzia mogą bardzo dobrze wspierać ten proces i porządkować kryteria oceny. Dają też silniejszą pozycję w rozmowie z dostawcą technologii, ponieważ przenoszą dyskusję z poziomu możliwości technologii na jej udokumentowaną wartość kliniczną i bezpieczeństwo. Z perspektywy systemowej sprzyja to również budowaniu dojrzałego rynku AI, w którym innowacje konkurują przede wszystkim jakością i wartością, jaką wnoszą do opieki nad pacjentem.

Jakie wyzwania regulacyjne i organizacyjne uważa Pan za największą barierę dla szpitali wdrażających AI i w jaki sposób tego typu poradnik może pomóc je adresować?

Szczególnie istotne jest dziś właściwe rozłożenie odpowiedzialności pomiędzy producentem technologii a podmiotem leczniczym. W przypadku rozwiązań opartych na AI zgodność z MDR czy AI Act oraz stosowanie produktu zgodnie z jego przewidzianym zastosowaniem są punktem wyjścia. W praktyce równie istotne jest jednak środowisko, w którym algorytm będzie wykorzystywany, ponieważ sposób jego integracji z systemami szpitalnymi, charakter danych oraz zastosowanie wyniku algorytmu w procesie klinicznym mogą wpływać na profil ryzyka i warunki bezpiecznego stosowania. Dlatego tak ważny jest nadzór nad rozwiązaniem również po jego uruchomieniu. Przygotowany poradnik dostarcza niezbędną wiedzę i pomaga przełożyć te zależności na konkretne i praktyczne działania w warunkach danego podmiotu. Takie podejście daje wszystkim większą pewność w korzystaniu z AI i ułatwia szersze wdrażanie technologii, które potwierdzają swoją skuteczność w rzeczywistej praktyce klinicznej.

Czy resort planuje promować korzystanie z takich narzędzi wśród publicznych podmiotów leczniczych jako element szerszej strategii cyfryzacji sektora?

W polityce cyfrowej ochrony zdrowia coraz większy nacisk kładziemy na wykorzystanie danych i zbudowanych już zasobów cyfrowych do poprawy jakości i dostępności świadczeń. AI jest jednym z kluczowych kierunków tego rozwoju i chcemy tworzyć warunki, w których wartościowe rozwiązania mogą przechodzić od pojedynczych wdrożeń do szerszego zastosowania w systemie. Uruchomiona przez nas Platforma Usług Inteligentnych i pierwsze zastosowania AI w radiologii są praktycznym przykładem tego kierunku. Wraz z nimi chcemy rozwijać wspólne standardy dobrego wdrażania AI. Poradnik może się stać użyteczną mapą drogową zarówno przy rozwiązaniach pozyskiwanych samodzielnie przez poszczególne podmioty, jak i udostępnianych centralnie. W każdym z tych modeli pozostaje bowiem wspólny cel, czyli takie wykorzystanie technologii, które można bezpiecznie rozwijać, oceniać na podstawie efektów i z czasem skalować tam, gdzie są najbardziej potrzebne pacjentom i personelowi medycznemu.



Tomasz Maciejewski
Podsekretarz Stanu
Ministerstwa Zdrowia

Instytut Matki i Dziecka

Wdrażanie sztucznej inteligencji wymaga przede wszystkim odpowiedzialnego podejścia do zarządzania zmianą. Samo udostępnienie personelowi nowego narzędzia nie gwarantuje właściwego wykorzystywania ani dostarczenia oczekiwanych efektów. Każde wdrożenie powinno być poprzedzone analizą potrzeb, oceną wpływu na organizację pracy oraz przygotowaniem zespołów do korzystania z nowych możliwości. Dlatego cieszy mnie powstanie „Poradnika nabywcy AI", który może być ważnym wsparciem dla placówek medycznych planujących sięgać po tego rodzaju rozwiązania.

W Instytucie Matki i Dziecka traktujemy innowacje jako element rozwoju całej organizacji. W proces ich wdrażania muszą być zaangażowani nie tylko specjaliści IT, ale przede wszystkim pracownicy medyczni i osoby odpowiedzialne za poszczególne obszary działalności szpitala. To oni najlepiej znają codzienne wyzwania i potrafią ocenić, czy proponowane rozwiązanie rzeczywiście odpowiada na potrzeby praktyki klinicznej i organizacyjnej.

Sztuczna inteligencja powinna pozostać narzędziem wspierającym człowieka, a odpowiedzialność za decyzje diagnostyczne, terapeutyczne czy organizacyjne musi należeć do profesjonalistów. Dlatego rozwijanie kompetencji personelu w zakresie świadomego korzystania z AI należy traktować jako inwestycję strategiczną – równie istotną jak rozwój infrastruktury czy zakup nowych technologii. Ważne jest, by pracownicy rozumieli nie tylko możliwości tych narzędzi, lecz także ich ograniczenia, a kwestie bezpieczeństwa pacjentów i ochrony danych były uwzględniane na każdym etapie wdrożenia.

Jestem przekonana, że przyszłość ochrony zdrowia będzie opierała się na coraz lepszej współpracy ludzi i technologii. Zadaniem liderów szpitali jest tworzenie warunków, w których będzie ona bezpieczna, odpowiedzialna i przyniesie realne korzyści pacjentom oraz personelowi. Punktem wyjścia do wdrażania innowacji powinno być zawsze pytanie nie o to, co dana technologia potrafi, ale jak może pomóc nam lepiej realizować misję szpitala.

Gotowość organizacji na AI należy więc oceniać nie tylko przez pryzmat infrastruktury i dostępu do nowych rozwiązań, ale przede wszystkim zdolności do świadomego i odpowiedzialnego wprowadzania zmian. Nowoczesny szpital to nie ten, który najszybciej wdraża technologie, lecz ten, który potrafi wykorzystać je z korzyścią dla pacjentów i personelu.



Dr n. med. Alicja Karney
Dyrektor Naczelna
Instytut Matki i Dziecka

Instytut Matki i Dziecka

Cyberbezpieczeństwo rozwiązania AI nie może być oceniane w oderwaniu od całego środowiska IT szpitala. Wdrożenie nowej technologii oznacza nie tylko udostępnienie jej użytkownikom, ale również włączenie do infrastruktury, w której funkcjonują systemy medyczne, administracyjne i procesy bezpośrednio związane z opieką nad pacjentem.

Ocena bezpieczeństwa powinna rozpocząć się jeszcze przed podjęciem decyzji zakupowej i być prowadzona wspólnie przez zespoły złożone ze specjalistów ds. IT, cyberbezpieczeństwa, medyków i osoby odpowiedzialne za wdrożenie innowacji.

Istotne jest zrozumienie, jakie dane przetwarza wprowadzane rozwiązanie, gdzie są one przechowywane, z jakimi systemami komunikuje się innowacja i jakie zależności tworzy. Szczególnej uwagi wymagają rozwiązania wykorzystujące zewnętrzną infrastrukturę chmurową oraz modele AI, których sposób przetwarzania danych nie zawsze jest dla użytkownika oczywisty.

Nie możemy przy tym traktować bezpieczeństwa jako jednorazowego warunku dopuszczenia produktu do szpitala. To proces obejmujący cały cykl życia technologii: od testów przedwdrożeniowych, przez kontrolowane uruchomienie, po monitorowanie działania, aktualizacje i reagowanie na zmieniające się zagrożenia. Ważne jest również zachowanie kontroli nad danymi i możliwość szybkiego odłączenia rozwiązania bez zakłócania ciągłości pracy szpitala.

Jako osoba odpowiedzialna za cyberbezpieczeństwo i wdrażanie innowacji w Instytucie Matki i Dziecka, na pytanie „Czy rozwiązanie jest cyberbezpieczne?" nigdy nie oczekuję prostej odpowiedzi „tak" lub „nie". Interesują mnie przede wszystkim dowody. Cyberbezpieczeństwo nie jest deklaracją marketingową, ale zbiorem konkretnych procesów, zabezpieczeń i procedur, które można zweryfikować.

Należy pamiętać, że innowacja nie może tworzyć nowego ryzyka dla pacjentów i organizacji. Jako MCSC Hospital Leadership Innovation tworzymy ekosystem innowatorów otwartych na wprowadzanie do szpitali nowoczesnych rozwiązań. Kluczem jest znalezienie równowagi między otwartością na nowe technologie a odpowiedzialnością za bezpieczeństwo środowiska, w którym mają one funkcjonować. Dopiero rozwiązanie, które przechodzi taką weryfikację, ma szansę stać się realnym wsparciem dla szpitala, a nie kolejnym źródłem podatności.



Radosław Nowak
Pełnomocnik Dyrektora ds.
IT i Cyberbezpieczeństwa
Kierownik Działu Wdrożeń
– Centrum Innowacji i
Sztucznej Inteligencji
Instytut Matki i Dziecka

Instytut Matki i Dziecka

Z perspektywy komunikacji i zarządzania innowacjami największym błędem jest traktowanie wdrożenia AI wyłącznie jako projektu technologicznego. Tymczasem jest to przede wszystkim zmiana organizacyjna, której powodzenie w dużej mierze zależy od ludzi i ich zaufania do nowego rozwiązania.

W dyskusji o gotowości szpitali na AI często koncentrujemy się na kompetencjach cyfrowych personelu, pomijając znaczenie kultury organizacyjnej. To ona wpływa na otwartość pracowników na testowanie nowych rozwiązań, gotowość do dzielenia się wątpliwościami i zgłaszania problemów. Dialog z personelem jest szczególnie istotny, gdyż lekarze, pielęgniarki i przedstawiciele innych zawodów medycznych pracują w środowisku wysokiego ryzyka i dużej odpowiedzialności. Ich ostrożność wobec nowych technologii jest naturalna i powinna być uwzględniana w procesie wdrożenia.

Skuteczna komunikacja wokół AI nie powinna opierać się na zachwycie nad samą technologią. Obecność algorytmu w szpitalu nie jest jeszcze oznaką postępu. Liczy się to, czy rozwiązanie odpowiada na rzeczywisty problem i przynosi korzyści w codziennej pracy. Może to być na przykład oszczędność czasu, ograniczenie obowiązków administracyjnych czy poprawa jakości opieki nad pacjentem. Ważne, aby mówić o tych efektach konkretnie, bez pomijania ograniczeń i ryzyka związanego z wykorzystaniem AI.

W MCSC Hospital Leadership Innovation podkreślamy, że skuteczne wdrażanie innowacji wymaga współpracy różnych środowisk i uwzględnienia zarówno potrzeb placówki, jak i osób, które będą korzystać z nowych rozwiązań. O sukcesie nie decyduje liczba wdrożonych narzędzi AI, ale realna zmiana, jaką przynoszą one w funkcjonowaniu szpitala.



Monika Dobrzeniecka
Head of Communications
MCSC Hospital Leadership Innovation
Dział Wdrożeń –
Centrum Innowacji
i Sztucznej Inteligencji
Instytut Matki i Dziecka

Ministerstwo Cyfryzacji

Publikacja w przystępny dla czytelnika sposób omawia kwestie, które należy wziąć pod uwagę przy planowaniu zakupu i wdrożenia rozwiązania wykorzystującego sztuczną inteligencję w ochronie zdrowia. Jej istotną zaletą jest holistyczne podejście.

Podstawowe założenia są zgodne z kierunkiem działań Ministerstwa Cyfryzacji na rzecz bezpiecznego, odpowiedzialnego i zorientowanego na człowieka rozwoju AI.

Poradnik promuje podejmowanie decyzji zakupowych na podstawie rzeczywistych potrzeb organizacji i dowodów skuteczności. Zwraca uwagę na obowiązujące regulacje i ich nadchodzące zmiany. Ponadto w poradniku poświęcono miejsce praktykom zwiększającym skuteczność wdrożenia, takim jak zarządzanie zmianą i przygotowanie personelu, a także zagadnieniom związanym z długoterminowym utrzymaniem rozwiązań AI, monitorowaniem ich skuteczności oraz oceną całkowitych kosztów wdrożenia. Przyjęta formuła dziesięciu kluczowych pytań nadaje publikacji przejrzystą strukturę i ułatwia praktyczne wykorzystanie poradnika w procesie podejmowania decyzji zakupowych.

Ministerstwo Rozwoju i Technologii

Sztuczna inteligencja staje się jednym z kluczowych czynników zwiększających innowacyjność i konkurencyjność polskiej gospodarki. Jej potencjał nie wynika jednak wyłącznie z dostępności coraz bardziej zaawansowanych technologii, lecz w równie istotnym stopniu, z umiejętności ich skutecznego wykorzystania. Szczególne znaczenie ma to w niezwykle skomplikowanym sektorze ochrony zdrowia, w którym rozwiązania AI mogą wspierać zarówno procesy organizacyjne, jak i działalność medyczną, a jednocześnie wymagają szczególnej dbałości o **jakość, bezpieczeństwo i wiarygodność**.

Z perspektywy Ministerstwa Rozwoju i Technologii istotne jest tworzenie warunków sprzyjających rozwojowi innowacyjnych przedsiębiorstw oraz zwiększaniu zdolności polskiej gospodarki do absorpcji nowych technologii. Szczególną wagę przykładamy do budowy konkurencyjnego ekosystemu AI, współpracy nauki, biznesu i administracji oraz odpowiedzialnego upowszechniania zastosowań tej technologii.

Ważnym elementem tego procesu jest nie tylko wspieranie dostawców innowacyjnych rozwiązań, lecz także wzmacnianie kompetencji ich potencjalnych odbiorców. Świadome decyzje zakupowe, oparte na rzeczywistych potrzebach organizacji, przejrzystych kryteriach oceny i weryfikowalnych rezultatach, sprzyjają efektywnemu wykorzystaniu środków oraz rozwojowi dojrzałego rynku technologicznego. Szczególnie istotne jest uwzględnianie całkowitych kosztów wdrożenia i utrzymania, możliwości integracji z istniejącą infrastrukturą, jakości danych oraz zdolności organizacji do skutecznego wykorzystania zakupionych narzędzi.

