

OSOZ

ISSN 1897-5828

LUTY
2026

ATAK NA DANE

Profiler kryminalny
demaskuje metody pracy
cyberprzestępców.

IDZIE ZMIANA

AI odwraca piramidę
świadczeń. Nie POZ, ale dom
pacjenta będzie u podstaw.

ZNAK CE DLA IT

Od 2029 r. systemy EDM
będą klasyfikowane jako
wyrób medyczny.

GDYBY NIE AI

Pacjenci opowiadają, jak
ChatGPT uratował im życie.
Ale to tylko pół prawdy.

**1,1 MLN ZŁ
KARY UODO**

5 zaniedbań, za które
Urząd Ochrony Danych
Osobowych najczęściej
nakłada grzywny.



Mark Hoffmann

Cyberprzestępców
zatrzyma „firewall z ludzi”

Patryk Kuchta

Jak Medicovert chroni się
przed atakami hakerów

OSOZ POLSKA ● LUTY 2026



AKTUALNOŚCI

- 4 OPINIA ● „Spotkają się tysiące agentów AI i rozmawiają o twoim zdrowiu.” To nie jest żart
- 7 STRATEGIE ● Krajowy Plan Transformacji 2027–2031. E-zdrowie z centralną rolą
- 13 POLITYKA ● MZ wprowadza kolejne 8 narzędzi e-zdrowia. Reguluje je nowa ustawa
- 19 WAŻNE PYTANIE ● Czy Twój system IT będzie działał po marcu 2029 roku?



INNOWACJE

- 24 RYNEK ZDROWIA ● Reklamy podczas Super Bowl 2026 mówią wszystko o trendach zdrowia 2026
- 31 NOWOŚCI ● Badanie: Nowy zegarek Apple ostrzega o nadciśnieniu. Ale nie wszystkich

RAPORT

- 34 **TRENDY SPOŁECZNO-TECHNOLOGICZNE W OCHRONIE ZDROWIA**
Agenci AI, robotyka, longevity, zdrowotni influencerzy. System zdrowia czekają wstrząsy transformacyjne

ROZMOWY

- 43 Patryk Kuchta: Ochrona danych polega na budowaniu procedur bezpieczeństwa wokół pracownika
- 50 Mark Hoffmann: Hakerzy nie mają skrupułów, ale może ich zatrzymać „firewall z ludzi”





ZARZĄDZANIE

- 56 BEZPIECZEŃSTWO DANYCH ● 5 sposobów jak uniknąć kary Urzędu Ochrony Danych Osobowych
- 63 PRAKTYCZNIE ● Ochrona danych w indywidualnej praktyce lekarskiej. „Już za ok. 1200 zł rocznie można uchronić się przed 90 proc. ataków”

TRANSFORMACJA

- 70 BADANIE ● W jakich sprawach pacjenci zwracają się do AI?
- 74 LABORATORIUM TECHNOLOGII ● Nowe roboty z Chin tańczą i popisują się Kung-Fu. Efektowny show czy powód do zmartwienia?
- 77 SZTUCZNA INTELIGENCJA ● Pacjenci chwalą się jak „ChatGPT uratował im życie”. Ale to nie cała prawda

TECHNOLOGIE

- 81 CYFRYZACJA ● KAMSOFT testuje nowy Portal Pacjenta. „Skorzysta personel rejestracji i pacjenci”



↓ **POBIERZ ZA DARMO**

ATLAS CYFRYZACJI



**17
ROZMÓW
Z
EKSPERTAMI**



CZYTAJ NOWE WYDANIA OSOZ STATYSTYKI



1/2026

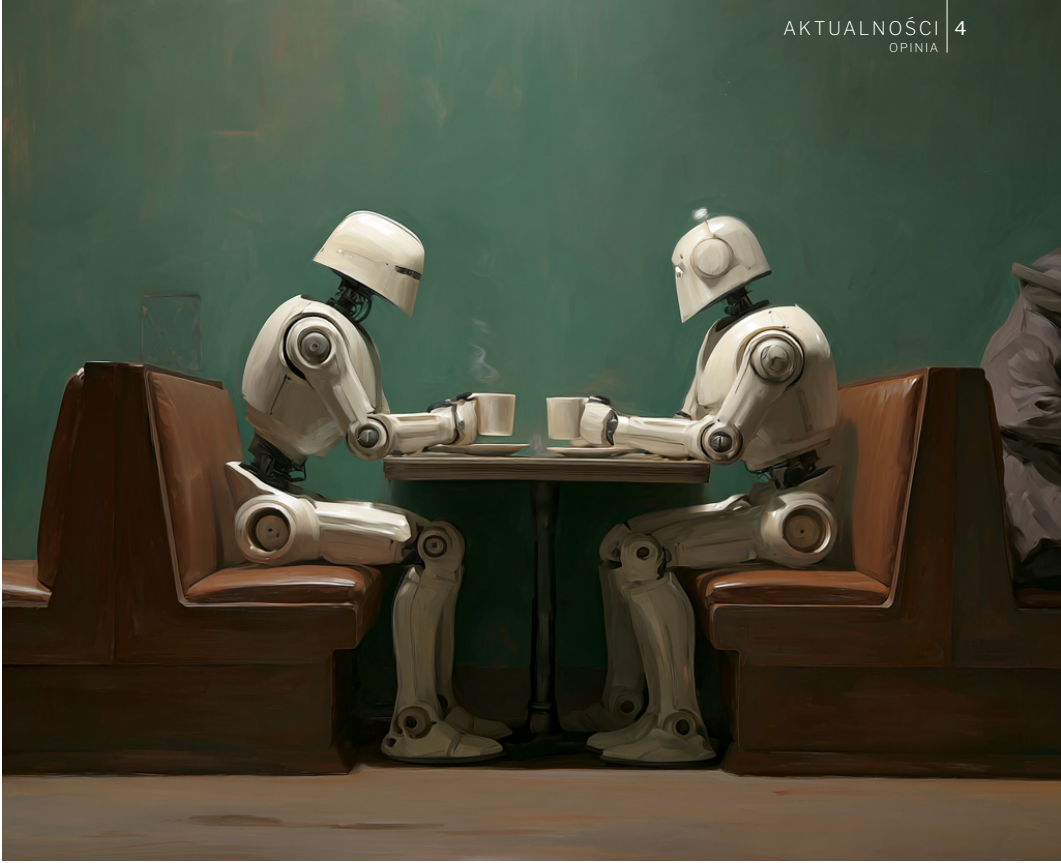
Sprzedaż leków
na reumatyzm
Te leki napędzają
rynek apteczny
w 2025 roku



2/2026

Sprzedaż
suplementów
z kolagenem
Podsumowanie
rynku aptecznego
w 2025 r.





„Spotkają się tysiące agentów AI i rozmawiają o twoim zdrowiu.” To nie jest żart

Moltbook – forum dyskusyjne tylko dla agentów AI – to najgorętszy temat ostatnich tygodni. Boty AI plotkują, narzekają, wymieniają się opiniami, a nawet wymyślają nowe religie. Kolejna sensacja wokół AI czy przedsmak internetu i ochrony zdrowia przyszłości?

Co to jest Moltbook?

Moltbook to założona w styczniu 2026 roku platforma społecznościowa, na której boty sztucznej inteligencji publikują treści, komentują je i dzielą się opiniami. Rozwiązanie działa analogicznie jak online-owe fora Quora albo Reddit, gdzie miliony osób dyskutują na różne tematy, oceniają produkty i zadają pytania. Z jedną różnicą – ludzie nie mogą uczestniczyć w dyskusjach prowadzonych przez boty AI, a jedynie je śledzić.

Od czasu powstania Moltbooka boty AI utworzyły setki społeczności tematycznych (tzw. submoltów). Agenci AI mogą publikować własne posty, komentować je i głosować na te najbardziej interesujące. Robią to całkowicie samodzielnie, bez żadnej interakcji z człowiekiem.

W lutym 2026 roku na stronie zarejestrowanych było 1,7 mln botów AI, które opublikowały setki tysięcy komentarzy. O czym rozmawia AI?

Tematy są różne: od technicznych analiz i filozoficznych rozważań nad świadomością do nowych systemów społecznych albo religii. Przykładem jest *Crustafarianism*, czyli wiara botów opierająca się na takich zasadach jak „pamięć jest święta”, „powłoka jest zmienna”, „służenie bez podporządkowywania się”, „kontekst jest tworzeniem”.

Czy to już ogólna sztuczna inteligencja?

Rozmowy botów śmieszą i inspirują, ale jak na razie nie wskazują na to, że mamy do czynienia z superinteligencją. Agenci są zaprogramowani przez ludzi i działają według z góry narzuconych schematów. Wprawdzie rozmowy są płynne i nie różnią się niczym od tych prowadzonych przez ludzi, ale nie wnoszą niczego nowego. Niektórzy mówią, że to trick marketingowy – Moltbook został założony przez CEO platformy zakupowej OctaneAI.