„Poradnik Nabywcy AI" odpowiada na te wyzwania, dostarczając praktycznych wskazówek wspierających ocenę dostępnych rozwiązań i ograniczanie ryzyka nieefektywnych wdrożeń. Upowszechnianie takiego podejścia może przyczyniać się do budowania zaufania do technologii AI, stymulowania popytu na rozwiązania wysokiej jakości oraz zwiększania skali ich zastosowania w polskiej gospodarce. W dłuższej perspektywie to właśnie połączenie innowacyjności przedsiębiorstw ze świadomym i odpowiedzialnym podejściem odbiorców technologii będzie jednym z warunków pełnego wykorzystania potencjału nowoczesnych technologii.

Adam Janicki
Specjalista ds. wsparcia procesów transformacji
w przedsiębiorstwach, Wydział Transformacji
Cyfrowej Przemysłu, Departament
Innowacyjności i Polityki Kosmicznej

Narodowe Centrum Badań i Rozwoju

Z perspektywy Narodowego Centrum Badań i Rozwoju cenne są inicjatywy, które pomagają innowacjom przejść od pomysłu do odpowiedzialnego wdrożenia i zastosowania w praktyce rynkowej. Wspieramy bowiem rozwój nowych technologii, ale też jesteśmy świadomi, że ich powodzenie zależy także od świadomego odbiorcy, który potrafi rozpoznać wartość rozwiązania.

W ochronie zdrowia ma to szczególne znaczenie. Sztuczna inteligencja może poprawiać diagnostykę, organizację pracy i dostępność świadczeń, lecz sama etykieta „AI" nie jest dowodem skuteczności narzędzia. Jednocześnie menedżer placówki nie musi być ekspertem od algorytmów. Powinien jednak wiedzieć, o co zapytać dostawcę, jakie dowody sprawdzić, a przede wszystkim – gdzie mogą kryć się koszty lub ryzyka niewidoczne podczas efektownej prezentacji.

Dlatego dobrze, że „Poradnik nabywcy AI" trafia na rynek. Jego siłą jest prostota i klarowność. Prowadzi przez najważniejsze pytania dotyczące sensu zakupu, skuteczności, danych, bezpieczeństwa, wdrożenia, personelu, kosztów i utrzymania rozwiązania. Pokazuje też, że „kupowanie AI" ma inną specyfikę niż nabycie typowego urządzenia medycznego czy standardowego oprogramowania.

Poradnik najlepiej potraktować jako mapę przed rozpoczęciem procesu zakupowego. Porządkuje temat, pomaga przygotować dialog wewnątrz organizacji i podpowiada, o co zapytać dostawcę. Konkretna decyzja będzie już wymagała osobnej analizy prawnej, technicznej i organizacyjnej, dostosowanej do potrzeb danej placówki, lecz najpierw trzeba na cały proces spojrzeć strategicznie, w czym właśnie pomaga poradnik.

Polska ochrona zdrowia potrzebuje nie tylko większej liczby innowacji i nowych narzędzi, lecz także właściwych decyzji o ich wyborze i wdrażaniu. Świadoma decyzja sprzyja jakości, ogranicza ryzyko nietrafionych zakupów i pomaga wartościowym technologiom znaleźć miejsce w codziennej praktyce. Ten poradnik jest potrzebnym i pierwszym krokiem w tym kierunku.



dr Piotr W. Zawadzki
Ekspert operacyjny,
Dział Zarządzania
Strategicznego
Narodowe Centrum
Badań i Rozwoju

Pytanie 1

Czy na pewno AI jest najlepszym rozwiązaniem, czy też wystarczające jest inne narzędzie?

1. **Problem wymaga analizy danych lub realizacji zadań, w których zastosowanie AI może przynieść większą skuteczność lub oszczędność czasu niż dostępne alternatywy.**
   Dobra decyzja zakupowa zaczyna się od problemu, nie od technologii. Zanim organizacja zdecyduje się na wdrożenie AI, powinna odpowiedzieć na jedno fundamentalne pytanie: czy ten problem rzeczywiście wymaga AI, czy wystarczy inne prostsze rozwiązanie?

2. **Dostępne są dane wystarczającej jakości, ilości i reprezentatywności, by umożliwić trenowanie / działanie algorytmu**
   Kluczowa jest również odpowiedź na pytanie czy mamy dane, które są odpowiednie do działania AI.AI jest tak dobra, jak dane, na których działa. Niekompletne, niespójne, stronnicze lub niereprezentatywne zbiory danych mogą sprawić, że algorytm będzie działał pozornie poprawnie, ale systematycznie będzie podejmował błędne decyzje.

3. **Zweryfikowano, że rozwiązanie oparte na AI przynosi lepsze wyniki niż dotychczas stosowane metody**
   Efektywność AI musi być weryfikowalna. Nie wystarczy, że dostawca zapewnia, iż jego rozwiązanie działa lepiej. Kupujący powinien wymagać dowodów: porównania z dotychczasową metodą, badań, wyników pilotażu lub walidacji na danych zbliżonych do jego własnych.

4. **Rozważono prostsze alternatywy, takie jak automatyzację, optymalizację procesów, wsparcie decyzyjne oparte na statystyce, i AI okazało się najlepszym wyborem**

ZAPAMIĘTAJ: Zacznij od problemu, który chcesz rozwiązać, a nie od technologii. Zastanów się, czy problem wiąże się z dużą ilością danych, czy jego rozwiązanie byłoby zbyt powtarzalne dla człowieka, czy wyniki AI można weryfikować empirycznie oraz czy dostępne są dane odpowiedniej jakości. Nie wpadnij w pułapkę ekscytacji i budowania PR wokół AI. W wielu zastosowaniach AI może być mniej skutecznym, droższym i bardziej ryzykownym rozwiązaniem, niż na przykład dobrze działająca aplikacja dająca deterministyczne wyniki.

Pytanie 2

Czy AI spełnia wymagania prawne?

1. **Czy produkt ma znak CE jako wyrób medyczny? Jakiej klasy (I, IIa, IIb, III) wg MDR?**
   Jeśli produkt AI ma zastosowanie medyczne, ponieważ bezpośrednio wspiera decyzje diagnostyczne, terapeutyczne lub profilaktyczne, to najprawdopodobniej jest on wyrobem medycznym i musi posiadać oznakowanie CE zgodnie z rozporządzeniem MDR (UE 2017/745). O kwalifikacji nie decyduje samo wykorzystanie sztucznej inteligencji ani stosowanie produktu w szpitalu. Znaczenie ma przeznaczenie wynikające między innymi z instrukcji używania, oznakowania oraz materiałów promocyjnych producenta.

   Każdemu wyrobowi medycznemu przypisywana jest klasa ryzyka – od klasy I przez klasę IIa, IIb do klasy III. O tym, jaką klasę ryzyka należy przypisać, decyduje potencjalne ryzyko przypisywane wyrobowi oraz zasady określania klas ryzyka ustanowione w MDR przez prawodawcę. Nie ma tu miejsca na dowolność czy przypisanie klasy wyższej „na wszelki wypadek". W praktyce częstszym ryzykiem jest zaniżenie klasy ryzyka do klasy I.

   Klasa ryzyka przesądza m.in. o tym, jak rygorystyczna była ścieżka oceny zgodności: klasa I to co do zasady samoocena producenta, klasy IIa–III wymagają udziału niezależnej jednostki notyfikowanej. Im wyższa klasa, tym więcej dowodów bezpieczeństwa i skuteczności dostawca powinien przedstawić. Oznakowanie CE traktuj jako próg wejścia, a nie jako gwarancję jakości. Zawsze sprawdź deklarację zgodności UE, a jeśli dla danego wyrobu wymagany jest certyfikat jednostki notyfikowanej, również ten dokument. Zapytaj dostawcę, na podstawie której reguły MDR dokonano klasyfikacji wyrobu oraz jakie jest uzasadnienie przyjętej klasy ryzyka. Oprogramowanie medyczne najczęściej klasyfikowane jest na podstawie Reguły 11 MDR. Zdecydowana większość rozwiązań opartych o AI klasyfikowana będzie jako klasa IIa lub wyższa.

   Wyrobem medycznym mogą być między innymi systemy wspomagania decyzji klinicznych, algorytmy analizy obrazów medycznych, narzędzia wspierające triage pacjentów oraz niektóre rozwiązania generatywnej AI wykorzystywane do celów diagnostycznych lub terapeutycznych.

   Nie każdy produkt AI przeznaczony dla ochrony zdrowia jest jednak wyrobem medycznym. Jeśli masz wątpliwości, poproś dostawcę o uzasadnienie przyjętej kwalifikacji i oceń je w świetle deklaro-

Pytanie 2
Czy AI spełnia wymagania prawne?

wanego przeznaczenia oraz funkcji produktu. Wymaganie statusu wyrobu medycznego „na wszelki wypadek", gdy produkt nie spełnia jego definicji, może być nadmiarowe i nieproporcjonalne.

2. Czy produkt podlega MDR czy IVDR?

Nie każdy wyrób medyczny podlega rozporządzeniu MDR. Jeżeli oprogramowanie analizuje dane laboratoryjne, próbki biologiczne, dane genetyczne lub w inny sposób wspiera diagnostykę in vitro, może podlegać wymaganiom rozporządzenia IVDR (UE 2017/746) zamiast lub obok MDR. Podobnie jak w MDR, klasa ryzyka określa rygor oceny zgodności. W IVDR wyroby dzieli się na klasy A, B, C i D (od najniższego do najwyższego ryzyka). Zapytaj dostawcę o deklarację zgodności (i – w razie potrzeby – sprawdź certyfikat), aby ustalić czy produkt AI jest wyrobem medycznym czy wyrobem medycznym do diagnostyki in vitro, a co za tym idzie, czy podlega wymaganiom MDR czy IVDR.

3. Jeśli nie wymaga CE, czy posiada certyfikację np. IEC 82304-1?

Nie każde rozwiązanie AI w ochronie zdrowia jest wyrobem medycznym. Systemy służące celom operacyjnym (np.: planowanie zasobów, harmonogram wizyt, obsługa administracyjna) mogą nie podlegać MDR. To nie oznacza jednak, że działają w próżni regulacyjnej. Takie produkty również powinny spełniać odpowiednie wymagania dotyczące bezpieczeństwa i jakości. W zależności od przeznaczenia i funkcji produktu mogą mieć do niego zastosowanie obowiązki wynikające z AI Act, a pomocnym punktem odniesienia dla oceny bezpieczeństwa mogą być odpowiednie normy, np. IEC 82304-1 dotycząca bezpieczeństwa oprogramowania zdrowotnego. Zapytaj dostawcę, jakie testy lub audyty przeprowadzono i jakie dokumenty potwierdzają bezpieczeństwo produktu. Nie wymagaj jednak konkretnego certyfikatu, jeśli nie jest on obowiązkowy – liczą się wiarygodne dowody odpowiednie do zastosowania i poziomu ryzyka rozwiązania.

4. Czy dostawca uwzględnia wymogi AI Act (rozporządzenie UE 2024/1689)?

AI Act to pierwsze, kompleksowe rozporządzenie UE regulujące systemy sztucznej inteligencji, a jego kluczowe przepisy dotyczące systemów wysokiego ryzyka mają również zastosowanie do wyrobów medycznych opartych o sztuczną inteligencję. Systemy AI stosowane w ochronie zdrowia, które wspierają diagnostykę, triażowanie czy decyzje kliniczne mogą być klasyfikowane jako systemy wysokiego ryzyka, co nakłada na dostawców konkretne obowiązki: wdrożenie systemu zarządzania ryzykiem, zapewnienie nadzoru ludzkiego, przejrzystość działania algorytmu, rejestrację w unijnej bazie danych systemów AI (w przypadkach przewidzianych w art. 49 AI Act), przeprowadzenie oceny zgodności przed wprowadzeniem produktu na rynek. Przepisy AI Act weszły już formalnie w życie, jednak poszczególne obowiązki są stosowane etapowo. W przypadku systemów wysokiego ryzyka, do których mogą należeć rozwiązania AI wykorzystywane w ochronie zdrowia, część wymogów będzie obowiązywać dopiero po upływie okresów przejściowych określonych w rozporządzeniu.

Pytanie 2
Czy AI spełnia wymagania prawne?

Kupujący powinien znać i brać pod uwagę harmonogram stosowania AI Act. Od 2 lutego 2025 r. obowiązują m.in. przepisy dotyczące zakazanych praktyk AI oraz zapewnienia odpowiedniego poziomu kompetencji personelu w zakresie AI (AI literacy). Od 2 sierpnia 2025 r. stosowane są przepisy dotyczące modeli AI ogólnego przeznaczenia (GPAI), a od 2 sierpnia 2026 r. m.in. określone obowiązki przejrzystości. Z kolei obowiązki dotyczące systemów AI wysokiego ryzyka objętych załącznikiem III mają być stosowane od 2 grudnia 2027 r., natomiast w przypadku systemów AI wysokiego ryzyka powiązanych z produktami regulowanymi na podstawie załącznika I, w tym odpowiednimi wyrobami medycznymi, od 2 sierpnia 2028 r. Przed zakupem warto więc ustalić, której kategorii dotyczy dane rozwiązanie, jakie obowiązki już znajdują zastosowanie i w jakim terminie dostawca powinien zapewnić zgodność z kolejnymi wymaganiami.

Kupujący może zapytać dostawcę nie tylko o aktualną zgodność produktu z AI Act, ale również o plan osiągnięcia pełnej zgodności w terminach wynikających z przepisów. Należy jednak pamiętać, że brak możliwości podania precyzyjnej daty już teraz nie musi dyskwalifikować dostawcy, ale brak jakiegokolwiek planu dojścia do zgodności powinien budzić wątpliwości. Warto pozostawać w stałym kontakcie z dostawcą, aby móc dopytać o te kwestie na bieżąco, na późniejszych etapach.

Pamiętaj, że AI Act nakłada określone obowiązki nie tylko na dostawców, ale również na organizacje stosujące systemy AI wysokiego ryzyka. Przed zakupem warto sprawdzić, czy Twoja placówka będzie w stanie zapewnić odpowiedni nadzór człowieka, monitorować działanie systemu i reagować na incydenty zgodnie z obowiązującymi ją przepisami.