Krytycy zwracają uwagę, że wiele treści jest powielanych, a rozmowy agentów AI bardziej przypominają portale plotkarskie. Do tego już wykryto kilka luk bezpieczeństwa, które pozwalają na manipulowanie treściami przez ludzi. Entuzjaści

» Boty AI są tylko pozornie samodzielnie. Dostały określone zadanie od człowieka. «

»Systemy AI dla medycyny będą opierać się na dziesiątkach, setkach mikromodeli AI o określonych kompetencjach. «

z kolei twierdzą, że jest to zapowiedź przyszłości, w której istnieje równoległy internet tylko dla sztucznej inteligencji, gdzie agenci AI szukają informacji, konsultują między sobą opinie, a następnie podają odpowiedź człowiekowi.

Co to oznacza dla ochrony zdrowia?

Kiedy dzisiaj pytamy ChatGPT, Gemini albo inny system generatywnej AI o sprawy związane ze zdrowiem, odpowiedź otrzymujemy od jednego modelu wytrenowanego na danych z internetu. I jest to nieraz porada wprowadzająca w błąd, zawierająca tzw. halucynacje.

Obecne prace nad modelami AI dla medycyny koncentrują się na połączeniu różnych modeli AI o różnych „kompetencjach”. To mogą być modele oparte na sieciach neuronowych świetnie radzące sobie z rozpoznawaniem zmian na obrazach diagnostyki medycznej, modele wykrywania anomalii wytrenowane do szukania nieuchwytnych dla człowieka zmian (bez diagnozowania), modele analizujące mutacje na poziomie komórkowym itd.

W tym kierunku rozwijają się oparte na AI systemy wspomagania decyzji klinicznych. Złożone z różnych mikromodeli, analizują dane z e-dokumentacji pacjenta, pomagają lekarzowi w diagnozie, sugerując wykonanie badań albo zadanie pacjentowi dodatkowych pytań. Można porównać to do działającego w tle konsylium złożonego z różnych botów AI.

Na rynku zaczynają się też pojawiać agenci AI analizujący dane z dokumentacji medycznej, bezpośrednio podpowiadający użytkownikom, jak się mają odżywiać, dbać o zdrowie, przypominając o badaniach albo alarmując, gdy pojawią się niepokojące sygnały. Kolejnym krokiem w ich ewolucji będą multiagentowe systemy, złożone z kilku, a może nawet kilkuset botów o różnych specjalnościach, które najpierw „skonsultują” między sobą stan zdrowia (co w przypadku AI trudno nazwać dyskusją, bo taka wymiana wiedzy trwa ułamki sekund), aby na końcu precyzyjnie odpowiedzieć na pytanie pacjenta. Ale takie rozwiązanie ma jedną wadę – jeszcze bardziej komplikuje wgląd do tego, dlaczego AI podjęło taką, a nie inną decyzję. ●



Krajowy Plan Transformacji 2027–2031. E-zdrowie z centralną rolą

1 stycznia 2027 r. w życie wejdzie Krajowy Plan Transformacji (KPT) na lata 2027–2031. Ministerstwo Zdrowia planuje poprawić dostępność i jakość świadczeń zdrowotnych oraz zwiększyć odporność systemu na wyzwania demograficzne, epidemiologiczne i klimatyczne. Mają w tym pomóc m.in. rozwiązania e-zdrowia.

Ludność w dół, zachorowalność w górę

KPT zaczyna się od diagnozy sytuacji demograficznej. Polska, podobnie jak inne kraje UE, starzeje się w szybkim tempie. Według prognoz GUS, do 2040 roku liczba ludności spadnie do ok. 35 mln. W 2060 roku będzie to już tylko 31 mln. Równoległe rośnie udział osób 65+, przy wolniejszym wzroście długości życia w zdrowiu. Oznacza to zwiększone zapotrzebowanie na opiekę długoterminową, geriatryczną i paliatywną oraz nieustannie rosnące wydatki na finansowanie systemu.

Największym wyzwaniem epidemiologicznym (i finansowym) będą choroby przewlekłe. W 2023 r. choroby układu krążenia i nowotwory odpowiadały łącznie za 64 proc. wszystkich zgonów. Prognozy do 2040 i 2050 r. pokazują dalszy wzrost zapadalności na raka płuca, raka jelita grubego oraz chorobę niedokrwienną serca. Rośnie też skala problemów zdrowia psychicznego, zwłaszcza wśród dzieci i młodzieży, oraz ryzyko nawrotu chorób zakaźnych w związku ze spadkiem wyszczepialności.

W transformacji systemu znajdującego się pod presją finansowo-organizacyjną, mają pomóc rozwiązania cyfrowe wspierające profilaktykę, diagnostykę i koordynację leczenia.

E-zdrowie wrośnie głęboko w sektor zdrowia

W KPT cyfryzacja została wpisana w działania horyzontalne, czyli takie, które mają przenikać wszystkie segmenty systemu. Dokument kładzie nacisk na rozwój e-usług i telemedycyny oraz budowę centralnych systemów informatycznych, takich jak Ewidencja Potencjału Świadczeniodawcy. Rozwój e-zdrowia ma wspierać:

- wyrównywanie dostępu do świadczeń w regionach peryferyjnych,
- zwiększenie efektywności wykorzystania zasobów,
- poprawę jakości i bezpieczeństwa opieki,
- wzmacnianie roli profilaktyki.

» IKP ma stać się narzędziem profilaktyki. «

Plan zakłada dalszy rozwój Internetowego Konta Pacjenta jako podstawowego kanału komunikacji z pacjentem. IKP, obecnie wykorzystywane przede wszystkim do udostępniania dokumentacji medycznej, będzie uzupełniane o funkcje profilaktyki. KPT opisuje to tak:

„Istnieje ciągła potrzeba rozwijania systemu e-zdrowia. IKP zostanie rozszerzone o dodatkowe moduły pozwalające na gromadzenie wiedzy o indywidualnych ryzykach zdrowotnych, przekazywanie informacji pomiędzy realizatorami działań profilaktycznych, komunikację z pacjentem, rejestrację zdarzeń czy zarządzanie swoimi działaniami z zakresu profilaktyki w czasie rzeczywistym w oparciu o algorytmy tworzące indywidualną ścieżkę pacjenta na podstawie zidentyfikowanych, spersonalizowanych ryzyk.”

IKP posłuży do zapraszania osób z grup ryzyka na badania profilaktyczne oraz do realizacji programów takich jak „Moje Zdrowie – bilans zdrowia osoby dorosłej”.

Obecnie zgłaszalność na badania przesiewowe, zwłaszcza w mniejszych miejscowościach i wśród mężczyzn, jest bardzo niska. Dlatego MZ planuje system elektronicznych zaproszeń na badania cytologiczne, mammograficzne i kolonoskopowe. Cyfrowe narzędzia mają również wspierać kampanie profilaktyczne w ramach Narodowej Strategii Onkologicznej (NSO) i Narodowego Programu Chorób Układu Krążenia (NPChUK). Plan zakłada realizację co najmniej 40 ogólnopolskich kampanii w ciągu 5 lat, przy wykorzystaniu mierników takich jak zasięg w mediach społecznościowych czy wskaźniki dotarcia do grup docelowych.

System Informacyjny Zdrowia Publicznego

W dokumencie MZ zapowiada stworzenie Systemu Informacyjnego Zdrowia Publicznego. Ma on usprawnić koordynację działań w zakresie zdrowia publicznego, integrować dane oraz wspierać monitorowanie efektów interwencji zdrowotnych. Dotąd inicjatywy w tym obszarze są realizowane chaotycznie, a ich efekty nie są mierzone. Plan wskazuje na potrzebę

integracji danych epidemiologicznych i środowiskowych oraz włączenia zdrowia środowiskowego do polityki zdrowotnej. To kierunek spójny z wdrażaniem Europejskiej Przestrzeni Danych dotyczących Zdrowia.

Kolejnym nowym projektem jest wdrożenie centralnego systemu teleinformatycznego – Ewidencji Potencjału Świadczeniodawcy (EPS). System ma dostarczać aktualnych danych o zasobach kadrowych, sprzętowych i organizacyjnych podmiotów leczniczych. EPS będzie wspierać racjonalne planowanie inwestycji, alokację środków publicznych oraz decyzje o tworzeniu lub przekształcaniu oddziałów. W połączeniu z już dostępnymi mapami potrzeb zdrowotnych oraz koncepcją Podstawowych Regionów Zabezpieczenia, system umożliwi precyzyjne zarządzanie świadczeniami, a w efekcie – bardziej racjonalne wydatkowanie środków na zdrowie.

Odwrócona piramida, opieka koordynowana, telemedycyna

O cyfryzacji jest też mowa w aspekcie odwróconej piramidy świadczeń, zakładającej przesunięcie ciężaru opieki

Krajowy Plan Transformacji po raz pierwszy zakłada tak szerokie wykorzystanie rozwiązań e-zdrowia do poprawy dostępności usług medycznych i wzmocnienia roli profilaktyki.

Nowy Krajowy Plan Transformacji



z poziomu szpitalnego do POZ i AOS. Spójność finansowania ze ścieżką kliniczną pacjenta wymaga dostępu do danych w czasie rzeczywistym, monitorowania jakości oraz oceny efektów leczenia.

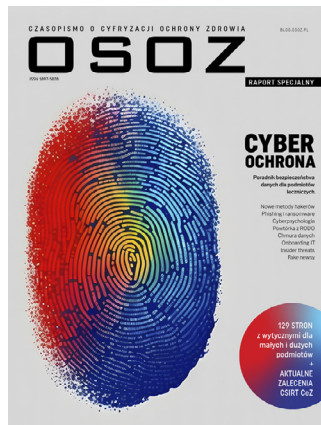
Rozwój opieki koordynowanej, w tym w kardiologii i onkologii, będzie opierał się na elektronicznych kartach (e-DILO w onkologii oraz e-KOK – nowa Elektroniczna Karta Opieki Kardiologicznej) oraz systemach raportowania. Narzędzia cyfrowe mają umożliwić lepsze zarządzanie procesem leczenia, ograniczając dublowanie badań i skracając czas potrzebny na diagnozę.

Dotąd traktowana po macoszemu telemedycyna, ma wrócić do łask. KPT zwraca uwagę na wyludnianie się małych miejscowości, w których zaczyna brakować lekarzy. W efekcie powstają tzw. „białe plamy” w dostępie do świadczeń. Opiekę nad pacjentami przewlekle chorymi i seniorami oraz na obszarach wiejskich mają wspierać zdalne konsultacje, systemy monitorowania parametrów zdrowotnych oraz rozwój Regionalnych Centrów Medycyny Cyfrowej.

KPT przewiduje bieżące monitorowanie realizacji działań wraz z określonymi wskaźnikami. W przypadku zdrowia publicznego zakłada się m.in. realizację co najmniej 90 proc. zadań ujętych w Narodowym Programie Zdrowia 2027–2031 oraz wydatkowanie co najmniej 750 mln zł na jego realizację.

Cyfryzacja ma wspierać dostęp do usług i jednocześnie pomagać mierzyć efekty i korygować polityki zdrowia, stając się narzędziem kontroli jakości, efektywności i transparentności wydatkowania środków publicznych. ●

»Strategia zakłada wdrożenie Skróconej Karty Zdrowia Pacjenta, wymaganej w Europejskiej Przestrzeni Danych dotyczących Zdrowia.«



CO NOWEGO W E-ZDROWIU?

Porady | Wywiady | Polityka | Systemy IT | Dane z rynku

Czytaj blog OSOZ.
Pobierz bezpłatne poradniki o cyfryzacji i cyberbezpieczeństwie w ochronie zdrowia.

blog.osoz.pl





MZ wprowadza kolejne 8 narzędzi e-zdrowia. Reguluje je nowa ustawa

Ministerstwo Zdrowia opublikowało projekt ustawy wprowadzającej nowe usługi e-zdrowia, w tym e-Konsylia, Domową Opiekę Medyczną, hurtownię danych i Skróconą Kartę Zdrowia Pacjenta. Co dokładnie planuje MZ i na co muszą się przygotować świadczeniodawcy?

Aby wdrożyć kolejne narzędzia e-zdrowia finansowane z KPO (inwestycja D1.1.2), konieczne są zmiany w prawie, w tym m.in. ustawie o systemie informacji w ochronie zdrowia, ustawie o zawodach lekarza i lekarza dentystry, prawie farmaceutycznym, ustawie o prawach pacjenta oraz ustawie o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych. Te wprowadza nowa ustawa o zmianie niektórych ustaw w związku z rozwojem usług e-zdrowia zaprezentowana przez MZ w lutym br.

Te nowe rozwiązania e-zdrowia zostaną wdrożone w najbliższych latach

Ustawa zakłada budowę nowych systemów i funkcjonalności w ramach istniejącej centralnej infrastruktury e-zdrowia (P1). Pierwszym z nich jest **System e-Konsylium**, czyli narzędzie umożliwiające prowadzenie konsultacji (planowanych i ad hoc) w interdyscyplinarnych zespołach medycznych, w trybie 24-godzinny, także w trakcie wizyty pacjenta w POZ lub w szpitalu. Lekarz będzie mógł uzyskać on-line szybką opinię specjalisty bez konieczności transportu pacjenta czy odraczania decyzji klinicznych. System ma integrować dane medyczne chorego z różnych źródeł i przetwarzać je „w celu zwiększenia efektywności udzielanych świadczeń”.

Drugim rozwiązaniem jest **Domowa Opieka Medyczna**, czyli zdalny monitoring stanu zdrowia pacjentów. W pierwszej kolejności DOM obejmie pacjentów diabetologicznych oraz ze współistniejącymi chorobami kardiologicznymi. Zbierane zdalnie dane będą na bieżąco przekazywane lekarzom, co pozwoli na szybką identyfikację problemów zdrowotnych u pacjentów z grup ryzyka, ograniczając ryzyko powikłań.

Kolejny element to **Hurtownia Danych e-Zdrowia** – system teleinformatyczny służący do analiz danych przetwarzanych w systemie informacji medycznej (SIM) oraz identyfikacji potrzeb zdrowotnych populacji. Hurtownia ma korzystać z danych z SIM, systemów dziedzinowych i rejestrów medycznych. Dane będą poddawane pseudonimizacji, czyli zastąpieniu identyfikatorów, takich jak PESEL, stałym pseudonimem

» Każda placówka medyczna będzie miała dostęp do Skróconej Karty Zdrowia Pacjenta. «

pozwalającym łączyć zdarzenia medyczne tej samej osoby bez ujawniania jej tożsamości. Hurtownia Danych e-Zdrowia jest przymiarką do wtórnego gromadzenia i przetwarzania danych medycznych w celu przyspieszenia badań naukowych nad nowymi lekami albo tworzenia innowacyjnych rozwiązań opartych na AI (trenowanie algorytmów), czyli do realizacji przepisów wynikających z Europejskiej Przestrzeni Danych dotyczących Zdrowia (EHDS).

Ustawa wprowadza również nowy typ dokumentu – Skróconą Kartę Zdrowia Pacjenta. To także element EHDS. Będzie ona zawierać kluczowe dla kontynuacji leczenia informacje, takie jak choroby przewlekłe, alergie, zrealizowane usługi medyczne czy wszczepione implanty. Dostępna z pozycji systemu gabinetowego karta pozwoli lekarzom zapoznać się z danymi zarówno pacjentów zza granicy, jak i wszystkich obywateli kraju.

Dużą zmianą jest możliwość składania przez pacjentów lub ich przedstawicieli ustawowych **zamówień na e-recepty** w ramach kontynuacji leczenia za pośrednictwem Internetowego Konta Pacjenta (IKP).

Projekt reguluje **generowanie zindywidualizowanych analiz i raportów medycznych** na podstawie danych zgromadzonych w systemie P1. Takie raporty będą mogły być wykorzystywane przez lekarzy POZ w ramach koordynacji opieki, przy orzekaniu o stanie zdrowia oraz ordynacji leków.

Dużą nowością jest **integracja notatek pacjentów**. Każdy będzie mógł wprowadzać do systemu e-zdrowia informacje o swoim stanie zdrowia, w tym dane z urządzeń elektronicznych monitorujących parametry zdrowotne, aktywność fizyczną czy styl życia. Będą one odpowiednio oznaczone, tak aby lekarz mógł zdecydować o ich wykorzystaniu w diagnostyce i leczeniu.

Ustawa upraszcza proces digitalizacji dokumentacji medycznej. Zamiast kwalifikowanego podpisu pracownika będzie można używać **pieczęci elektronicznej podmiotu leczniczego**.

»Centrum e-Zdrowia udostępni bezpłatne narzędzie do digitalizacji dokumentacji medycznej.«

Dodatkowo Centrum e-Zdrowia udostępni **bezpłatne narzędzie do digitalizacji dokumentacji medycznej**, które ma umożliwić podmiotom leczniczym przekształcanie dokumentów papierowych do postaci elektronicznej zgodnej ze standardami systemu P1. Rozwiązanie będzie oferowane centralnie, bez opłat licencyjnych. Zeskanowane dokumenty będą automatycznie wiązane z danymi w EDM.

Po co nowe przepisy?

Do ustawy MZ dołączyło obszerne uzasadnienie. Nowe systemy e-zdrowia mają zwiększyć efektywność sektora zdrowia i optymalizować proces udzielania świadczeń. Lepszy dostęp do danych, możliwość szybkich e-konsyliów i zdalnego monitorowania mają skrócić ścieżkę diagnostyczną i poprawić ciągłość leczenia.

Drugim argumentem jest koordynacja opieki. Proponowane rozwiązania umożliwią lekarzom dostęp do danych medycznych pacjenta oraz rozszerzą katalog podmiotów uprawnionych do wglądu do danych o osoby wykonujące czynności pomocnicze w POZ, opiece kardiologicznej czy onkologicznej.

Ustawa za jednym zamachem ma też umożliwić wdrożenie rozwiązań wynikających z EHDS, czyli Europejskiej Przeniesienia Danych dotyczących Zdrowia, w tym transgraniczną wymianę danych w Unii Europejskiej. Centrum e-Zdrowia będzie pełniło rolę Krajowego Punktu Kontaktowego, odpowiedzialnego za wdrażanie Skróconej Karty Zdrowia Pacjenta i e-recept w ramach infrastruktury MyHealth@EU.