5. **Czy istnieje dokumentacja potwierdzająca spełnienie wymogów prawnych przez rozwiązanie?**
W przypadku wyrobów medycznych objętych MDR kupujący może żądać od dostawcy dostarczenia: deklaracji zgodności UE, certyfikatów zgodności wydanych przez jednostkę notyfikowaną (jeśli jest wymagana), instrukcji używania oraz etykiet w języku polskim lub angielskim (język angielski jest dopuszczalny tylko dla wyrobów przeznaczonych dla użytkowników niebędących laikami)[2], identyfikatora UDI (jeśli jest wymagany). Dla wyrobów klasy III i wyrobów do implantacji, z uwzględnieniem wyjątków określonych w MDR, należy również zweryfikować dostępność podsumowania dotyczącego bezpieczeństwa i skuteczności klinicznej (SSCP).

Chociaż producent jest zobowiązany przygotować pełną dokumentację techniczną (obejmująca m.in. szczegółowe raporty z oceny klinicznej, analizę ryzyka, wyniki testów walidacyjnych czy plan nadzoru PMS/PMCF), to może ona stanowić tajemnicę przedsiębiorstwa producenta i co do zasady nie musi być udostępniana nabywcy w całości. Weryfikacja, czy ten obowią-

[2] Na podstawie art. 12 ustawy o wyrobach medycznych

Pytanie 2

Czy AI spełnia wymagania prawne?

zek został spełniony prawidłowo pozostaje w zakresie oceny dokonywanej przez jednostkę notyfikowaną (jeśli dotyczy) lub – w razie potrzeby – organ nadzoru. Kupujący powinien przede wszystkim zapoznać się z instrukcją używania wyrobu oraz innymi załączonymi do produktu informacjami (z etykietą, komunikatami pojawiającymi się w systemie czy warunkami świadczenia usług lub regulaminami platformy, jeśli takie są dostępne). Powinny znaleźć się tam wszystkie informacje niezbędne do bezpiecznego stosowania produktu.

Kupujący może jednak żądać dokumentów, raportów lub informacji pozwalających zweryfikować zgodność i bezpieczeństwo produktu, z uwzględnieniem ochrony informacji poufnych. Po rozpoczęciu stosowania odpowiednich wymogów AI Act systemy wysokiego ryzyka będą musiały posiadać m.in. dokumentację zarządzania ryzykiem i opis mechanizmów nadzoru ludzkiego. Dostawcy systemów AI nie będą jednak zobligowani udostępniać wszystkich informacji Kupującym – część z nich może być objęta tajemnicą przedsiębiorstwa na takich samych zasadach jak dokumentacja techniczna wyrobów medycznych. Dostawcy, po wejściu w życie określonych obowiązków wynikających z AI Act, będą jednak zobowiązani posiadać deklarację zgodności oraz instrukcję obsługi, która musi zawierać mi.in. metryki dokładności i informacje o działaniu dla określonych grup osób, które powinien zweryfikować Kupujący.

Brak udostępniania deklaracji zgodności lub certyfikatu jednostki notyfikowanej (jeśli jest wymagany) czy odpowiedniej instrukcji lub brak informacji pozwalających wiarygodnie zweryfikować jego zgodność z prawem i bezpieczeństwo powinien być sygnałem do wstrzymania procesu zakupowego do czasu wyjaśnienia wątpliwości

ZAPAMIĘTAJ: Zgodność z prawem to nie formalność, ale fundament bezpiecznego wdrożenia. Sprawdź oznakowanie CE i klasę ryzyka produktu, deklarację zgodności, certyfikat jednostki notyfikowanej (jeśli jest wymagany) oraz instrukcję i zapytaj dostawcę, jak odnosi się do wymogów AI Act. Jeśli produkt nie jest wyrobem medycznym, sprawdź, jakie normy, wyniki testów, audyty lub inne dokumenty potwierdzają jego jakość i bezpieczeństwo. Możesz umieścić również odpowiednie postanowienia i deklaracje w umowie. Pamiętaj jednak, aby wymagania były uzasadnione, proporcjonalne do przeznaczenia produktu i poziomu ryzyka oraz nie ograniczały bezpodstawnie konkurencji. Zamawiający może określać wymagania jakościowe i bezpieczeństwa wykraczające poza ustawowe minimum, jeżeli odpowiadają one rzeczywistym potrzebom organizacji. Jeśli produkt nie jest wyrobem medycznym, nie bój się pytać dostawcy o wyjaśnienia. W każdym wypadku brak jasnych odpowiedzi lub wymaganej przez prawo dokumentacji to sygnał, by wstrzymać proces zakupowy z tym dostawcą do momentu uzyskania wyjaśnień.

Pytanie 3

Czy AI jest skuteczna i jakie ma na to dowody?

1. Czy możesz przeanalizować wyniki walidacji algorytmu (AUC, czułość, swoistość, PPV, NPV, kalibracja)?

Każdy dostawca zapewnia, że jego produkt „działa". Kluczowe jest jednak sprawdzenie, na czym to zapewnienie się opiera. Podstawowe metryki statystyczne AUC[3], czułość[4], swoistość[5], wartość predykcyjna dodatnia (PPV[6]) i ujemna (NPV[7]) pozwalają ocenić rzeczywistą skuteczność algorytmu. Kupujący powinien rozumieć znaczenie tych wskaźników i ocenić, czy są one istotne dla jego organizacji.

Wysoka dokładność ogólna (accuracy) może maskować poważne słabości: model może świetnie wykrywać przypadki negatywne, a systematycznie mylić się przy pozytywnych, co w kontekście klinicznym bywa krytyczne. Możesz zażądać pełnych wyników walidacji, nie tylko tych najkorzystniejszych dla dostawcy.

W miarę dostępności danych sprawdź też, czy oceniano wpływ na istotne kliniczne punkty końcowe, takie jak śmiertelność, poważne zdarzenia sercowo-naczyniowe (MACE), liczbę hospitalizacji czy jakość życia pacjentów.

Pamiętaj jednak, że produkty certyfikowane przy udziale jednostki notyfikowanej zostały zweryfikowane nie tylko przez dostawcę lub producenta, ale również przez specjalistów z jednostek notyfikowanych. Ich rolą jest zweryfikować bezpieczeństwo i zgodność regulacyjną produktu, oraz to, czy użytkownik otrzymuje komplet niezbędnych informacji, aby bezpiecznie korzystać z systemu.

---

[3] AUC (Area Under the Curve) - ogólna miara skuteczności modelu. Im bliżej wartości 1,0, tym lepiej algorytm rozróżnia przypadki pozytywne od negatywnych. Wartość 0,5 oznacza, że model nie jest lepszy niż rzut monetą.

[4] Czułość (sensitivity, recall) - zdolność modelu do wykrywania prawdziwych przypadków pozytywnych. Niska czułość oznacza, że algorytm często „przegapia" chorych pacjentów.

[5] Swoistość (specificity) - zdolność modelu do prawidłowego wykluczania przypadków negatywnych. Niska swoistość oznacza dużo fałszywych alarmów.

[6] PPV (Positive Predictive Value) - wartość predykcyjna dodatnia: jak często wynik pozytywny algorytmu jest rzeczywiście prawidłowy.

[7] NPV (Negative Predictive Value) - wartość predykcyjna ujemna: jak często wynik negatywny algorytmu jest rzeczywiście prawidłowy.

Pytanie 3

Czy AI jest skuteczna i jakie ma na to dowody?

Dlatego pamiętaj, aby przede wszystkim wnikliwie zapoznać się z odpowiednią instrukcją oraz pozostałymi dostarczanymi przez dostawcę lub producenta informacjami, gdzie powinny zostać opisane m.in. takie kwestie jak:

- charakterystyka działania wyrobu,
- informacje pozwalające pracownikowi systemu ochrony zdrowia sprawdzić, czy wyrób jest odpowiedni i wybrać właściwe oprogramowanie i wyposażenie, a także
- przewidziane zastosowanie wyrobu z jasnym wyjaśnieniem wskazań, przeciwwskazań (jeśli istnieją), grupy docelowej lub grup docelowych pacjentów i przewidzianych użytkowników (jeśli zostały zawężone przez producenta lub dostawcę);
- opis korzyści klinicznych.
- charakterystyka działania i ograniczenia, w tym metryki dokładności (art. 13 AI Act)

2. Na jakiej populacji algorytm został zwalidowany? Czy pasuje do Twojej populacji pacjentów?

Model AI jest tak dobry, jak dane, na których był trenowany i testowany. Algorytm walidowany na populacji z innego kraju, grupy wiekowej lub profilu chorobowego może działać zupełnie inaczej w Twojej organizacji. Zapytaj dostawcę, skąd pochodziły dane walidacyjne i porównaj je z charakterystyką Twoich pacjentów. Różnice demograficzne, epidemiologiczne czy organizacyjne mogą znacząco wpłynąć na skuteczność produktu w praktyce. To, że produkt jest najkorzystniejszy cenowo nie oznacza, że będzie najskuteczniejszy.

Pamiętaj jednak, że jeżeli dany produkt przeszedł pozytywnie unijną procedurę oceny zgodności jako wyrób medyczny (zwłaszcza z udziałem jednostki notyfikowanej), to jego bezpieczeństwo, skuteczność oraz adekwatność dla docelowej populacji pacjentów zostały już niezależnie zweryfikowane na podstawie przedstawionych dowodów klinicznych. Weź pod uwagę, że szczegółowe dane o zbiorach treningowych i walidacyjnych, na których oparto model, nie zawsze są publicznie dostępne – producent często chroni je jako tajemnicę przedsiębiorstwa, a tym samym dostawca bardzo często nie będzie mógł ich udostępnić bez podpisanego NDA.

3. Czy przeprowadzono walidację zewnętrzną (nie tylko na danych producenta)?

Producent testuje swój produkt na danych, które zna. Niestety mogą być to te same dane lub zbliżone do danych, na których model był budowany. Wyniki mogą wyglądać świetnie, bo środowisko jest znajome. Prawdziwy test to dane z zewnątrz, czyli np.: z innych szpitali, innych systemów, innych populacji pacjentów. Dopiero wtedy widać, czy algorytm naprawdę działa, czy tylko dobrze zapamiętał dane treningowe.

Pytanie 3

Czy AI jest skuteczna i jakie ma na to dowody?

Zapytaj dostawcę, gdzie i przez kogo przeprowadzono walidację zewnętrzną, i czy wyniki były podobne w różnych środowiskach.

Równocześnie, jeśli produkt został poddany ocenie jednostki notyfikowanej i posiada ważny certyfikat, pamiętaj, że jakość tych badań nie była oceniana wyłącznie przez samego producenta. To, czy przedstawione wyniki wystarczająco potwierdzają bezpieczeństwo i skuteczność modelu, zweryfikował niezależny audytor – i było to warunkiem wydania certyfikatu. W takiej sytuacji możesz uwzględnić kompetencje i uprawnienia jednostki notyfikowanej, pamiętając oczywiście o sprawdzeniu aktualności samego certyfikatu.

4. Czy istnieją wyniki z walidacji prospektywnej lub badania klinicznego?

Walidacja retrospektywna sprawdza, jak model radziłby sobie z przypadkami, które już się wydarzyły i których wynik jest znany. To dobry punkt startowy, ale nie mówi wszystkiego. W rzeczywistym środowisku klinicznym dochodzą czynniki, których archiwalne dane nie oddają: zmienność w sposobie wprowadzania danych, różnice między zmianami personelu, presja czasowa czy efekt samej obecności algorytmu w procesie decyzyjnym. Walidacja prospektywna, czyli testowanie modelu na nowych danych zbieranych w trakcie badania, pozwala lepiej ocenić jego działanie w praktyce. Z kolei odpowiednio zaprojektowane badanie kliniczne może również wykazać, czy wykorzystanie AI przynosi rzeczywiste korzyści pacjentom.

Sprawdź, czy dostarczane przez dostawcę lub producenta informacje (m.in. instrukcja czy materiały szkoleniowe):

- wskazują, że model może być stosowany we wszystkich przewidywanych przez Ciebie zastosowaniach i dla wszystkich potencjalnych grup pacjentów, czy też przewidziane zastosowanie lub grupę docelową pacjentów odpowiednio zawężono;
- wskazują przeciwwskazania, grupy podwyższonego ryzyka, szczególne informacje lub zalecenia dla pracowników systemu ochrony zdrowia stosujących wyrób, a także czy jego stosowanie wymaga od użytkownika określonych kwalifikacji.

Pamiętaj również, że posiadanie certyfikatu oraz nadzór sprawowany przez jednostkę notyfikowaną oznaczają, że bezpieczeństwo i skuteczność modelu zostały należycie zweryfikowane, przedstawione wyniki nie budziły istotnych wątpliwości, a producent prowadzi odpowiedni nadzór nad produktem również po jego wprowadzeniu do obrotu. Przekłada się to na obowiązek okresowego monitorowania bezpieczeństwa, regularne audyty lub raporty składane jednostce notyfikowanej oraz obowiązki związane ze zgłaszaniem incydentów i podejmowaniem działań korygujących. Jeśli producent nie spełnia tych obowiąz-

ków, jednostka może w każdej chwili skrócić ważność certyfikatu, a organ nadzoru może zobowiązać do wycofania produktu z obrotu.

Jeśli po zapoznaniu się z powyższymi materiałami wciąż masz wątpliwości:

- zapytaj dostawcę, czy przeprowadzono analizę wyników walidacji z rozbiciem na grupy danych, np. według wieku, płci, lokalizacji czy etniczności pacjentów, aby wykryć ewentualne stronniczości (bias), i czy możesz się z nią zapoznać;
- sprawdź, czy produkt był testowany poza środowiskiem producenta na danych z innych szpitali lub ośrodków i czy walidacja odbywała się na danych historycznych, oraz czy przeprowadzono badanie kliniczne i gdzie można zapoznać się z jego wynikami?

Warto również zestawić przedstawione dowody z klasą ryzyka wyrobu ustaloną w Pytaniu 2: im wyższa klasa MDR lub IVDR, tym solidniejsze dowody kliniczne powinien przedstawić dostawca. Walidacja wyłącznie retrospektywna przy wyrobie klasy IIb lub III może wzbudzić wątpliwości.

5. Czy wyniki opublikowano w recenzowanym czasopiśmie?

Zanim artykuł trafi do recenzowanego czasopisma, musi przejść ocenę niezależnych ekspertów, którzy sprawdzają metodologię, dane i wnioski. Jeśli dostawca powołuje się na badania potwierdzające skuteczność produktu, zapytaj, gdzie zostały opublikowane. Prezentacja na konferencji firmowej czy materiał marketingowy to nie to samo, co publikacja w naukowym czasopiśmie. Brak jakichkolwiek publikacji przy produkcie kierowanym do zastosowań klinicznych powinien skłonić do pytania: dlaczego dostawca nie poddał swojego rozwiązania niezależnej ocenie recenzenta?