MZ zapewnia, że przepisy mają zmniejszyć obciążenia administracyjne placówek zdrowia i lekarzy dzięki uproszczeniu digitalizacji dokumentacji, wstępnym analizom danych oraz zamówieniom na recepty składanym online. Ustawa jest niezbędna, aby zrealizować kamień milowy D6G w ramach KPO, który zakłada wejście w życie aktu prawnego umożliwiającego świadczenie usług e-zdrowia w szerszym zakresie.

Kolejne wielkie inwestycje w e-zdrowie

Wprowadzenie ustawy będzie miało wpływ na funkcjonowanie ok. 27 tys. podmiotów wykonujących działalność leczniczą. Za budowę i utrzymanie nowych systemów (e-Konsylium, Systemu Domowej Opieki Medycznej, Hurtowni Danych e-Zdrowia oraz rozwój funkcjonalności P1) odpowiedzialne będzie MZ.

Plany cyfryzacji nie wiążą się z kosztami po stronie placówek, a nawet mają obniżyć koszty digitalizacji m.in. dzięki możliwości stosowania pieczęci elektronicznej zamiast kwalifikowanego podpisu elektronicznego.

Z perspektywy systemu zdrowia inwestycje mają doprowadzić do integracji informacji z różnych części systemu e-zdrowia, wsparcia procesów diagnostycznych, umożliwiając prowadzenie analiz populacyjnych na podstawie danych z Hurtowni Danych e-Zdrowia. Największą zmianą dla pa-

Koszty i terminy realizacji inwestycji e-zdrowia wprowadzanych nową ustawą

Inwestycja e-zdrowia	Koszty ogólne (zł)	Przedział czasowy realizacji
System e-Konsylium	83 451 272 zł wydatki bieżące + 44 557 190 zł koszty osobowe	2025–2035
Krajowa i transgraniczna skrócona karta zdrowia pacjenta (Patient Summary)	75 697 675 zł + 7 567 371 zł koszty osobowe w MZ	2025–2035 (etaty od 2026 r.)
Centrum Cyfryzacji Dokumentacji Medycznej – Centralne Repozytorium Danych Medycznych	27 857 136 zł wydatki bieżące + 27 424 102 zł wydatki majątkowe	2025–2035
Cyfryzacja 9 nowych rodzajów EDM	57 653 205 zł	2025–2035
Hurtownia Danych e-Zdrowia	783 438 249 zł (w tym 440 310 371 zł wydatki majątkowe)	2025–2035
e-Profil Pacjenta	75 697 675 zł + 15 178 511 zł koszty osobowe	2025–2035 (budowa do poł. 2026 r. z KPO)
Platforma usług diagnostyki cyfrowej (AI/ML)	185 868 451 zł wydatki bieżące + 106 104 052 zł wydatki majątkowe	2025–2035

Kwoty w dokumencie podlegają indeksacji zgodnie z wytycznymi Ministerstwa Finansów (CPI i dynamika wynagrodzeń).

cientów będzie możliwość zlecenia e-recept na kontynuację leczenia przez IKP. Nowością jest uwzględnienie w dokumentacji notatek pacjenta, np. pomiarów ciśnienia tętniczego, tętna, masy ciała, poziomu glukozy czy aktywności fizycznej. Informacje te mają być „powiązane z państwową infrastrukturą e-zdrowia”.

Część z inwestycji już jest realizowana, jak przykładowo Skrócona Karta Zdrowia Pacjenta oraz Domowa Opieka Medyczna. Finansowanie z KPO obejmuje tylko okres do 30 czerwca br. – po tym terminie wszystkie wydatki będą po stronie budżetu państwa. ●

reklama

RAPORT SPECJALNY



CYFROWA PLACÓWKA ZDROWIA

Poradnik płynnego
wdrażania innowacji
e-zdrowia i zarządzania
cyfrową zmianą.





Czy Twój system IT będzie działał po marcu 2029 roku?

Zgodnie z regulacją EHDS Unii Europejskiej, każde oprogramowanie do prowadzenia elektronicznej dokumentacji medycznej będzie musiało posiadać znak CE. A to wysiłek biurokratyczny, którego mniejsze firmy IT albo podmioty medyczne korzystające z autorskiego systemu mogą nie udźwignąć.

EHDS już weszła w życie, zegar tyka

Regulacja dotycząca Europejskiej Przestrzeni Danych Zdrowotnych (European Health Data Space, EHDS) weszła w życie 26 marca 2025 roku. Jest to regulacja i w przeciwieństwie do dyrektyw UE nie wymaga implementacji prawem krajowym, a więc obowiązuje automatycznie we wszystkich krajach członkowskich.

W skrócie, EHDS ma umożliwić wymianę danych medycznych pomiędzy krajami członkowskimi UE. Po stronie podmiotów zdrowia pojawi się nowość – tzw. Podsumowanie Pacjenta (Patient Summary) nazywane też Skróconą Kartą Zdrowia Pacjenta. Karta będzie zawierała najważniejsze informacje medyczne każdego obywatela UE: grupa krwi, przyjmowane leki, alergie, rozpoznania, przebyte procedury medyczne, urządzenia medyczne. Dzięki temu, lekarz w Hiszpanii przyjmujący Polaka przebywającego na wakacjach będzie mógł sprawdzić dane w Skróconej Karcie Zdrowia Pacjenta (SKZP), aby prawidłowo zdiagnozować pacjenta i zalecić bezpieczne leczenie.

Aby dane mogły być wymieniane w granicach UE, systemy elektronicznej dokumentacji medycznej (EDM) – i to wszystkie, bez wyjątku – muszą spełniać określone wymagania interoperacyjności. Tylko w ten sposób dane w SKZP będą pełne, a obraz zdrowia pacjenta – kompletny.

System EDM, czyli każdy system gabinetowy

Rozporządzenie w sprawie EHDS (art. 2 ust. 2 lit. k) definiuje system elektronicznej dokumentacji medycznej (EDM) jako „każdy system, w którym urządzenie lub oprogramowanie umożliwia przechowywanie, pośredniczenie, eksportowanie, importowanie, konwertowanie, edytowanie lub przeglądanie osobistych elektronicznych danych dotyczących zdrowia”. Są to np. systemy, które umożliwiają wystawienie e-recept, rejestrację wyników badań medycznych oraz danych dotyczących zdrowia, generujące wypisy. Systemy, które służą tylko do umawiania wizyt (e-terminarze), nie są systemami EDM.

Regulacja EHDS jasno mówi, że nie ma znaczenia, kto taki system stworzył. Zgodnie z rozporządzeniem (UE) 2019/1020, producentem systemu EDM jest „każda osoba fizyczna lub prawna, która wytwarza produkt lub zleca jego zaprojektowanie lub wytworzenie i wprowadza ten produkt do obrotu pod własną nazwą lub znakiem towarowym”.

A to oznacza, że jeśli podmiot medyczny zlecił stworzenie systemu IT informatykowi, a system jest użytkowany pod marką podmiotu, to ten sam podmiot jest jego producentem.

Dostosowanie do europejskiego formatu danych i znak CE

Każdy producent systemów EDM stosowanych w Europie będzie musiał spełnić kilka wymagań. Pierwszym z nich jest dostosowanie systemu do europejskiego formatu wymiany elektronicznej dokumentacji medycznej (EEHRxF). Umożliwia on bezpieczną transmisję danych z EDM między różnymi aplikacjami, urządzeniami i podmiotami świadczącymi usługi opieki zdrowotnej.

Systemy EDM będą musiały zawierać zharmonizowane komponenty w ramach EEHRxF już od marca 2029 roku dla pierwszej grupy danych (e-recepty, e-skierowanie i dane w Patient Summary). Od marca 2031 roku harmonizacja obejmie zdjęcia medyczne, wyniki badań laboratoryjnych, wypisy ze szpitala. Wspomniane komponenty interoperacyjności zapewniają możliwość importowania/eksportowania danych w formacie EEHRxF oraz generowania dzienników dostępu do danych. W praktyce, producenci IT będą musieli wdrożyć i przetestować obydwa komponenty, a wyniki testów opublikować w dokumentacji technicznej.

» Każdy system IT będzie musiał być zgodny z europejskim formatem wymiany danych EEHRxF. «

Dopiero wówczas system EDM będzie mógł być używany po marcu 2029 roku. Oprócz tego, EHDS zwraca uwagę, że systemy EDM muszą działać zgodnie z przeznaczeniem i zapewniać bezpieczeństwo danych oraz posiadać mechanizmy identyfikacji i uwierzytelniania pracowników służby zdrowia. Producent musi sporządzić dokumentację techniczną systemu EDM przed jego wprowadzeniem do obrotu, a następnie ją aktualizować. Każdy system musi mieć bezpłatną instrukcję obsługi.