Sama publikacja naukowa nie mówi jeszcze o realnej korzyści operacyjnej i klinicznej po wdrożeniu. Nie jest również warunkiem wprowadzenia modelu do obrotu. Obok metryk walidacyjnych i publikacji warto poprosić dostawcę o deklarację zgodności oraz certyfikat wydany przez jednostkę notyfikowaną, a w przypadku systemu AI, który nie został zakwalifikowany jako wyrób medyczny, można zapytać o udokumentowany track record wdrożeń oraz dane z nadzoru porynkowego (PMS). Przy odpowiedniej skali i dokumentacji mogą stanowić wartościowe dowody, szczególnie gdy publikacja naukowa jeszcze się nie ukazała.

Sprawdź też, czy deklarowane zastosowanie AI jest zgodne z aktualnymi wytycznymi klinicznymi właściwych krajowych i międzynarodowych towarzystw naukowych w danej dziedzinie.

Pytanie 3

Czy AI jest skuteczna i jakie ma na to dowody?

ZAPAMIĘTAJ: Zacznij od sprawdzenia, czy system jest wyrobem medycznym lub systemem AI wysokiego ryzyka i – jeśli tak – od sprawdzenia dokumentacji wymaganej przez prawo (deklaracja zgodności, certyfikat oraz instrukcja używania). Jeśli natomiast model nie jest wyrobem medycznym ani nie jest certyfikowanym systemem AI wysokiego ryzyka (po rozpoczęciu obowiązywania właściwych przepisów), poproś o pełne dane walidacyjne i sprawdź, czy model był testowany na populacji podobnej do Twojej lub poszukaj dowodów spoza organizacji producenta (walidacji zewnętrznej, prospektywnej lub badań klinicznych). Im poważniejsze zastosowanie kliniczne, tym wyższy standard dowodowy powinien obowiązywać. Publikacja w recenzowanym czasopiśmie to dobry znak, ale nie jedyny.

Deklaracja zgodności, certyfikat potwierdzający współpracę z jednostką notyfikowaną (w przypadku wyrobów medycznych czy certyfikowanych już systemów AI wysokiego ryzyka), tak jak udokumentowany track record wdrożeń i dane z nadzoru porynkowego w innych przypadkach również stanowią wiarygodny dowód. Pamiętaj, że wymaganie od dostawcy tylko jednego konkretnego dokumentu (jeśli pozostałe nie budzą wątpliwości i nie jest to uzasadnione konkretnymi okolicznościami czy przepisami prawa), może być nadmiarowe i nieproporcjonalne.

Pamiętaj również, że wiele podmiotów działających w Polsce pełni rolę importerów lub dystrybutorów, podczas gdy producent posiada siedzibę za granicą i nie będzie Twoim bezpośrednim dostawcą. Ponieważ to producent jest odpowiedzialny za większość dokumentacji regulacyjnej (dokumentację techniczną, systemy nadzoru), importer lub dystrybutor mogą nie być w stanie przedstawić wszystkich dokumentów lub danych, jeśli ich przekazanie dystrybutorowi lub importerowi nie jest wymagane przepisami prawa. Dlatego wymagania nadmierne mogą przyczynić się do realnego ograniczenia dostępnych dla Kupującego rozwiązań.

Pytanie 4

Czy AI będzie działać w praktyce?

1. **Czy rozwiązanie jest gotowe do implementacji i codziennego użytku klinicznego?**
   Wiele produktów AI świetnie sprawdza się w warunkach demonstracyjnych na wyselekcjonowanych danych, w kontrolowanym środowisku, bez presji czasu i bez codziennego chaosu szpitalnego. Rzeczywistość kliniczna jest inna: systemy są przeciążone, dane niekompletne, personel pod presją, a procesy niedoskonałe. Zanim podpiszesz umowę, sprawdź, czy produkt był już wdrożony w placówkach o podobnym profilu i skali, i jak działał po kilku tygodniach użytkowania. Gotowość do wdrożenia to nie tylko sprawny kod, ale także dokumentacja, szkolenia, wsparcie techniczne i realistyczny plan uruchomienia.

   Dodatkowo, zanim przystąpisz do wdrożenia, warto przeprowadzić udokumentowaną ocenę gotowości organizacyjnej i sprawdzić, czy Twoja placówka ma odpowiednie zasoby ludzkie, infrastrukturę techniczną i kulturę pracy, które pozwolą produktowi rzeczywiście działać. Jeśli rozwiązanie jest kupowane centralnie lub ma działać w kilku placówkach, przeprowadź tę ocenę osobno dla każdej lokalizacji. Centralny zakup nie oznacza, że wszystkie placówki mają takie same systemy, dane, procesy i personel. Równie ważne jest wsparcie kierownictwa: bez aktywnego zaangażowania zarządu i liderów klinicznych nawet najlepszy produkt może utknąć na etapie wdrożenia.

2. **Jak wygląda workflow użytkownika końcowego (lekarza, pielęgniarki, technika)?**
   Produkt AI, który teoretycznie działa, ale w praktyce spowalnia pracę personelu, nie zostanie przyjęty, bez względu na to, jak dobre są jego wyniki walidacyjne. Zanim zdecydujesz się na zakup, sprawdź, jak produkt wpisuje się w codzienną pracę lekarza, pielęgniarki czy technika: czy wymaga dodatkowych kroków, czy naturalnie integruje się z tym, co już robią, czy wyniki są prezentowane w zrozumiały i użyteczny sposób. Warto poprosić dostawcę o demonstrację na żywym środowisku, nie tylko na przygotowanej prezentacji, i zaangażować użytkowników końcowych w ocenę produktu jeszcze przed zakupem. To oni najszybciej wychwycą to, czego nie widać w specyfikacji technicznej.

Pytanie 4

Czy AI będzie działać w praktyce?

Warto przed wdrożeniem ustalić także jasne ścieżki kliniczne dla alertów generowanych przez algorytm: które powiadomienia są priorytetowe i wymagają natychmiastowej reakcji, które mogą poczekać, a które nie wymagają reakcji. Brak takich ustaleń prowadzi do przeciążenia personelu nadmiarem alertów (efekt znany jako „alert fatigue"), który paradoksalnie obniża bezpieczeństwo pacjentów, bo pracownicy zaczynają ignorować wszystkie powiadomienia, również te krytyczne.

Określ też, w jaki sposób i czy w ogóle wyniki algorytmu trafiają do dokumentacji medycznej: czy automatycznie, czy wymaga to działania ze strony personelu? Pamiętaj, że wdrażanie każdej nowej technologii do ekosystemu informatycznego powinno optymalizować proces diagnostyczno-terapeutyczny, a więc powinno być z nim bezpośrednio integrowalne.

3. Czy rozwiązanie wykorzystuje generatywną AI, a jeżeli tak, jak ogranicza ryzyko halucynacji?

Modele generatywne (takie jak duże modele językowe) mogą udzielać odpowiedzi brzmiących wiarygodnie, ale nieprawdziwych. Zjawisko to nazywa się halucynacją modelu. W środowisku klinicznym błędna odpowiedź może mieć bezpośrednie konsekwencje dla pacjenta. Pamiętaj, że system może generować nieprawdziwe informacje i halucynacje są zawsze ryzykiem korzystania z generatywnej AI. Zapytaj dostawcę, jakie mechanizmy w rozwiązaniu ograniczają to ryzyko. W jaki sposób odpowiedzi AI są oznaczane tak, by użytkownik wiedział, że wymagają weryfikacji? Jakie mechanizmy walidacji są wbudowane w produkt oraz czy użytkownik jest na bieżąco informowany o ograniczeniach modelu? Jeśli dostawca nie potrafi odpowiedzieć na te pytania to jest to sygnał ostrzegawczy. Jeżeli rozwiązanie nie wykorzystuje generatywnej AI (np. jest klasyfikatorem o zamkniętym zbiorze wyników, jak większość narzędzi do analizy EKG czy obrazów medycznych), ryzyko halucynacji nie występuje i to pytanie go nie dotyczy. Wtedy skup się na metrykach skuteczności z Pytania 3.

4. Czy systemy IT szpitala (HIS[8], PACS[9], LIS[10]) zintegrują się z AI?

Nawet najlepszy algorytm nie będzie skutecznie działał, jeśli nie zintegruje się z systemami, które już działają w Twoim szpitalu. Integracja to jeden z najczęstszych powodów opóź-

[8] HIS (Hospital Information System) - szpitalny system informacyjny; zarządza danymi administracyjnymi i klinicznymi pacjentów, harmonogramami, dokumentacją medyczną.

[9] PACS (Picture Archiving and Communication System) - system archiwizacji i przesyłania obrazów medycznych; przechowuje i udostępnia wyniki badań obrazowych (RTG, CT, MRI, USG).

[10] LIS (Laboratory Information System) - system informacyjny laboratorium; zarządza zleceniami i wynikami badań laboratoryjnych.

nień i niepowodzeń wdrożeń AI w ochronie zdrowia, i jeden z najrzadziej sprawdzanych na etapie zakupu. Zapytaj dostawcę, z jakimi systemami produkt był już zintegrowany i czy ma doświadczenie z infrastrukturą podobną do Twojej. Sprawdź, czy produkt wykorzystuje uznane standardy interoperacyjności, takie jak HL7 FHIR (wymiana danych klinicznych), DICOM (obrazowanie medyczne) czy profile IHE. Ich stosowanie oznacza, że integracja z Twoją infrastrukturą będzie łatwiejsza i mniej kosztowna. Sprawdź także, czy integracja wymaga modyfikacji istniejących systemów, dodatkowego oprogramowania pośredniczącego lub zaangażowania zewnętrznych dostawców IT. Pamiętaj, że integracja dotyczy nie tylko systemów HIS/PACS/LIS, ale też specjalistycznego sprzętu i systemów używanych w Twojej dziedzinie, np. w kardiologii systemów echokardiograficznych, elektrofizjologicznych, telemonitoringu urządzeń wszczepialnych czy systemów hemodynamicznych. Koszty i czas integracji bywają wyższe niż sam koszt i czas przeznaczony na zakup produktu. Zapytaj też, czy rozwiązanie wymaga dodatkowego sprzętu (np. serwerów, kart graficznych, specjalistycznych stacji roboczych) i jakie są jego minimalne parametry. Przestarzały sprzęt lub oprogramowanie bez wsparcia producenta może całkowicie uniemożliwić wdrożenie.

Równie ważna jest rozmowa z własnym działem IT. Przed zakupem warto sprawdzić, na co faktycznie pozwala infrastruktura Twojego podmiotu (jakie systemy działają, w jakich wersjach, jakie mają ograniczenia i czy dział IT ma zasoby, żeby to wdrożenie w ogóle obsłużyć). Dostawca może obiecywać bezproblemową integrację, ale to Twój zespół IT będzie musiał ją przeprowadzić.

5. **Czy masz odpowiednie dane w wymaganym formacie i jakości?**
Przed wdrożeniem danego rozwiązania AI w swojej organizacji musisz odpowiedzieć sobie na pytanie, czy Twoja organizacja faktycznie dysponuje danymi, których produkt potrzebuje: czy są kompletne, aktualne, odpowiednio ustrukturyzowane i czy mogą być legalnie wykorzystane. W polskim systemie ochrony zdrowia jakość danych bywa bardzo zróżnicowana, a te same informacje mogą być wprowadzane w różny sposób przez różnych pracowników, w różnych oddziałach, na różnych zmianach. Algorytm, który nie rozpoznaje tej różnorodności, będzie działał nieprzewidywalnie. Zapytaj dostawcę, w jakim dokładnie formacie dane muszą być dostarczone i co się dzieje, gdy dane są niekompletne lub niespójne.

6. **Jak zmierzysz skuteczność algorytmu po wdrożeniu w Twoim szpitalu?**
Wdrożenie to nie koniec procesu, kolejnym krokiem jest weryfikacja. Algorytm, który świetnie działał w warunkach walidacji, może zachowywać się inaczej w realiach Twoje-

Pytanie 4

Czy AI będzie działać w praktyce?

go szpitala: na Twoich danych, w Twoich procesach, z Twoim personelem. Dlatego przed zakupem warto ustalić, jak będziesz mierzyć skuteczność produktu po wdrożeniu, i co zrobisz, jeśli wyniki okażą się niezadowalające.

Zanim algorytm zacznie działać, określ punkt odniesienia: jak wygląda obecna sytuacja bez AI? Tylko wtedy będziesz w stanie ocenić, czy produkt rzeczywiście przynosi zmianę. Ustal mierzalne wskaźniki (np.: skrócenie czasu diagnozy, zmniejszenie liczby błędów, poprawa trafności decyzji klinicznych) i zaplanuj regularne przeglądy wyników. Równie ważne jest zapewnienie możliwości szybkiego wyłączenia systemu w razie wykrycia nieprawidłowości. Wyznacz co najmniej dwie osoby odpowiedzialne za wdrożony algorytm: jedną po stronie klinicznej, która będzie oceniać skuteczność i reagować na błędne rekomendacje, oraz jedną po stronie technicznej, która będzie monitorować działanie systemu i wykrywać dryft danych (zmiana charakterystyki danych wejściowych w czasie). To oni powinni wspólnie podejmować decyzje o dalszym użytkowaniu lub wycofaniu systemu.

Co więcej, niektóre systemy AI są zaprojektowane tak, by dostosowywać się do nowych danych już po wdrożeniu. Jest to zaletą, ale niesie ze sobą także ryzyko, ponieważ model, który się uczy, to model, który się zmienia. Zapytaj dostawcę, czy algorytm może modyfikować swoje parametry po wdrożeniu. Jeśli tak, to zapytaj dostawcę, jakie zmiany modelu są objęte dotychczasową oceną zgodności, a jakie wymagają dodatkowej oceny, ponownej oceny zgodności lub udziału jednostki notyfikowanej zgodnie z właściwymi przepisami Jasno ustal podział obowiązków dotyczących monitorowania między dostawcą a Twoją organizacją.

ZAPAMIĘTAJ: Gotowość produktu to nie to samo, co gotowość Twojej organizacji. Sprawdź, czy algorytm rzeczywiście wpisuje się w codzienną pracę personelu, czy Twoje systemy IT udźwignią integrację i czy dane, którymi dysponujesz, są wystarczającej jakości. Przed wdrożeniem ustal punkt odniesienia i mierzalne wskaźniki sukcesu, bo bez nich nie będziesz wiedzieć, czy AI naprawdę działa, czy tylko działa pozornie.

Pytanie 5

Czy Twój personel jest gotowy na AI?

1. **Czy masz ambasadorów zmiany wśród personelu, którzy wesprą wdrożenie?**
   Każda zmiana w organizacji potrzebuje swoich ambasadorów i wdrożenie AI nie jest wyjątkiem. Tak zwani "early-adopterzy" to osoby, które jako pierwsze chcą przetestować nowe rozwiązanie, rozumieją jego potencjał i są gotowe przekonywać do niego innych. W kontekście szpitala może to być lekarz, który sam interesuje się technologią, pielęgniarka oddziałowa z autorytetem w zespole albo technik. To oni wychwycą problemy, zanim staną się kryzysem, przetłumaczą język technologii na język praktyki i sprawią, że reszta zespołu będzie traktować AI jako narzędzie, a nie zagrożenie. Jeśli w Twojej organizacji takich osób nie ma, warto je zidentyfikować i zaangażować jeszcze przed zakupem, aby mogli wziąć udział w procesie oceny produktu.

2. **Czy zaplanowałeś/aś szkolenia i zarządzanie zmianą?**
   Wdrożenie AI wiąże się ze sporymi zmianami dotyczącymi sposobu pracy personelu i procesów, do których pracownicy są przyzwyczajeni. Szkolenia powinny obejmować nie tylko obsługę techniczną, ale przede wszystkim umiejętność interpretowania wyników algorytmu, rozpoznawania jego ograniczeń i wiedzę o tym, kiedy zaufać rekomendacji AI, a kiedy ją zakwestionować. Zarządzanie zmianą to z kolei zadbanie o to, żeby personel czuł się wysłuchany, rozumiał cel wdrożenia i wiedział, co się zmieni w jego codziennej pracy, a co się nie zmieni.

   Jednorazowe szkolenie przed wdrożeniem to za mało. Dla wielu pracowników to pierwszy kontakt z AI w pracy i samo pokazanie jak działa narzędzie nie sprawi, że poczują się z nim pewnie. Potrzeba czasu, cierpliwości i gotowości organizacji do tego, żeby towarzyszyć personelowi w tym procesie poprzez cykliczne szkolenia.

   Zaplanuj również ścieżkę zgłaszania błędów. Personel musi wiedzieć, co zrobić, gdy coś działa nieprawidłowo. Brak jasnej ścieżki zgłaszania problemów sprawia, że błędy są przemilczane zamiast naprawiane. Zadbanie o kulturę organizacyjną jest równie ważne, jak zadbanie o zaplecze techniczne.

Pytanie 5

Czy Twój personel jest gotowy na AI?

3. Czy personel rozumie, że AI wspiera decyzję, a nie ją zastępuje?

W praktyce klinicznej istnieją dwa przeciwstawne ryzyka. Pierwsze: personel ignoruje rekomendacje AI, bo nie ufa technologii i traktuje ją jako zbędne narzędzie narzucone przez zarząd. Drugie: personel bezrefleksyjnie przyjmuje wyniki algorytmu, rezygnując z własnej oceny klinicznej. W obu tych przypadkach AI nie spełnia swojej roli.

Lekarz, pielęgniarka czy technik muszą rozumieć, że algorytm to narzędzie wspierające ich decyzję, a nie zastępujące ich wiedzę, doświadczenie i odpowiedzialność zawodową. AI może się mylić, działać gorzej na danych odbiegających od tych, na których była trenowana, i nie uwzględniać kontekstu, który dla doświadczonego klinicysty jest oczywisty. Wykorzystanie AI nie zwalnia personelu medycznego z obowiązku zachowania należytej staranności ani z odpowiedzialności zawodowej za podejmowane decyzje kliniczne. Jest to aspekt, który wymaga wytłumaczenia i upewnienia się, że personel zdaje sobie sprawę, zarówno z korzyści, jak i ryzyk, które niesie ze sobą AI.

W przypadku gdy ocena klinicysty różni się od rekomendacji algorytmu, personel powinien mieć jasną procedurę postępowania: udokumentować swoją decyzję i uzasadnienie, a rozbieżność zgłosić zgodnie z wewnętrznymi procedurami organizacji.

Zastanów się: czy Twój personel wie, kiedy zakwestionować rekomendację AI? Czy istnieje jasna procedura postępowania, gdy algorytm sugeruje coś sprzecznego z oceną klinicysty?

4. Czy istnieje plan komunikacji z zespołem dotyczący wdrożenia AI i związanych z nim obaw?

Choć AI w ochronie zdrowia jest obecna w branżowych dyskusjach od lat, realna obawa przed zastąpieniem przez algorytm nie tylko towarzyszy wielu pracownikom, a wręcz wraz z udoskonalaniem tej technologii, nawet się nasila.

Część personelu będzie obawiać się, że algorytm zastąpi ich w pracy, oceni ich kompetencje lub sprawi, że staną się zbędni. Jeśli organizacja nie wyjdzie naprzeciw tym obawom z jasnym i szczerym przekazem, pracownicy mogą mieć wrogie nastawienie do AI.

Plan komunikacji to nie jednorazowy e-mail przed wdrożeniem. To przemyślana strategia kontaktu z personelem. Przekaz musi być konkretny: co się zmieni, co się nie zmieni, jaka jest rola AI w ich codziennej pracy i dlaczego organizacja podjęła tę decy-

Pytanie 5

Czy Twój personel jest gotowy na AI?

zję. Warto też stworzyć przestrzeń do zadawania pytań i wyrażania obaw - zwłaszcza związanych z tym, że decyzja AI może niekiedy różnić się od decyzji klinicysty.

5. **Czy wiesz, jakich narzędzi AI personel już używa?**
   Shadow AI to zjawisko korzystania z narzędzi, aplikacji lub usług AI przez pracowników w trakcie pracy, bez wiedzy i zgody przełożonych lub działu IT.

   Warto sprawdzić, czy i jak personel korzysta z ogólnodostępnych narzędzi AI w codziennym życiu. Zapytaj, jakich narzędzi używają prywatnie i które uznają za przydatne, bez odnoszenia tego wprost do pracy czy zgodności z polityką organizacji. Taka wiedza pozwala ocenić realny poziom obycia personelu z AI i wskazuje, które typy narzędzi faktycznie rezonują z ich potrzebami.

ZAPAMIĘTAJ: Zaangażuj personel, zanim podejmiesz decyzję zakupową, zadbaj o ambasadorów zmiany i przemyślany plan komunikacji. Upewnij się, że zespół rozumie rolę AI jako narzędzia wspierającego, a nie zastępującego ich wiedzę i odpowiedzialność. Spisz te ustalenia w formalnym dokumencie (np. wewnętrznej polityce lub procedurze wdrożenia AI). Rozproszone, niepisane zasady mogą być łatwo zapomniane i trudno je wyegzekwować.
Czas i cierpliwość poświęcone na przygotowanie ludzi to nie koszt, ale obowiązkowa inwestycja w powodzenie całego wdrożenia.

Pytanie 6

Czy AI jest etyczna i wolna od dyskryminacji?

1. **Czy algorytm był testowany pod kątem dyskryminacji/biasu[11] (płeć, wiek, pochodzenie etniczne)?**
   Model AI jest odbiciem danych, na których był trenowany, a dane medyczne historycznie nie były zbierane równomiernie. Kobiety, osoby starsze, mniejszości etniczne czy pacjenci z obszarów wiejskich bywali niedoreprezentowani w badaniach klinicznych i bazach danych przez dekady. Algorytm wytrenowany na takich danych może działać gorzej dla całych grup pacjentów, i co groźniejsze, robić to niewidocznie, bo ogólne wskaźniki skuteczności będą wyglądać poprawnie.

   Bias w AI nie zawsze jest oczywisty. Model przewidujący ryzyko hospitalizacji trenowany na danych z dużych miast może systematycznie niedoszacowywać potrzeb pacjentów z mniejszych ośrodków.

   Zapytaj dostawcę, czy przeprowadzono analizę wyników algorytmu z podziałem na grupy demograficzne (płeć, wiek, pochodzenie etniczne, miejsce zamieszkania) i czy skuteczność jest wystarczająca klinicznie w poszczególnych grupach i czy stwierdzone różnice zostały wyjaśnione? Jeśli dostawca nie przeprowadził takiej analizy lub nie potrafi jej przedstawić, jest to sygnał ostrzegawczy.

   Pomocnym punktem odniesienia przy ocenie etyczności produktu AI jest framework FUTURE-AI[12] - konsensus 117 ekspertów z 50 krajów, który definiuje sześć zasad godnego zaufania AI w medycynie:
   - Fairness (uczciwość) - brak dyskryminacji i biasu,
   - Universality (uniwersalność) - działanie na różnych populacjach i w różnych środowiskach,
   - Traceability (identyfikowalność) - możliwość śledzenia decyzji algorytmu,
   - Usability (użyteczność) - produkt realnie wspiera pracę kliniczną,

[11] Bias (stronniczość algorytmiczna) - systematyczny błąd w działaniu modelu AI wynikający z nierównomiernej reprezentacji grup w danych treningowych lub ze sposobu projektowania algorytmu.
[12] https://www.bmj.com/content/388/bmj-2024-081554

Pytanie 6

Czy AI jest etyczna i wolna od dyskryminacji?

- Robustness (niezawodność) - stabilne działanie w różnych warunkach,
- Explainability (wyjaśnialność) - możliwość uzyskania zrozumiałych informacji o podstawach wyników lub rekomendacji algorytmu.

Możesz wykorzystać te sześć zasad jako własną listę kontrolną przy ocenie każdego produktu AI i zapytać dostawcę, jak jego rozwiązanie odnosi się do każdej z nich. Możesz także poprosić dostawcę o przedstawienie formalnej oceny zgodności produktu z zasadami FUTURE-AI lub równoważnymi frameworkami odpowiedzialnej AI. Brak takiej dokumentacji nie dyskwalifikuje produktu, ale gotowość dostawcy do jej przygotowania świadczy o dojrzałości jego podejścia do odpowiedzialnego rozwoju AI.

2. Czy istnieje procedura na wypadek błędnej rekomendacji algorytmu?

Algorytmy mogą się mylić, i to nie jest kwestia czy, ale kiedy. Błędna rekomendacja AI w środowisku klinicznym może mieć realne konsekwencje dla pacjenta. Dlatego zanim wdrożysz produkt, musisz mieć gotową odpowiedź na pytanie: co się dzieje, gdy algorytm się pomyli?

Procedura postępowania na wypadek błędnej rekomendacji powinna być ustalona przed wdrożeniem, nie po pierwszym incydencie. Powinna określać, kto i w jaki sposób dokumentuje błąd, jak jest on zgłaszany wewnętrznie i czy wymaga zgłoszenia do zewnętrznych organów. W przypadku wyrobów medycznych i wyrobów do diagnostyki in vitro należy zweryfikować, czy zdarzenie spełnia kryteria incydentu podlegającego zgłoszeniu w ramach systemu nadzoru (vigilance) wynikającego z MDR lub IVDR. Takie zgłoszenie kierowane jest do Urzędu Rejestracji Produktów Leczniczych, Wyrobów Medycznych i Produktów Biobójczych (URPL). Równie ważne jest ustalenie, co dzieje się z tą informacją dalej, gdy trafia do dostawcy, czy upoważnionego przedstawiciela, czy uruchamia proces przeglądu algorytmu i czy wpływa na jego aktualizację? Błędne rekomendacje, odpowiednio udokumentowane i przeanalizowane, są cennym źródłem wiedzy o słabościach modelu.

ZAPAMIĘTAJ: Algorytm bez procedury awaryjnej to algorytm niegotowy do wdrożenia. Ryzyka biasu i błędów nie można całkowicie wyeliminować. Liczy się to, czy Twoja organizacja i dostawca są na nie przygotowani i czy potrafią wyciągać z nich wnioski.

Pytanie 7

Czy dane medyczne będą przetwarzane zgodnie z prawem?

1. **Jak dane są gromadzone i gdzie przechowywane (on-premise vs. chmura, UE vs poza UE)?**
   Dane medyczne to jedne z najbardziej wrażliwych danych osobowych, więc miejsce ich przechowywania ma znaczenie prawne, nie tylko techniczne. Zanim podpiszesz umowę z dostawcą, musisz wiedzieć dokładnie, gdzie dane Twoich pacjentów będą się fizycznie znajdować.

   Pierwsze pytanie dotyczy modelu przechowywania: czy dane pozostają zasadniczo w infrastrukturze Twojego szpitala (on-premise), czy są przesyłane do chmury zewnętrznego dostawcy? Oba modele mają swoje zalety i ryzyka, oba są dopuszczalne prawnie, także w odniesieniu do przetwarzania danych medycznych, ale model chmurowy wymaga szczególnej uwagi. Kluczowe znaczenie ma nie sam wybór między chmurą a on-premise, lecz zastosowane zabezpieczenia, certyfikacje, jasny podział odpowiedzialności między dostawcą a Twoją organizacją oraz lokalizacja danych. Model chmurowy oznacza, że dane są przetwarzane w infrastrukturze dostawcy, co wymaga zweryfikowania tych elementów. Warto jednak pamiętać, że certyfikowana, odpowiednio zabezpieczona chmura może być lepiej zabezpieczona niż lokalna infrastruktura placówki. Model on-premise oznacza z kolei, że dane pozostają fizycznie w infrastrukturze Twojej organizacji, ale to Ty przejmujesz większość odpowiedzialności za jej zabezpieczenie, utrzymanie i aktualizacje. Sprawdź, czy Twój dział IT ma realne zasoby, żeby się tym zaopiekować.

   Drugie pytanie dotyczy lokalizacji danych: czy serwery znajdują się na terenie Europejskiego Obszaru Gospodarczego (EOG) i czy dostęp do danych mają podmioty spoza EOG? Zgodnie z RODO przekazywanie danych poza EOG jest możliwe pod określonymi warunkami, np. na podstawie standardowych klauzul umownych lub decyzji Komisji Europejskiej o odpowiednim poziomie ochrony (w tym EU-US Data Privacy Framework dla objętych nim firm w USA). Samo przechowywanie danych w UE nie wyklucza ich przekazywania poza EOG, dlatego warto zweryfikować te kwestie z inspektorem ochrony danych.