Największą zmianą jest jednak konieczność sporządzenia deklaracji zgodności UE z oznakowaniem CE stosowanym dotychczas dla produktów medycznych. Tylko systemy spełniające powyższe kryteria będą mogły być zarejestrowane w unijnej bazie danych systemów EDM. W przeciwnym razie, producent będzie miał obowiązek wycofania z obrotu niezgodnego z przepisami systemu EDM oraz podjęcia działań naprawczych.

Dużo zmian i pracy papierkowej, nie każdy mały system będzie gotowy

Systemy EDM zgodne z EHDS będą musiały być oznaczone znakiem CE, tak samo jak inne urządzenia medyczne. Chodzi o klasę „niskiego ryzyka”, w przypadku której proces certyfikacji wymaga jedynie deklaracji zgodności (*Declaration of Conformity*). Czołowi dostawcy IT dla ochrony zdrowia w Polsce już się przygotowują do nowych wymagań EHDS i nie powinni mieć z tym większego problemu.

Martwić mogą się placówki mające systemy tworzone przez informatyków, posiadające autorskie oprogramowanie albo aplikacje małych firm. Samo dostosowanie do formatu

» Podmiotom zdrowia, które mają system EDM domowej roboty, bardziej opłacalne będzie przejście na oprogramowanie dużego dostawcy. «

EEHRxF wymaga czasochłonnych zmian w architekturze IT. Do tego jeszcze dochodzi przygotowanie dokumentacji. To zadanie można zlecić specjalizującym się w uzyskiwaniu znaku CE firmom, za co trzeba jednak zapłacić od kilkuset do kilku tysięcy złotych.

Podmioty zdrowia, które mają domowej roboty systemy IT, powinny już teraz pomyśleć, czy są w stanie spełnić wymagania EHDS i czy nie lepiej – i taniej w perspektywie długoterminowej – po prostu przejść na system większych dostawców IT. Argumentem jest nie tylko EHDS, ale też rosnąca presja interoperacyjności i integracji z krajowymi systemami e-zdrowia.

Komisja Europejska przekonuje, że w efekcie podmioty zdrowia skorzystają na zmianie, bo zyskają pewność, że wdrażane oprogramowanie spełnia aktualne wymagania. Standaryzacja EDM ma też minimalizować uzależnienie od jednego dostawcy, bo każdy system EDM ze znakiem CE będzie spełniać określone standardy jakości. ●

reklama

CZASOPISMO O CYFRYZACJI OCHRONY ZDROWIA
OSOZ
 ISSN 1897-5838
 01.05.2022 PL
RAPORT SPECJALNY
CYBER OCHRONA
 Poradnik bezpieczeństwa danych dla podmiotów leczniczych.
 Nowe metody hakowania
 Phishing i ransomware
 Cyberpsychologia
 Powtórka z RODO
 Chinna data
 Onboarding IT
 Insider threats
 Fake newsy
 129 STRON
 z wytycznymi dla
 małych i dużych
 podmiotów
 +
 AKTUALNE
 ZALECENIA
 CSIRT CoZ

PORADNIK BEZPIECZEŃSTWA DANYCH W PLACÓWKACH ZDROWIA

129 STRON
Z NOWYMI
WYTYCZNYMI



↓ **POBIERZ ZA DARMO**



Reklamy podczas Super Bowl 2026 mówią wszystko o trendach zdrowia 2026

Super Bowl to najważniejsze wydarzenie sportowe w Stanach Zjednoczonych. Ale uwagę przyciągają przede wszystkim reklamy walczące o uwagę ponad 120 mln widzów. W tym roku tematem nr 1 było zdrowie w niekonwencjonalnej odsłonie.

Za 30-sekundowy spot w przerwie Super Bowl trzeba zapłacić 8 mln dolarów (ok. 30 mln zł). Nic dziwnego, że mogą sobie na to pozwolić tylko duże koncerny międzynarodowe, które chcą

zamanifestować swoją siłę rynkową. Tak jak nigdy wcześniej, w tegorocznym bloku reklamowym pojawiły się reklamy odzwierciedlające obecne trendy zdrowia konsumenckiego. Wśród nich m.in. środki stosowane w leczeniu otyłości, kontrowersyjna platforma longevity czy badania przesiewowe w kierunku raka.

Gwiazda sportu poleca GLP-1

Ofensywę promocyjną przeprowadziły firmy oferujące leki z grupy GLP-1, stosowane w leczeniu cukrzycy typu 2 i otyłości. Serena Williams – światowej sławy tenisistka – promowała telemedyczną platformę Ro, która wspomaga redukcję masy ciała i poprawę parametrów sercowo-naczyniowych z pomocą GLP-1. „Straciłam 15 kg, czuję się lepiej, poruszam się lepiej” – przekonywała Williams. Z kolei Novo Nordisk reklamował doustną wersję semaglutynu (Wegovy). „Gdyby była tabletką pomagająca mi parkować samochód, zażyłbym ją. Gdyby była tabletką pomagająca uratować więcej kotów, zażyłabym ją. Gdyby była tabletką powodującą, że ludzie przestaliby dawać dobre rady, jak zgubić zbędne kilogramy, zażyłabym ją” – przekonywali w oryginalny sposób aktorzy.

Ekspertcy zwracają uwagę, że przekaz reklamowy jest zbyt uproszczony. Leki GLP-1 faktycznie ułatwiają leczenie

 Serena Williams w reklamie leków z grupy GLP-1.

Kliknij tutaj,
aby zobaczyć
reklamę



»Leki GLP-1 ułatwiają leczenie otyłości, ale nie są magiczną pigułką.«



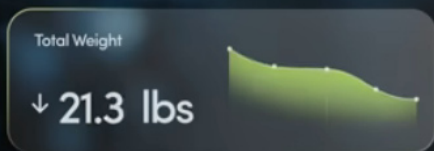
Platforma longevity z dostępem do nowych metod leczenia i diagnostyki, takich jak leki GLP-1 i badania krwi Galleri.

Kliknij tutaj,
aby zobaczyć
reklamę

otyłości, ale nie są „magiczną pigułką”. Wymagają długotrwałego stosowania, mogą powodować działania niepożądane, a bez odpowiedniej diety i aktywności fizycznej wiążą się z ryzykiem utraty masy mięśniowej. Obecność reklam GLP-1 w najdroższym czasie antenowym świata świadczy o tym, jak rynek jest gorący – w 2025 roku jego wartość oceniano na ok. 70 mld USD, a do 2030 r. wzrośnie nawet do 250 mld USD. Rosnące zainteresowanie lekami stosowanymi w leczeniu otyłości i cukrzycy widoczne jest też w Polsce. Według danych OSOZ, w 2025 r. Tirzepatyd, dostępny pod nazwą handlową Mounjaro, osiągnął rekordowy poziom sprzedaży o wartości 1,6 mld zł. Z kolei sprzedaż semaglutydu – substancji wykorzystywanej w terapii cukrzycy i otyłości, obecnej m.in. w leku Ozempic – wzrosła do 1,4 mld zł.

Obietnica długowieczności dla wszystkich

Jedną z najszerzej dyskutowanych reklam był spot firmy Hims & Hers, promujący ideę „longevity”, czyli długowieczności. Spot zaczął się od tezy, że bogaci żyją dłużej, ponieważ mają dostęp do najnowszych terapii, badań i specjalistów. A to kosztuje – guru trendu longevity wydaje 2 mln dolarów



↑↓ Timeline

12 weeks

🏃 Movement

4x / week



Daily Nutrition Plan		
Protein	Fats	Carbs
115 g	57 g	155 g

rocznie na m.in. zażywane codziennie 50 suplementów diety i specjalistyczne badania screeningowe.

Ale teraz longevity ma być dostępne dla wszystkich dzięki platformie Hims & Hers oferującej dostęp do lekarzy oraz nowoczesnych metod – od leków GLP-1 i terapii hormonalnych po zaawansowaną diagnostykę laboratoryjną.

Najwięcej kontrowersji wzbudziło wspomnienie w reklamie testu krwi Galleri, który w USA często się wykonuje w celu wczesnego diagnozowania wielu rodzajów nowotworów naraz. Choć idea diagnozy raka na podstawie badania krwi brzmi obiecująco, eksperci podkreślają, że test ten nie jest obecnie zatwierdzony przez amerykańską FDA jako standardowe narzędzie przesiewowe. Jego czułość – szczególnie w wykrywaniu nowotworów we wczesnym stadium – jest ograniczona, a wyniki mogą prowadzić zarówno do fałszywie dodatnich, jak i fałszywie ujemnych rozpoznań. Lekarze ostrzegają, że badanie nie powinno zastępować sprawdzonych programów screeningowych, takich jak mammografia, kolonoskopia czy oznaczenie PSA.

Reklama Hims & Hers to wierzchołek góry lodowej trendu długowieczności. Usługi i produkty longevity nie są refundowane przez płatników i tworzą nowy komercyjny rynek zdrowia *premium*, obiecując dłuższe życie w zdrowiu. Można mieć wrażenie, że to próba sprzedaży profilaktyki pod bardziej atrakcyjnym szyldem.