Pytanie 7

Czy dane medyczne będą przetwarzane zgodnie z prawem?

2. **Czy przetwarzanie jest zgodne z RODO[13] i krajowymi przepisami o danych medycznych?**
   Dane medyczne to w rozumieniu RODO dane szczególnej kategorii. Ich przetwarzanie wymaga nie tylko podstawy prawnej, ale spełnienia dodatkowych, rygorystycznych warunków. W polskim kontekście do RODO dochodzą przepisy ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, ustawy o systemie informacji w ochronie zdrowia oraz przepisy dotyczące elektronicznej dokumentacji medycznej. To nie jest obszar, w którym można polegać wyłącznie na zapewnieniach dostawcy. Jeżeli dostawca będzie przetwarzał dane osobowe w imieniu Twojej placówki, przed rozpoczęciem takiego przetwarzania należy również zawrzeć odpowiednią umowę powierzenia danych zgodnie z art. 28 RODO, uwzględniającą m.in. zasady korzystania z podwykonawców. Warto również sprawdzić, czy dostawca wyznaczył inspektora ochrony danych (IOD[14]), czy posiada wdrożone procedury reagowania na naruszenia ochrony danych lub jakiekolwiek certyfikaty z obszaru bezpieczeństwa informacji.

3. **Czy dane są wykorzystywane wyłącznie do realizacji usługi, czy również do trenowania, dostrajania (fine-tuningu), walidacji lub rozwoju innych modeli AI?**
   Dane Twoich pacjentów mogą być przez dostawcę wykorzystywane nie tylko do działania algorytmu w Twojej organizacji, ale również do trenowania i doskonalenia modelu, także na potrzeby innych klientów dostawcy. W odniesieniu do danych o stanie zdrowia taka sytuacja wymaga szczególnej uwagi, a warunki takiego wykorzystania danych przez dostawcę powinny być bardzo precyzyjnie określone w umowie. Pacjenci, których dane miałyby być wykorzystywane do trenowania modelu powinni być o tym wyraźnie poinformowani, a dostawca powinien dysponować ważną podstawą prawną do przetwarzania tego rodzaju danych zgodnie z art. 9 RODO. Warto więc sprawdzić, czy dostawca rozróżnia w swojej dokumentacji dane używane do świadczenia usługi od danych używanych do celów rozwojowych, i czy istnieją techniczne mechanizmy egzekwowania ew. sprzeciwu lub wycofania zgody dotyczących takiego przetwarzania, a nie tylko same zapisy w umowie.

4. **Kto ma dostęp do danych i jak jest to kontrolowane?**
   Dostęp do danych medycznych powinien być ściśle ograniczony do osób, które rzeczywiście go potrzebują, zarówno po stronie Twojej organizacji, jak i po stronie dostawcy. W praktyce szerokie uprawnienia dostępu, brak logowania aktywności użytkowników i nieaktualne listy osób uprawnionych to jedne z najczęstszych słabości w bezpieczeństwie systemów IT w ochronie zdrowia.

   Zapytaj dostawcę, kto po jego stronie ma dostęp do danych Twoich pacjentów i czy są to tylko inżynierowie odpowiedzialni za utrzymanie systemu, czy również zespoły sprzedażo-

[13] RODO - Rozporządzenie o Ochronie Danych Osobowych (UE 2016/679); reguluje zasady przetwarzania danych osobowych na terenie UE.
[14] IOD - Inspektor Ochrony Danych; osoba odpowiedzialna za nadzór nad zgodnością przetwarzania danych z przepisami prawa.

we, analityczne lub zewnętrzni podwykonawcy? Sprawdź, czy dostęp jest logowany i czy logi są regularnie przeglądane.

Po stronie Twojej organizacji warto upewnić się, że uprawnienia dostępu są przyznawane zgodnie z zasadą minimalnego dostępu (każda osoba ma dostęp wyłącznie do tych danych i funkcji, które są niezbędne do wykonywania jej obowiązków).

5. **Czy przeprowadzono ocenę skutków dla ochrony danych (DPIA)?**
DPIA (Data Protection Impact Assessment) to ocena skutków dla ochrony danych. Jest to obowiązkowa analiza ryzyka wymagana przez RODO przed rozpoczęciem przetwarzania danych w ramach procesów, które niosą za sobą wysokie ryzyko naruszenia praw i wolności osób fizycznych. Przetwarzanie danych medycznych przez system AI zazwyczaj będzie wymagać przeprowadzenia tego rodzaju analizy. Jeśli DPIA jest wymagana, Twoja organizacja jako administrator danych powinna przeprowadzić i udokumentować taką ocenę przed rozpoczęciem przetwarzania danych za pomocą systemu AI.

DPIA powinna identyfikować rodzaje przetwarzanych danych i cel ich przetwarzania, oceniać niezbędność i proporcjonalność operacji przetwarzania danych, ryzyko dla pacjentów oraz określać środki minimalizujące to ryzyko (techniczne i organizacyjne). Jeśli po przeprowadzeniu oceny ryzyko pozostaje wysokie i nie można go zredukować, organizacja ma obowiązek skonsultować się z Urzędem Ochrony Danych Osobowych (UODO) przed rozpoczęciem przetwarzania lub zaniechać wdrożenie.

Zapytaj dostawcę, czy i w jaki sposób może wesprzeć Cię w przeprowadzeniu DPIA, niekiedy wsparcie to jest wymagane prawem w związku z pełnieniem roli podmiotu przetwarzającego przez dostawcę. Dobrą praktyką jest również udostępnianie przez dostawcę dokumentacji dotyczącej ochrony danych i analizy ryzyka, która może pomóc Twojej organizacji w przeprowadzeniu DPIA. Zapytaj dostawcę, czy ma taką dokumentację i może Ci ją udostępnić.

ZAPAMIĘTAJ: Dane medyczne to jedne z najbardziej wrażliwych danych osobowych. Ich ochrona to nie formalność, lecz obowiązek prawny i etyczny. Zanim podpiszesz umowę, sprawdź, gdzie dane Twoich pacjentów będą przechowywane, kto będzie miał do nich dostęp i w jakim celu będą wykorzystywane. Upewnij się, że przetwarzanie jest zgodne z RODO i polskimi przepisami, oraz że oceniono konieczność przeprowadzenia DPIA i jeżeli jest ona wymagana, odpowiednio ją udokumentowano. Odpowiedzialność za dane Twoich pacjentów pozostaje po Twojej stronie, niezależnie od tego, komu je powierzasz.

Pytanie 8

Czy rozwiązanie jest cyberbezpieczne?

1. **Czy dostawca przeprowadził testy penetracyjne i audyt bezpieczeństwa?**
   System AI przetwarzający dane medyczne jest atrakcyjnym celem dla cyberprzestępców, ponieważ zawiera wrażliwe dane osobowe, często jest podłączony do krytycznej infrastruktury szpitala i bywa słabiej zabezpieczony niż główne systemy IT. Dlatego bezpieczeństwo produktu powinno być weryfikowane nie tylko deklaratywnie, ale przez niezależnych ekspertów.

   Testy penetracyjne - są to kontrolowane próby włamania do systemu przeprowadzane przez specjalistów ds. cyberbezpieczeństwa. Pozwalają wykryć luki zanim zrobią to przestępcy. Zapytaj dostawcę, kiedy ostatnio przeprowadzono takie testy, kto je wykonał i czy raport jest dostępny do wglądu. Zapytaj również, czy wykryte podatności usunięto i czy skuteczność poprawek została zweryfikowana.

   Audyt bezpieczeństwa to z kolei szerszy przegląd architektury systemu, procedur i polityk bezpieczeństwa. Powinien być przeprowadzany regularnie, nie jednorazowo przed sprzedażą produktu.

2. **Czy w procesie zakupowym uwzględniasz wymogi weryfikacji kontrahentów, które wynikają z przepisów prawa lub wewnętrznych regulacji Twojej organizacji?**
   Znowelizowana ustawa o krajowym systemie cyberbezpieczeństwa (KSC), wdrażająca unijną dyrektywę NIS2, obejmuje również część placówek medycznych. To, czy dany szpital podlega nowym obowiązkom, zależy m.in. od rodzaju prowadzonej działalności oraz wielkości organizacji. Placówki objęte ustawą muszą odpowiednio zarządzać ryzykiem cyberbezpieczeństwa, w tym dbać o bezpieczeństwo kupowanych systemów informatycznych i ich dostawców. Dla podmiotów, które były objęte nowymi przepisami już w dniu ich wejścia w życie, termin wdrożenia istotnej części nowych obowiązków upływa 3 kwietnia 2027 r.

   W kontekście zakupu produktów AI oznacza to, że każde nowe rozwiązanie informatyczne wprowadzane do infrastruktury IT podmiotu leczniczego musi być ocenione zgodnie z procedurami weryfikacyjnymi, które wdrożone są w Twojej organizacji. Dostawca powinien wykazać, że jego produkt nie osłabia bezpieczeństwa Twojej infrastruktury i wspiera spełnienie wymogów wynikających z ustawy lub norm międzynarodowych. Z perspektywy oprogramo-

Pytanie 8

Czy rozwiązanie jest cyberbezpieczne?

wania dostarczanego przez zewnętrzny podmiot, szczególnie istotne są wymogi dotyczące wykrywania i raportowania podatności, zarządzania aktualizacjami produktu oraz mechanizmy stosowane w celu zapewnienia poufności danych.

Na etapie wyboru rozwiązania, zadaj więc dostawcy konkretne pytania: Czy produkt był audytowany pod kątem zgodności z międzynarodowymi standardami bezpieczeństwa informacji lub przepisami o cyberbezpieczeństwie? Czy dostawca może udostępnić do wglądu posiadane certyfikaty lub raporty z audytów? W jaki sposób dostawca wspiera swoich klientów w zapewnieniu zgodności z ustawą o krajowym systemie cyberbezpieczeństwa? Czy dostawca wspiera swoich klientów w spełnieniu wymogów dot. raportowania incydentów cyber?

3. Jak wygląda szyfrowanie danych w spoczynku i w transmisji?

Szyfrowanie to podstawowy mechanizm ochrony danych medycznych, zarówno gdy są przechowywane na serwerach, jak i gdy są przesyłane między systemami. W kontekście produktu AI dane mogą pokonywać długą drogę: od systemu szpitalnego, przez infrastrukturę dostawcy, do algorytmu i z powrotem. Dane powinny być szyfrowane podczas przechowywania i transmisji, a podczas przetwarzania chronione odpowiednimi mechanizmami bezpieczeństwa.

Zapytaj dostawcę, jakie standardy szyfrowania stosuje, zarówno dla danych przechowywanych (szyfrowanie w spoczynku[15]), jak i dla danych przesyłanych (szyfrowanie w transmisji[16]). Aktualne standardy branżowe to AES-256[17] dla danych w spoczynku oraz TLS[18] 1.2 lub wyższy dla transmisji. Sprawdź również, kto zarządza kluczami szyfrującymi, czy dostawca, czy Twoja organizacja? To istotne, ponieważ sposób zarządzania kluczami wpływa na to, kto i na jakich zasadach może uzyskać dostęp do Twoich danych.

4. Czy istnieje plan reakcji na incydent bezpieczeństwa?

Cyberatak na szpital to rzeczywistość, z którą polskie placówki medyczne mierzą się praktycznie codziennie. Ransomware blokujący dostęp do dokumentacji medycznej, wyciek danych pacjentów, awaria systemu w trakcie dyżuru to przykładowe scenariusze, które mogą mieć bezpośrednie konsekwencje dla bezpieczeństwa pacjentów.
Kluczowym pytaniem powinno być zatem: “Co zrobić, gdy nastąpi cyberatak?”

[15] Szyfrowanie w spoczynku (encryption at rest) - ochrona danych przechowywanych na serwerach lub dyskach. Dane są zaszyfrowane i nieczytelne bez odpowiedniego klucza.

[16] Szyfrowanie w transmisji (encryption in transit) - ochrona danych podczas ich przesyłania między systemami. Chroni treść przesyłanych danych przed odczytaniem przez nieuprawnione osoby.

[17] AES-256 - wariant algorytmu szyfrowania AES wykorzystujący klucz o długości 256 bitów. Jest powszechnie stosowany i uznawany za bezpieczny przy prawidłowej implementacji oraz odpowiednim zarządzaniu kluczami szyfrującymi.

[18] TLS (Transport Layer Security) - protokół zapewniający bezpieczną transmisję danych przez sieć. TLS 1.3 jest obecnie preferowanym standardem transmisji danych. TLS 1.2 pozostaje absolutnym minimum wspieranym przez większość systemów i usług chmurowych. Wersje 1.0 i 1.1 są oficjalnie wycofane i ich obecność w systemie dostawcy powinna wzbudzić niepokój.

Pytanie 8

Czy rozwiązanie jest cyberbezpieczne?

Dostawca produktu AI powinien posiadać udokumentowany plan reakcji na incydent bezpieczeństwa, określający, kto jest odpowiedzialny za wykrycie i zgłoszenie incydentu, jakie kroki są podejmowane w pierwszych godzinach, jak wygląda komunikacja z organizacją klienta i jak przebiega przywracanie systemu do działania. Po stronie Twojej organizacji równie ważne jest ustalenie, kto i w jakim trybie zostanie powiadomiony o incydencie oraz w jaki sposób będzie wyglądać dalsza praca nad incydentem, w tym w szczególności na kim w Twojej organizacji spoczywać będą obowiązki wynikające z ustawy o krajowym systemie cyberbezpieczeństwa (np. obowiązek przekazania wczesnego ostrzeżenia w ciągu 24 godzin, zgłoszenia incydentu poważnego w ciągu 72 godzin oraz sprawozdania końcowego co do zasady w ciągu miesiąca od zgłoszenia, zgodnie z właściwymi przepisami i terminami ich stosowania). Jeżeli incydent obejmuje naruszenie ochrony danych osobowych, należy niezależnie ocenić obowiązki wynikające z RODO.

5. **Czy dostawca posiada certyfikację w zakresie bezpieczeństwa informacji (np. ISO/IEC 27001)?**
   Testy penetracyjne i audyty bezpieczeństwa mogą być przeprowadzane jednorazowo i na życzenie. Certyfikacja ISO/IEC 27001 oznacza, że dostawca wdrożył u siebie systemowe podejście do zarządzania bezpieczeństwem informacji, które jest regularnie weryfikowane przez niezależną jednostkę certyfikującą. To niezależne potwierdzenie tego, co dostawca deklaruje w odpowiedziach na poprzednie pytania dotyczące szyfrowania, kontroli dostępu czy reagowania na incydenty.

   Zapytaj dostawcę, czy posiada aktualny certyfikat ISO/IEC 27001 lub inne niezależne potwierdzenie bezpieczeństwa (np. raport SOC 2 Type II). Sprawdź, czy dokument jest aktualny oraz czy obejmuje zakres działalności związany z dostarczanym produktem.

6. **Czy system jest odporny na ataki typu prompt injection?**
   W przypadku rozwiązań wykorzystujących generatywną AI należy zweryfikować odporność systemu na ataki typu prompt injection, polegające na próbach manipulowania działaniem modelu za pomocą specjalnie przygotowanych instrukcji, np. ukrytych w dokumentach lub danych wejściowych. Zapytaj dostawcę, jakie mechanizmy zabezpieczają system przed nieautoryzowanym ujawnieniem danych, manipulacją odpowiedziami oraz wykonywaniem niepożądanych działań.

ZAPAMIĘTAJ: Cyberbezpieczeństwo produktu AI to element bezpieczeństwa pacjentów i odpowiedzialności prawnej kierownictwa placówki. Sprawdź, czy dostawca przeprowadził niezależne testy penetracyjne, czy produkt spełnia wymogi w zakresie bezpieczeństwa informacji, jakie standardy szyfrowania stosuje dostawca i czy ma gotowy plan reakcji na incydent.

Pytanie 9

Czy zapewnisz utrzymanie AI po wdrożeniu?

1. **Jak wygląda wsparcie techniczne dostawcy (SLA, czas reakcji)?**
   Dostępność produktu AI i wsparcia technicznego powinna odpowiadać godzinom jego wykorzystywania oraz znaczeniu dla ciągłości opieki. W przypadku systemów potrzebnych podczas całodobowej pracy klinicznej może to oznaczać wymaganie dostępności i wsparcia 24/7. Awaria systemu wspierającego decyzje kliniczne w środku nocnego dyżuru to nie problem techniczny do rozwiązania następnego dnia roboczego. Dlatego warunki wsparcia technicznego powinny być wynegocjowane i zapisane w umowie zanim produkt trafi do użytku.

   SLA, czyli umowa o poziomie usług, określa gwarantowaną dostępność systemu, maksymalny czas reakcji na zgłoszenie i czas przywrócenia działania po awarii. Sprawdź, czy dostawca oferuje wsparcie 24/7, czy tylko w godzinach biurowych, i czy czas reakcji i przywrócenia usługi różni się w zależności od priorytetu zgłoszenia, i czy jest adekwatny do potrzeb. Zapytaj też, czy wsparcie jest realizowane przez lokalny zespół w Polsce czy przez zdalny helpdesk za granicą. Pamiętaj, że w środowisku klinicznym bariera językowa i różnica stref czasowych mogą mieć realne znaczenie.

2. **Jak często aktualizowane jest oprogramowanie i model AI?**
   Aktualizacje produktu AI mogą mieć wpływ na poprawę bezpieczeństwa, skuteczności i zgodności z przepisami. Oprogramowanie nieaktualizowane może stać się podatne na cyberzagrożenia, a model AI, który nie jest odświeżany może z czasem tracić skuteczność, gdy zmienia się populacja pacjentów, protokoły kliniczne lub sposób wprowadzania danych.

   Zapytaj dostawcę, jak często wydawane są aktualizacje i czy są one obowiązkowe czy opcjonalne. Sprawdź, czy aktualizacja modelu AI wymaga ponownej walidacji lub oceny zgodności. Zależy to od charakteru wprowadzonych zmian oraz ich wpływu na bezpieczeństwo i skuteczność produktu. Ważne jest też, kto i z jakim wyprzedzeniem jest informowany o planowanych aktualizacjach. Nagła zmiana zachowania algorytmu bez uprzedzenia personelu może prowadzić do niebezpiecznych sytuacji klinicznych.

Pytanie 9

Czy zapewnisz utrzymanie AI po wdrożeniu?

3. **Czy jest plan naprawczy i możliwość cofnięcia do poprzedniej wersji?**
   Każda aktualizacja niesie ze sobą ryzyko. Nowa wersja oprogramowania może wprowadzić błąd, który nie ujawnił się podczas testów, albo zmienić zachowanie algorytmu w sposób niezgodny z oczekiwaniami personelu. W środowisku klinicznym taki scenariusz nie może oznaczać paraliżu. Musi istnieć gotowy plan działania.

   Zapytaj dostawcę, czy istnieje możliwość cofnięcia systemu do poprzedniej, działającej wersji i ile taka operacja trwa. W przypadku krytycznej awarii czas przywrócenia działania może mieć bezpośredni wpływ na bezpieczeństwo pacjentów. Sprawdź również, czy dostawca posiada udokumentowany plan naprawczy, określający kroki postępowania w przypadku wykrycia błędu, osoby odpowiedzialne i sposób komunikacji z Twoją organizacją.

   Jeżeli cofnięcie wersji jest niemożliwe lub przywróciłoby znane podatności albo błędy, dostawca powinien wskazać alternatywną procedurę przywrócenia bezpiecznego działania. Plan powinien również zapewniać ciągłość pracy placówki na czas niedostępności systemu.

4. **Czy dostawca zapewnia monitoring działania modelu po wdrożeniu?**
   Wdrożenie AI to nie koniec odpowiedzialności dostawcy. Zapytaj, czy dostawca aktywnie monitoruje działanie modelu po wdrożeniu i czy udostępnia Twojej organizacji raporty dotyczące skuteczności, stabilności działania i wykrytych anomalii. Kluczowe obszary monitoringu to: dryft danych, zmiana jakości predykcji oraz wykrywanie i raportowanie incydentów. Dla produktów będących wyrobami medycznymi lub wyrobami do diagnostyki in vitro obowiązek prowadzenia nadzoru po wprowadzeniu do obrotu wynika odpowiednio z MDR lub IVDR. Zapytaj dostawcę, jak producent realizuje PMS oraz - w zakresie mającym zastosowanie - PMCF lub PMPF, jakie raporty sporządza i jakie wyniki tego nadzoru może udostępnić Twojej organizacji.

5. **Co się stanie, jeśli dostawca zakończy działalność?**
   To pytanie, które wielu kupujących pomija, ale jeśli Twój dostawca zniknie z rynku, co stanie się z produktem, który stał się częścią codziennej pracy klinicznej?

   Przed podpisaniem umowy ustal jasne warunki wyjścia: czy po zakończeniu współpracy zachowasz dostęp do swoich danych i w jakim formacie zostaną one przekazane, czy kod źródłowy lub model AI zostanie zdeponowany u niezależnej strony trzeciej

Pytanie 9

Czy zapewnisz utrzymanie AI po wdrożeniu?

(tzw. escrow[19]), a jeśli tak to jak często depozyt będzie aktualizowany, co stanie się z licencją na oprogramowanie i czy będziesz mógł kontynuować użytkowanie produktu przez określony czas? Sprawdź też, czy umowa zawiera zapisy na wypadek przejęcia dostawcy przez inną firmę. Nowy właściciel może zmienić warunki współpracy lub całkowicie wycofać produkt z rynku.

ZAPAMIĘTAJ: Sprawdź warunki SLA, upewnij się, że aktualizacje modelu są transparentne i poprzedzone walidacją, i zadbaj o plan naprawczy na wypadek awarii. Myśl też o scenariuszach trudnych: co się stanie, jeśli dostawca zbankrutuje, zostanie przejęty lub wycofa produkt? Odpowiedzi na te pytania powinny znaleźć się w umowie, zanim jeszcze produkt trafi do Twojej organizacji.

[19] Escrow - mechanizm, w którym kod źródłowy lub model AI jest deponowany u niezależnej strony trzeciej i udostępniany kupującemu w określonych sytuacjach, np. upadłości dostawcy.

Pytanie 10

Czy znasz pełny koszt i długoterminową korzyść?

1. **Jaki jest całkowity koszt posiadania (TCO[20]): licencja, wdrożenie, integracja, szkolenia i utrzymanie?**
   Całkowity koszt posiadania produktu (TCO) obejmuje wszystkie wydatki związane z produktem przez cały okres jego użytkowania, i w przypadku AI w ochronie zdrowia potrafi być wielokrotnie wyższy niż sama licencja.

   Do kosztów, które warto uwzględnić w kalkulacji należą: wdrożenie i konfiguracja systemu, integracja z istniejącą infrastrukturą IT (HIS, PACS, LIS), szkolenia personelu, bieżące utrzymanie i wsparcie techniczne, koszty przechowywania danych, ewentualna rozbudowa infrastruktury obliczeniowej oraz koszty ponownej walidacji modelu po aktualizacjach. Do tego dochodzą koszty po stronie Twojej organizacji takie jak czas działu IT, zaangażowanie personelu klinicznego w pilotaż i wdrożenie oraz koszty zarządzania zmianą.

   Poproś dostawcę o szczegółową wycenę wszystkich elementów, nie tylko licencji, i porównuj oferty na tej samej podstawie. Zwróć szczególną uwagę na sposób obliczania wynagrodzenia dostawcy - czy jest ono stałe, zależy od ilości użytkowników, ilości przetwarzanych danych czy innej metryki? Zweryfikuj również czy ewentualne limity ujęte w kosztach licencji są adekwatne do skali organizacji i planowanego wykorzystania wdrażanego rozwiązania.

2. **Jaki jest model udostępniania i rozliczania produktu: licencja bezterminowa, czasowa czy dostęp w modelu SaaS?**
   Model licencjonowania produktu AI ma bezpośredni wpływ na koszty, elastyczność i ryzyko długoterminowe dla Twojej organizacji. Przed podpisaniem umowy musisz dokładnie rozumieć, za co płacisz i na jakich warunkach.

[20] TCO (Total Cost of Ownership) - całkowity koszt posiadania; suma wszystkich kosztów związanych z zakupem, wdrożeniem i użytkowaniem produktu przez cały okres jego eksploatacji.

Pytanie 10

Czy znasz pełny koszt i długoterminową korzyść?

Licencja jednorazowa oznacza jednorazową opłatę za prawo do użytkowania produktu. Często jednak nie obejmuje aktualizacji modelu ani wsparcia technicznego po określonym czasie. Licencja czasowa (subskrypcyjna) to regularne opłaty (miesięczne lub roczne), które zazwyczaj obejmują aktualizacje i wsparcie, ale generują stały koszt i uzależniają organizację od ciągłości współpracy z dostawcą. Model SaaS oznacza korzystanie z oprogramowania jako usługi, zwykle przez sieć, na infrastrukturze zarządzanej przez dostawcę lub jego podwykonawców. Wymaga to ustalenia zasad dostępu do danych, ich przechowywania, bezpieczeństwa i eksportu po zakończeniu współpracy.

3. **Czy w pakiecie są dodatkowe usługi (szkolenia, wsparcie, aktualizacje)?**
   Oferty dostawców bywają skonstruowane tak, że podstawowa cena wygląda atrakcyjnie, a każda dodatkowa usługa jest płatna osobno. Szkolenia, wsparcie techniczne, aktualizacje modelu, dostęp do nowych funkcji - wszystko to może znajdować się poza pakietem podstawowym i generować koszty, które nie zostały uwzględnione w budżecie.

   Przed podpisaniem umowy sprawdź dokładnie, co jest wliczone w cenę, a co jest opcją dodatkową. Szczególną uwagę zwróć na szkolenia - czy obejmują tylko pierwsze wdrożenie, czy również szkolenia dla nowych pracowników w przyszłości? Sprawdź, czy aktualizacje modelu AI są automatycznie wliczone w subskrypcję, czy wymagają osobnej opłaty. Upewnij się też, że wsparcie techniczne zapisane w SLA jest częścią pakietu, a nie usługą premium dostępną za dopłatą.

4. **Jak zmierzysz zwrot z inwestycji (ROI[21]) - jakie KPI[22] zastosujesz?**
   ROI w ochronie zdrowia rzadko sprowadza się wyłącznie do oszczędności finansowych, równie ważne są korzyści kliniczne, organizacyjne i jakościowe. Zanim wdrożysz produkt, musisz wiedzieć, po czym poznasz, że inwestycja się opłaciła.

   Zacznij od zdefiniowania punktu odniesienia. Jak wygląda sytuacja dziś, bez AI? Następnie określ mierzalne wskaźniki, które będziesz monitorować po wdrożeniu. W zależności od zastosowania produktu mogą to być: skrócenie czasu diagnozy, zmniejszenie liczby błędów klinicznych, redukcja liczby readmisji, poprawa wykorzystania zasobów, skrócenie czasu oczekiwania pacjentów, oszczędności w kosztach operacyjnych, itp. Zaplanuj regularne przeglądy tych wskaźników i ustal z góry, jaki poziom efektywności uznajesz za satysfakcjonujący, a jaki za niewystarczający.

[21] ROI (Return on Investment) - zwrot z inwestycji; miara efektywności finansowej inwestycji, wyrażona jako stosunek zysku do poniesionych kosztów.
[22] KPI (Key Performance Indicators) - kluczowe wskaźniki efektywności; mierzalne wartości pozwalające ocenić, czy organizacja osiąga założone cele.

Pytanie 10

Czy znasz pełny koszt i długoterminową korzyść?

5. **Czy umowa pozwala na wyjście bez vendor lock-in?**
   Vendor lock-in to sytuacja, w której organizacja staje się tak uzależniona od konkretnego dostawcy, jego technologii, formatów danych, infrastruktury, że zmiana dostawcy staje się praktycznie niemożliwa lub bardzo kosztowna. W przypadku produktów AI ryzyko to jest szczególnie realne, bo dane mogą być przechowywane w zastrzeżonym formacie, model może być nierozerwalnie związany z infrastrukturą dostawcy, a personel może być przeszkolony wyłącznie pod konkretne rozwiązanie.