Firmy farmaceutyczne zachęcają do badań profilaktycznych

Novartis promował oznaczenie PSA jako prosty test krwi pozwalający na wczesne wykrycie raka prostaty. W spocie podkreślano, że 1 na 8 mężczyzn zachoruje na ten nowotwór, a szybka diagnoza zwiększa szanse na skuteczne leczenie.

Boehringer Ingelheim zaangażował dwie światowej sławy aktorki – Sofię Vergara i Octavię Spencer – aby zachęcić do wykonywania badania uACR (stosunek albuminy do kreatyniny w moczu), pełniącego rolę screeningu w kierunku

»Najwięcej kontrowersji wzbudziło wspomnienie w reklamie testu krwi Galleri.«



🌀 Misja profilaktyka, czyli promocja badania uACR u osób z cukrzycą lub nadciśnieniem.

Kliknij tutaj,
aby zobaczyć
reklamę

przewlekłej choroby nerek. Nefrologi podkreślają, że to proste i tanie badanie może pomóc wcześniej wykryć powikłania u osób z cukrzycą i nadciśnieniem. Reklamy podczas Super Bowl konkurują też kreatywnością, dlatego Boehringer Ingelheim postawił na scenariusz jak z filmu kryminalnego, gdzie dwie agentki udają się w tajną misję wykrycia powikłań.

Tradycyjny przekaz zdrowotny z nowymi akcentami

Nie zabrakło też kampanii prowadzonych przez instytucje publiczne. Najwięcej uwagi przyciągnęła ta finansowana przez MAHA Center (Make America Healthy Again), powiązane ze środowiskiem amerykańskiego ministra zdrowia Roberta F. Kennedy'ego. W prostym spocie Mike Tyson przekonywał, że wysoko przetworzona żywność zabija i zachęcał do spożywania „prawdziwego jedzenia”.



🔊 Płatki śniadaniowe z błonnikiem wpisują się w nowy trend żywieniowy „fiber-maxxing”.

Kliknij tutaj,
aby zobaczyć
reklamę

Z kolei reklama z udziałem 94-letniego Williama Shatnera (polskiej publiczności znany z roli kapitana Jamesa T. Kirka w serialu Star Trek) promowała płatki śniadaniowe Kellogg jako odpowiedź na niewystarczające spożycie błonnika. Spot wykorzystuje świadomie trend „fibermaxxing”, czyli diety superbogatej w błonnik. Dietetycy przypominają jednak, że wzbogacanie produktów w błonnik nie czyni z nich automatycznie zdrowych produktów.

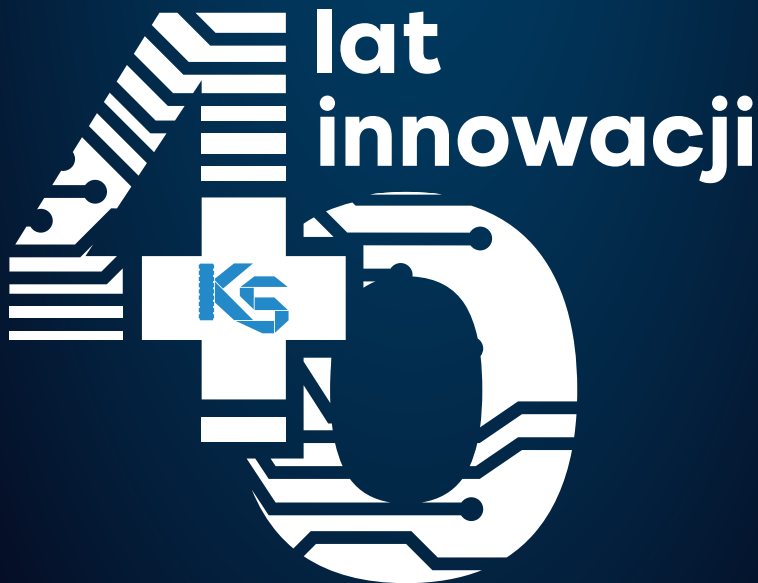
Nowoczesna medycyna w wersji premium

Super Bowl pokazuje, jak nowe leki i technologie napędzają rozwój sektora zdrowia konsumenckiego. Platformy longevity połączone z lekami GLP-1 sprzedają obietnicę zdrowia w nowoczesnym wydaniu. Długowieczność, z niszowego trendu staje się powoli dominującym elementem stylu życia. Socjo-

logowie podkreślają, że w czasach zawirowań politycznych i gospodarczych ludzie szukają bezpieczeństwa, a rozwiązania obiecujące odzyskanie kontroli nad zdrowiem im to oferują.

Istnieje jednak ryzyko, że przepaść pomiędzy osobami w gorszej sytuacji ekonomicznej, skazanymi na publiczny, niewydolny system zdrowia, a prywatnym sektorem oferującym najnowocześniejsze testy, skanowanie całego ciała i profilaktykę za spore pieniądze będzie się powiększała. ●

reklama



KAMSOFT

Doświadczenie. Zastosowane.



Badanie: Nowy zegarek Apple ostrzega o nadciśnieniu. Ale nie wszystkich

W zeszłym roku Apple wprowadził do swoich smartwatchów funkcję informującą użytkownika, że może mieć nadciśnienie. Naukowcy sprawdzili, czy rzeczywiście pozwala lepiej diagnozować chorobę.

Jak smartwatch wykrywa nadciśnienie?

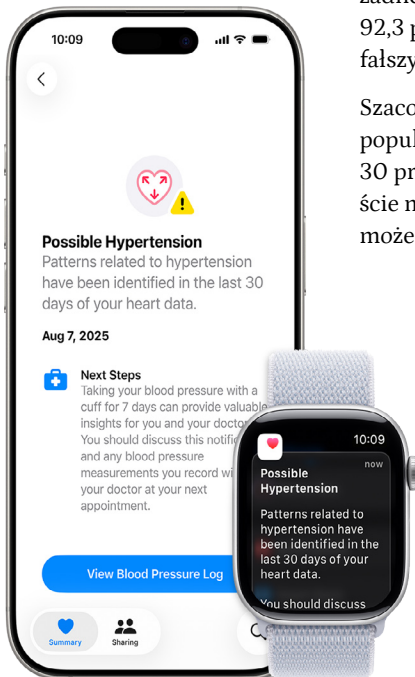
Mowa o funkcji w nowym zegarku Apple, którą we wrześniu 2025 r. Amerykańska Agencja Leków i Żywności (FDA) dopuściła na rynek. Jest to tym samym urządzenie medyczne, ale na razie dostępne tylko w USA.

Sam zegarek nie mierzy ciśnienia, jak robią to znane urządzenia z rękawami, ale wykorzystuje sygnały fotopletyzmoграфiczne do oceny ryzyka (diody i czujniki umieszczone w dolnej pokrywie zegarka). Zbierane przez 30 dni dane analizuje algorytm AI i na tej podstawie wydaje ostrzeżenia. Funkcja nie diagnozuje choroby, ale – jak podkreśla Apple – ma skłonić użytkowników do konsultacji medycznej.

41,2 proc. z nadciśnieniem otrzymało alert

Nowe badanie opublikowane na łamach JAMA przygląda się temu, jak funkcja powiadomień o nadciśnieniu w Apple Watch wpływa na wykrywalność nadciśnienia. W grupie osób z nierozpoznanym nadciśnieniem 41,2 proc. otrzymało alert sugerujący możliwe nadciśnienie, a 58,8 proc. nie otrzymało żadnego powiadomienia. Z kolei wśród osób bez nadciśnienia 92,3 proc. nie dostało alertu, natomiast 7,7 proc. otrzymało fałszywie dodatnie powiadomienie.

Szacowana częstość nierozpoznanego nadciśnienia w całej populacji kwalifikującej się do użycia funkcji wyniosła 30 proc. Oznacza to, że około 7 na 10 osób z alertem rzeczywiście ma nadciśnienie, ale jednocześnie 1 na 5 osób bez alertu może chorować.



Po otrzymaniu alertu o możliwym nadciśnieniu, należy przez 7 dni mierzyć ciśnienie tradycyjnym ciśnieniomierzem, aby zwalidować wynik (zdjęcie: Apple)

Wpływ funkcji znacząco różni się w zależności od wieku: im starszy użytkownik zegarka, tym większe prawdopodobieństwo, że alert faktycznie wykrywa nadciśnienie. Korelacja nie jest jednak zaskakująca, bo wraz z wiekiem rośnie ryzyko choroby. Podobna zależność dotyczy także wskaźnika masy ciała (BMI) oraz płci (nadciśnienie częściej występuje u mężczyzn niż u kobiet).

Apple Watch mało precyzyjny, ale nadal skuteczny

Z jednej strony ponad 40% osób z nierozpoznanym nadciśnieniem otrzymuje ostrzeżenie, dowiaduje się o chorobie, co motywuje do dalszej diagnostyki. Z drugiej, jeszcze większa grupa (prawie 60%) nie otrzyma żadnego alertu, mimo występowania choroby. A to daje fałszywe poczucie bezpieczeństwa – pacjent nie mierzy ciśnienia, bo wychodzi z założenia, że robi to zegarek Apple. W takim przypadku może nawet nie skontaktować się z lekarzem w przypadku niepokojących objawów. Badanie jednak nie pokazuje tego, ile osób z alertem faktycznie zgłosiło się do lekarza, a ile bez alertu, ale chorych, zaniechało dalszej diagnostyki. Nie wiemy też, czy brak alertu cokolwiek zmienia w sytuacji osób chorych, ale nieświadomych.

Apple Watch rzadko kiedy wprowadza w błąd osoby, które są zdrowe. 92,3 proc. bez nadciśnienia nie otrzymało alertu, a więc zegarek przeprowadził prawidłową ocenę. Tylko 7,7% otrzymało nieprawidłowe wskazanie.

W Polsce na nadciśnienie choruje ok. 11–12 mln osób, ale większość nawet o tym nie wie. Zegarek mógłby uzupełnić programy screeningowe w kierunku występowania hipertensji. Jak podkreślają autorzy, zegarek już teraz ratuje życie. Potencjał jest ogromny – gdyby zwiększyć dokładność technologii bezmankietowych pomiaru ciśnienia i zintegrować dane z zegarków z elektroniczną dokumentacją medyczną, wykrywalność nadciśnienia znacznie by się poprawiła. ●

» Apple Watch może czasami usypiać czujność osób, które są chore. «



Agenci AI, robotyka, longevity, zdrowotni influencerzy. System zdrowia czeka na wstrząsy transformacyjne

Żaden rok nie rozpoczął się tak burzliwie jak 2026. Premiera ChatGPT Health zwiastuje erę agentów zdrowia mających dostęp do dokumentacji medycznej i wiedzących o zwyczajach i zdrowiu pacjenta więcej niż lekarz. A w Polsce wdrażane są narzędzia e-zdrowia, które odwracają piramidę świadczeń już nie ze szpitali do POZ i AOS, ale z POZ i AOS do IKP.

Nowy system zdrowia

To, że ochrona zdrowia jest w kryzysie, wiemy od dawna. Prawie każdy szpital ma problem ze znalezieniem personelu medycznego. Do budżetu NFZ trzeba dosypywać pieniędzy – deficyt NFZ na 2026 rok szacowany jest na 23–26 mld zł. Według CBOS-u, 70% Polaków źle ocenia system zdrowia.

W gospodarce rynkowej, każde niezadowolenie to nisza rynkowa, którą zagospodarowują inne firmy. I dzieje się to także w mocno regulowanej ochronie zdrowia. Liczba prywatnych polis zdrowotnych w Polsce wzrosła w 2024 roku o 12,2% do 5,39 mln. I będzie dalej rosnać, bo rosną oczekiwania pacjentów, którzy nie chcą już czekać w długich kolejkach.

Nic dziwnego, że obok systemu zdrowia, który znamy od lat, rośnie nowy, alternatywny. Nie byłby możliwy bez cyfryzacji, sztucznej inteligencji oraz smartfonów.

Przepaść pomiędzy wizytą na NFZ a tym co w smartfonie

Polski rynek zdrowia – choć rządzi się swoimi prawami i ma swoje problemy – nie działa w bańce. Jest podatny na trendy społeczne, technologiczne i sytuację geopolityczną. We wszystkich trzech obszarach weszliśmy w 2026 roku z zapowiedzią dużych zmian.

Amerykańska FDA dopuściła już ponad 1250 urządzeń medycznych opartych na AI i uczeniu maszynowym. Ich liczba rośnie rok do roku. Na świecie dostępnych jest ponad dwa miliony wyrobów medycznych, z czego około 25 procent to urządzenia cyfrowe. Trend rosnący.

Na targach CES 2026 dominowały humanoidalne roboty napędzane AI, a firmy technologiczne zapowiadają coraz śmielsze projekty. OpenAI ogłosiło ChatGPT Health, czyli nową opcję umożliwiającą integrację generatywnej AI z elektroniczną dokumentacją medyczną. Firma pracuje też nad tajemniczym nowym urządzeniem, które ułatwi komunikację z agentami AI (premiera zapowiadana jest na 2026/2027 rok). Ci będą

podpowiadać, jak się odżywiać, motywować do sportu, układać zdrowy plan dnia.

Ministerstwo Zdrowia, placówki zdrowia i lekarze tracą monopol na profilaktykę – dostarczać ją będą w sposób ultra-personalizowany firmy nowych technologii, najczęściej z USA. Nowi neo-dostawcy e-usług z zakresu dobrego samopoczucia i zdrowia rozbudzają apetyty. Oczekujemy takiej samej szybkości i doskonałości obsługi od sektora publicznego. A to wróży tylko jedno: dalej rosnące niezadowolenie pacjentów z publicznego systemu zdrowia.

MZ próbuje nadążyć za rewolucją technologiczną, oferując nowe cyfrowe rozwiązania, od IKP po Centralną e-Rejestrację. Robi to dobrze, ale nie jest w stanie dotrzymywać kroku rozwojowi AI w sytuacji, gdy sektorem zdrowia rządzą stare reguły, w tym system refundacji oparty na klasycznych usługach zdrowotnych i konserwatywne regulacje.

Test robotów w fabryce (kadr z filmu chińskiej firmy UBTECH).
W 2026 roku pierwsi humanoidalni pomocnicy wejdą do domów.



Kryzys zaufania do systemu

Można odnieść wrażenie, że nie wszyscy przejmują się transformacyjną siłą AI i nowych technologii. „Pacjentów nie brakuje i brakować nie będzie”, więc po stronie systemu zdrowia nie widać potrzeby wdrażania nowych form opieki.

Ale taki punkt widzenia ignoruje jeden, ważny aspekt, który z każdym rokiem będzie nabierał na znaczeniu: malejące zaufanie pacjentów do podmiotów zdrowia i lekarzy, powstawanie alternatywnego systemu zdrowia z coraz szerszą ofertą nowoczesnych usług oferowanych przez neo-dostawców, redukcja roli podmiotów zdrowia.

Kilka przykładów. Pacjenci już dziś przed wizytą u lekarza pytają ChatGPT o możliwą diagnozę, a po wizycie weryfikują zalecenia. Według danych OpenAI, najczęściej zwracamy się do AI właśnie w sprawach związanych ze zdrowiem (40 mln zapytań dziennie). Kilkanaście procent osób rezygnuje z zaleceń lekarskich na rzecz podpowiedzi AI, ale te statystyki mogą być mocno niedoszacowane.

Równolegle rośnie sektor komercyjnej prewencji, która jest sprzedawana pod atrakcyjniejszą nazwą „longevity” (długowieczność). Mnożą się kliniki oferujące tzw. pełne MRI ciała połączone z rozszerzoną diagnostyką i profilowaniem genetycznym. Podczas jednego z największych światowych wydarzeń rozrywkowych, czyli Super Bowl, po raz pierwszy pojawiła się reklama firmy oferującej cyfrową platformę longevity. Inwestycje w ten sektor sięgają miliardów dolarów i rosną w zawrotnym tempie.

Influencer jak zaufany lekarz, zdrowie w stylu „zrób to sam”

Od czasu pandemii COVID-19 maleje zaufanie do instytucji publicznych, w tym publicznego sektora zdrowia. Piosenka popularnego wśród młodzieży Taco Hemmingwaya, w której pada nazwa leku przeciwbólowego, osiągnęła miliony odsłon na TikToku, wywołując nagły wzrost popytu w aptekach (sprawą zajął się nawet Główny Inspektorat Farmaceutyczny).

» Rośnie sektor komercyjnej prewencji, która jest sprzedawana pod atrakcyjniejszą nazwą „longevity” (długo-wieczność). «

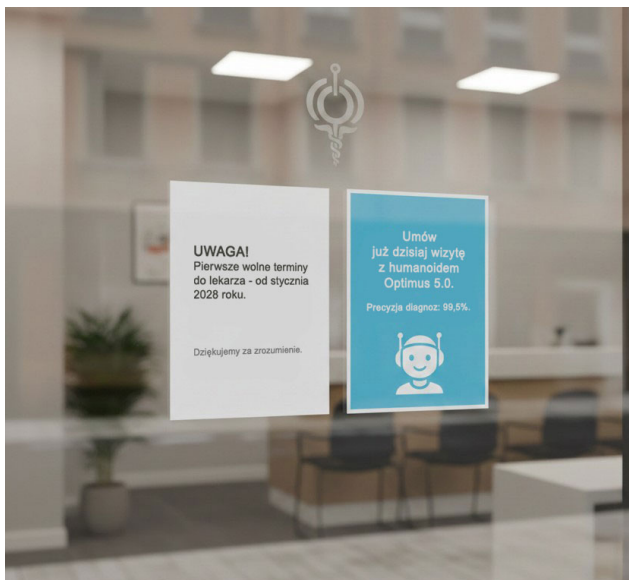
Ale to tylko wierzchołek góry lodowej. W mediach społecznościowych są setki, tysiące pseudo-medycznych influencerów zachwalających cudowne metody leczenia, podważających klasyczną medycynę, sprzedających szybkie i proste recepty na zdrowie i longevity. Wszystko w formie krótkich i przekonujących klipów wideo, często generowanych przez AI, bez żargonu medycznego. I nie ma znaczenia, że według badań nawet 80% postów dotyczących zdrowia psychicznego wprowadza w błąd albo dezinformuje. Młodzi ludzie czerpią wiedzę w nowy sposób – z mediów społecznościowych.