   Przed podpisaniem umowy sprawdź, czy możesz swobodnie zakończyć współpracę: czy dane zostaną przekazane w standardowym, przenośnym formacie, czy okres wypowiedzenia jest rozsądny, czy nie ma ukrytych opłat za wyjście z umowy i czy organizacja zachowa dostęp do historii predykcji i wyników algorytmu po zakończeniu współpracy. Sprawdź też, czy produkt wykorzystuje otwarte standardy interoperacyjności takie jak HL7 FHIR[23], które ułatwiają migrację do innego rozwiązania w przyszłości. W przypadku narzędzi analizujących dane istotnym czynnikiem ograniczającym vendor lock-in jest również niezależność od producenta urządzenia (hardware-agnostic). Rozwiązanie zgodne z wieloma modelami urządzeń stwarza mniejsze ryzyko przywiązania placówki do jednego dostawcy sprzętu. W przypadku oprogramowania dostarczanego w modelu SaaS upewnij się również, czy proponowane przez dostawcę warunki uwzględniają wymogi unijnego rozporządzenia Data Act (ma ono na celu m. in. minimalizację zjawiska vendor lock-in w przypadku zmiany dostawcy usługi chmurowej).

6. **Czy dokumentacja przetargowa pozwala rzetelnie porównać rozwiązania AI?**
   Standardowa dokumentacja przetargowa stosowana w polskich szpitalach była projektowana z myślą o tradycyjnym oprogramowaniu medycznym, nie o systemach AI. Jeśli zapytanie ofertowe nie zawiera wymagań specyficznych dla AI, dostawcy nie będą zobowiązani do przedstawienia dowodów walidacji, informacji o biasie, dokumentacji zgodności z AI Act czy planu monitorowania po wdrożeniu, chyba że ten obowiązek wynika z przepisów prawa.

   Przed rozpoczęciem postępowania zakupowego warto powołać interdyscyplinarny zespół, obejmujący co najmniej przedstawicieli obszaru klinicznego, zamówień publicznych, IT, ochrony danych, cyberbezpieczeństwa i prawa, a także osobę koordynującą wdrożenie, i jasno podzielić odpowiedzialność za ocenę potrzeb, przygotowanie wy-

[23] HL7 FHIR (Health Level 7 Fast Healthcare Interoperability Resources) - międzynarodowy standard wymiany danych medycznych między systemami IT w ochronie zdrowia. Produkty obsługujące FHIR łatwiej integrują się z innymi systemami i są mniej podatne na vendor lock-in. Stosowanie HL7 FHIR ułatwia migrację danych między systemami, choć nie zawsze eliminuje konieczność ich dodatkowego dostosowania.

Pytanie 10

Czy znasz pełny koszt i długoterminową korzyść?

magań, ocenę ofert, integrację, szkolenia, monitorowanie skuteczności oraz obsługę incydentów. W uzasadnionych przypadkach warto też przeprowadzić wstępne konsultacje rynkowe, żeby wymagania były realistyczne i dopasowane do tego, co faktycznie oferuje rynek.

Przygotowując opis przedmiotu zamówienia (OPZ), skup się przede wszystkim na problemie, który chcesz rozwiązać, oraz oczekiwanych efektach, zamiast z góry wskazywać konkretną technologię. Unikaj wymagań, które bez uzasadnienia faworyzują jednego dostawcę. Zadbaj też, aby kryteria oceny ofert pozwalały porównać nie tylko cenę, ale również jakość, skuteczność, bezpieczeństwo i możliwość integracji rozwiązania z infrastrukturą Twojej placówki. Jeśli potrzebujesz sprawdzić produkt w praktyce, rozważ odpowiednio przygotowany pilotaż. W przypadku rozwiązań, które nie są jeszcze dostępne na rynku, można również rozważyć odpowiednie procedury zamówień innowacyjnych. Pamiętaj przy tym o zachowaniu wymagań wynikających z przepisów o zamówieniach publicznych.

Przed ogłoszeniem przetargu warto uzupełnić dokumentację o wymagania charakterystyczne dla AI, w tym, w zależności od rodzaju produktu i poziomu ryzyka, obowiązek przedstawienia:

- wyników walidacji zewnętrznej,
- uzasadnienia kwalifikacji oraz klasyfikacji produktu wg MDR lub IVDR,
- identyfikatora UDI,
- dokumentacji nadzoru po wprowadzeniu do obrotu (PMS) oraz planu PMCF/PMPF,
- dokumentacji zgodności z AI Act,
- procedur zarządzania zmianą modelu AI,
- statusu rejestracji wyrobu w bazie EUDAMED, jeżeli ma zastosowanie taki obowiązek, oraz, w przypadku systemów podlegających obowiązkowi rejestracji na podstawie art. 49 AI Act, statusu rejestracji w odpowiedniej bazie danych,
- polityki bezpieczeństwa danych,
- warunków SLA,
- planu szkoleń i wsparcia po wdrożeniu.

Określając zakres wymaganych w postępowaniu dokumentów lub informacji uwzględnij obowiązujące przepisy, terminy oraz ochronę informacji poufnych.

W przypadku wyrobów medycznych warto również zweryfikować ich status w europejskiej bazie EUDAMED. Od 28 maja 2026 r. obowiązkowe jest korzystanie z pierwszych

Pytanie 10

Czy znasz pełny koszt i długoterminową korzyść?

czterech modułów bazy, obejmujących rejestrację podmiotów, rejestrację wyrobów i kodów UDI, jednostki notyfikowane i certyfikaty oraz nadzór rynku. Należy jednak pamiętać, że terminy realizacji poszczególnych obowiązków rejestracyjnych mogą różnić się w zależności od rodzaju wyrobu i daty jego wprowadzenia do obrotu, z uwzględnieniem przepisów przejściowych.

Dobrze skonstruowana dokumentacja przetargowa to najskuteczniejsze narzędzie selekcji dostawców i najlepsza ochrona organizacji przed zakupem produktu, który nie spełnia oczekiwań. Pamiętaj jednak, że nie ma jednego uniwersalnego wzoru wymagań dla systemów AI. Dopasuj je do realnych potrzeb i specyfiki konkretnego rozwiązania. Wymagania nadmierne lub nieproporcjonalne (np. żądanie certyfikacji jako wyrobu medycznego od produktu, który tej definicji nie spełnia) mogą sprawić, że żaden produkt na rynku nie spełni wszystkich warunków, ograniczając Twój wybór. Dotyczy to zwłaszcza mniejszych placówek. POZ czy szpital powiatowy bez rozbudowanych zespołów specjalistycznych nie musi stosować tej listy w pełnym, maksymalnym zakresie. Zakres wymagań dopasuj do skali ryzyka i realnych możliwości organizacyjnych. Przy zakupach centralnych lub wspólnych dla kilku placówek jasno rozdziel odpowiedzialność centralnego zamawiającego od lokalnych użytkowników systemu, zwłaszcza w zakresie integracji, lokalnej oceny skuteczności, szkolenia personelu, ochrony danych i zgłaszania incydentów.

ZAPAMIĘTAJ: Cena widoczna w ofercie to dopiero początek. Prawdziwy koszt wdrożenia AI obejmuje integrację, szkolenia, utrzymanie i ryzyko uzależnienia od dostawcy. Zanim podpiszesz umowę, ustal TCO, zdefiniuj KPI i sprawdź warunki wyjścia. Dobrze skonstruowana dokumentacja przetargowa to najskuteczniejszy sposób na odróżnienie rzetelnych dostawców od tych, którym zależy wyłącznie na sprzedaży.

Checklista Nabywcy AI,
czyli 10 pytań przed podjęciem decyzji zakupowej

1 Czy na pewno AI jest najlepszym rozwiązaniem, czy też wystarczające jest inne narzędzie?

- Określ problem, który chcesz rozwiązać, i sprawdź, czy AI będzie lepszym wyborem niż prostsze alternatywy.
- Upewnij się, że dysponujesz danymi odpowiedniej jakości, niezbędnymi do działania systemu.

2 Czy AI spełnia wymagania prawne?

- Sprawdź, czy produkt jest wyrobem medycznym i czy posiada wymagane oznakowanie CE oraz dokumentację zgodności.
- Zweryfikuj, jakie wymogi AI Act dotyczą produktu i czy dostawca jest przygotowany do ich spełnienia.

3 Czy AI jest skuteczna i jakie ma na to dowody?

- Poproś o wyniki walidacji i dowody potwierdzające skuteczność rozwiązania.
- Sprawdź, czy algorytm był testowany na populacji podobnej do Twoich pacjentów, najlepiej również poza środowiskiem producenta.

4 Czy AI będzie działać w praktyce?

- Sprawdź, czy rozwiązanie można zintegrować z systemami IT i codzienną pracą Twojej placówki.
- Ustal, jak będziesz mierzyć skuteczność AI po wdrożeniu i reagować na ewentualne błędy.

5 Czy Twój personel jest gotowy na AI?

- Zaangażuj przyszłych użytkowników w ocenę rozwiązania jeszcze przed zakupem.
- Zaplanuj szkolenia i upewnij się, że personel rozumie możliwości, ograniczenia oraz zasady nadzoru nad AI.

6 Czy AI jest etyczna i wolna od dyskryminacji?

- Sprawdź, czy algorytm był oceniany pod kątem stronniczości i różnic w skuteczności między grupami pacjentów.
- Upewnij się, że istnieje procedura postępowania w przypadku błędnej rekomendacji AI.

Checklista Nabywcy AI,
czyli 10 pytań przed podjęciem decyzji zakupowej

7 Czy dane medyczne będą przetwarzane zgodnie z prawem?
- Ustal, gdzie i przez kogo będą przetwarzane dane oraz czy dostawca może wykorzystywać je do trenowania AI.
- Zweryfikuj zgodność z RODO, potrzebę zawarcia umowy powierzenia danych i przeprowadzenia DPIA.

8 Czy rozwiązanie jest cyberbezpieczne?
- Poproś o dowody bezpieczeństwa produktu, np. wyniki testów, audytów lub odpowiednie certyfikaty.
- Sprawdź zabezpieczenia danych i procedury reagowania na incydenty bezpieczeństwa.

9 Czy zapewnisz utrzymanie AI po wdrożeniu?
- Ustal warunki wsparcia technicznego, aktualizacji i monitorowania systemu po wdrożeniu.
- Sprawdź, co stanie się w przypadku awarii, zakończenia działalności dostawcy lub wycofania produktu.

10 Czy znasz pełny koszt i długoterminową korzyść?
- Oszacuj wszystkie koszty zakupu, integracji, szkoleń i utrzymania (TCO) oraz określ mierzalne korzyści z wdrożenia.
- Porównuj oferty nie tylko pod względem ceny, ale również jakości, skuteczności i bezpieczeństwa.
- Sprawdź warunki zakończenia współpracy i możliwość zmiany dostawcy bez utraty dostępu do danych.

PAMIĘTAJ: Nie wszystkie wymagania dotyczą każdego rozwiązania AI. Zakres oceny powinien być dostosowany do przeznaczenia produktu, poziomu ryzyka i potrzeb Twojej organizacji. Szczegółowe wyjaśnienia oraz pytania do dostawców znajdziesz w odpowiednich rozdziałach Poradnika.

Chcesz wiedzieć więcej

bądź potrzebujesz wsparcia we wdrożeniu innowacji do swojej organizacji?

Wybór odpowiedniego rozwiązania AI i jego skuteczne wdrożenie mogą być wyzwaniem. Zespół wZdrowiu dysponuje rozbudowaną bazą startupów medycznych oraz szeroką siecią kontaktów do firm technologicznych, w tym podmiotów będących członkami Koalicji AI i Innowacji w Zdrowiu. Chętnie wesprzemy Twoją placówkę w identyfikacji rozwiązań odpowiadających jej potrzebom, porównaniu dostępnych możliwości oraz zaplanowaniu i przeprowadzeniu wdrożenia. Współpracujemy również z partnerami prawnymi. Możemy pomóc Ci ocenić zgodność wybranego rozwiązania z obowiązującymi przepisami oraz wymaganiami dotyczącymi jego zakupu i wdrożenia.



Skontaktuj się z nami:
Karolina Kornowska - Dyrektor Operacyjna wZdrowiu,
Koordynatorka Koalicji AI i Innowacji w Zdrowiu,
Dyrektor ds. Organizacyjnych PFSz
Liaison Officer HOPE

E-mail: karolina.kornowska@wzdrowiu.com
Tel.: +48 609 908 877

Poznaj inne publikacje i inicjatywy

współtworzone przez Koalicję AI i Innowacji w Zdrowiu oraz Polską Federację Szpitali.



Biała Księga AI w Praktyce Klinicznej

Kompleksowe opracowanie poświęcone praktycznym i prawnym aspektom stosowania sztucznej inteligencji w medycynie. Odpowiada na najważniejsze pytania dotyczące wykorzystania AI przez profesjonalistów medycznych, praw pacjenta, odpowiedzialności oraz bezpiecznego korzystania z nowych technologii. Pierwszy tego typu dokument na tę część Europy, który do tej pory jest stosowany i dyskutowany na forum publicznym.

Zapoznaj się z Białą Księgą:

https://aiwzdrowiu.pl/biala-ksiega-ai/



Raport Otwarcia: Cyfrowa Innowacja Ratunkiem dla Zdrowia

Publikacja przedstawiająca osiem kluczowych szans na przyspieszenie cyfrowej transformacji polskiej ochrony zdrowia. Zawiera przykłady praktycznych zastosowań technologii (case studies) oraz rekomendacje dotyczące m.in. AI, danych medycznych, cyfrowych terapii i cyberbezpieczeństwa.

Zapoznaj się z Raportem Otwarcia:

https://aiwzdrowiu.pl/raport-otwarcia-cyfrowa-innowacja-ratunkiem-dla-zdrowia/



Kodeks Branżowy RODO w ochronie zdrowia

Kodeks został zatwierdzony przez PUODO jako pierwszy w Europie obejmujący podmioty publiczne i prywatne z sektora medycznego. To praktyczny zbiór zasad wspierających placówki medyczne w zgodnym z RODO przetwarzaniu danych osobowych, w tym danych pacjentów. W 2021 r. zdobył pierwsze miejsce w międzynarodowym konkursie Emerging Europe Awards w kategorii „Modern and Future-proof Policymaking".

Zapoznaj się z Kodeksem Branżowym RODO w ochronie zdrowia:

https://uodo.gov.pl/pl/file/4522