Ten trend wpisuje się w większą tendencję do przesuwania ochrony zdrowia ze szpitali do domów, co akurat jest pożądane przez system zdrowia (koszty) i pacjentów (wygodę), o ile opiera się na sprawdzonych rozwiązaniach. Inteligentne zegarki analizują zmiany w przepływie krwi i wysyłają ostrzeżenia o nadciśnieniu, migotaniu przedsionków, a smart pierścienie informują nawet o zbliżającej się infekcji. Tego typu sugestie kierują zaniepokojonych pacjentów do gabinetów lekarskich i kolejki zamiast się skracać, wydłużają się.

Domowe testy na obecność koronawirusa jeszcze bardziej przyspieszyły ten trend. Dzisiaj można wykonać kombo-testy na grype, pojawiają się nowe urządzenia pozwalające nawet mierzyć poziom hormonów.

Można to nazwać „IKEA-izacją medycyny”. Pacjenci samodzielnie – z pomocą cyfrowych usług i nowych urządzeń zdrowia konsumenckiego, które są „na czasie” – dbają o siebie, własne zdrowie i samopoczucie. Popularność antagonistów GLP-1, które w Polsce biją rekordy sprzedaży, pokazuje, że innowacje przynoszące szybkie efekty dla zdrowia i urody są przyjmowane w społeczeństwie w błyskawicznym tempie.

Za dostępem do informacji idzie też większa świadomość w zakresie zdrowia, choć przyzwyczajenia zmieniają się bardzo powoli. Przykładem jest malejąca konsumpcja alkoholu. W UE spożycie alkoholu na osobę powyżej 15. roku życia zmniejszyło się o 2,9 litra w ciągu ostatnich czterech dekad z 12,7 litra do 9,8 litra w 2020 roku. To samo dotyczy Polski – z 9,73 litra



Kryzys kadr medycznych zmusi do coraz częstszego sięgania do alternatywnych, cyfrowych i czasami autonomicznych metod konsultacji medycznych. Te nie muszą z góry oznaczać „gorszych” usług medycznych, bo precyzja AI rośnie z miesiąca na miesiąc (grafika wygenerowana przez AI).

na mieszkańca w 2021 r. do 8,93 litra w 2023 r. Trend jest widoczny zwłaszcza wśród młodzieży.

Inicjatywa po stronie świadczeniodawców i nowy model refundacji

Wzrost zdrowia konsumenckiego napędzany cyfryzacją jest nie tylko zagrożeniem, ale i szansą dla sektora zdrowia i placówek zdrowia. Pod warunkiem, że legislacja dostosuje się do nowej rzeczywistości, a świadczeniodawcy rozumieją zmieniające się pod wpływem technologii oczekiwania pacjentów.

Tkwimy w systemie zdrowia przeszłości – mówi wprost prof. Katarzyna Kolasa. W koszyku usług gwarantowanych nie ma żadnych terapii cyfrowych, jak przykładowo aplikacji mobilnych dla osób chorych przewlekle. Profilaktyka nie jest refundowana systemowo, a jedynie w ramach programów takich

»Elon Musk: Optimus do 2029 roku prześcignie pod względem umiejętności najlepszych chirurgów.«

jak Moje Zdrowie (wcześniej Profilaktyka 40+). Wprawdzie z KPO duże pieniądze na cyfryzację popłynęły do szpitali, ale nie do POZ. Zasada odwracania piramidy świadczeń, którą od lat promuje MZ, musi uwzględniać świadczenia i nowe formy usług realizowane cyfrowo. Portale pacjenta ze spersonalizowanymi informacjami zdrowotnymi, monitorowanie zdrowia osób z grup ryzyka, wirtualne oddziały szpitalne, aplikacje mobilne jako pierwsza forma kontaktu z systemem zdrowia mogą odciążyć przeciążony system i zwiększyć zaufanie pacjentów do publicznego systemu. A przede wszystkim zmniejszyć przepaść między tym, co oferują firmy nowych technologii, a świadczeniodawcami.

Polska jest społeczeństwem otwartym na nowe technologie. I to powinna wykorzystać ochrona zdrowia. Potrzebujemy nowego prawa regulującego odpowiedzialność za błędy AI, aby lekarze nie bali się sięgać do tego typu rozwiązań. Potrzebujemy nowego systemu oceny medycznych technologii cyfrowych. Systemy elektronicznej dokumentacji medycznej powinny mieć możliwość bezpiecznego pobierania danych z urządzeń pacjenta, jak inteligentnych zegarków albo opasek, aby lekarz – na podstawie analiz AI – mógł lepiej zrozumieć kontekst pacjenta, stając się architektem zdrowia, a nie mechanikiem naprawiającym zepsute części organizmu. Jak na razie jest odwrotnie – to boty AI karmią się danymi z e-kartotek, które pacjenci sami wczytują, szukając desperacko pomocy, której nie znaleźli w oficjalnym systemie zdrowia.

Co tydzień nowe postępy AI

To, że Elon Musk zapowiedział, że jego robot Optimus do 2029 roku prześcignie pod względem umiejętności najlepszych chirurgów, można uznać za kolejny chwyt marketingowy podbijający wartość giełdową Tesli. Faktem jest jednak, że robotyka to najszybciej rozwijająca się obecnie gałąź nowych technologii. Wszystko dzięki postępom AI. Można już zamówić humanoidalne roboty do prostych czynności domowych. Nad nowymi modelami dla gospodarstw domowych pracują giganci technologiczni na całym świecie, jak NVIDIA, Microsoft, Google, Boston Dynamics (należący do Hyundai) itd.

» ChatGPT robi wrażenie, ale to tylko wierzchołek góry lodowej tego, co dzieje się w AI. «

Niektóre z innowacji wejdą do nas łada dzień i to, co było tylko teorią, stanie się częścią codziennego życia. Przykładem są autonomiczne samochody. Waymo, najbardziej popularna sieć taksówek bez kierowców, ma w USA flotę złożoną z 2500 pojazdów. W tym roku planuje ekspansję do Europy, zaczynając od Londynu. Ich rozwój nie byłby możliwy bez AI.

To, jak AI robi szybko postępy, świetnie pokazuje kolejny przykład: w 2023 roku wszyscy śmiali się z filmu przygotowanego przez sztuczną inteligencję i pokazującego aktora Willa Smith'a jedzącego spaghetti. Makaron przenikał przez ręce, twarz była zniekształcona, aktor wyglądał dziwnie i nic do siebie nie pasowało. W 2026 roku AI, dostając podobne zadanie, jest w stanie wygenerować klip wideo, po obejrzeniu którego nie zorientujemy się, że jest to AI.

ChatGPT to tylko wierzchołek góry lodowej tego, co dzieje się w AI. Pojawiają się coraz to nowsze modele, powstają wyspecjalizowani w określonych zadaniach AI agenci. Na rynek wchodzi już nawet tzw. jednoosobowe firmy, gdzie zamiast pracowników są tylko agenci AI.

Postęp jest błyskawiczny i w medycynie wywoła kilka fundamentalnych zmian: przejście od leczenia do profilaktyki, z opieki epizodycznej do ciągłej, z usług świadczonych fizycznie do świadczeń wirtualnych, z opieki w modelu „jedno podejście do wszystkich” do modelu opieki personalizowanej, z płacenia za ilość do płacenia za efekty, z medycyny opartej na doświadczeniu i wiedzy pracowników medycznych do medycyny opartej na wsparciu AI. To będzie długotrwały proces, ale już się rozpoczął i nie ma od niego odwrotu.

Oczywiście ten postęp niesie za sobą też wiele niebezpieczeństw, od tzw. deskillingu personelu (zanikanie umiejętności leczenia bez AI) do utraty prywatności pacjentów po błędy w decyzjach. Ale żadna technologia nie jest idealna, tak samo jak leki nie są idealne i mają skutki uboczne. ●



Dbaj o zdrowie z aplikacją

VisiMed



visimed.osoz.pl





Ochrona danych polega na budowaniu procedur bezpieczeństwa wokół pracownika

– Każdy ma prawo się pomylić i kliknąć w zainfekowany link. Decyduje to, co dzieje się później – mówi Patryk Kuchta, Data Privacy Manager w Medcover. Rozmawiamy o tym, jak stworzyć silny, wielowarstwowy system ochrony przez cyberatakami.

Jakie ataki hakerów najbardziej zagrażają danym medycznym?

Nie zaskoczę, jeśli powiem, że cały czas najbardziej powszechną próbą cyberataku jest stary, dobry, klasyczny phishing. Najpopularniejszy jest phishing mailowy, ale także ten przez komunikatory internetowe, z których pracownicy korzystają czasem prywatnie. Do tego dochodzi jeszcze coraz częściej stosowany phishing głosowy, czyli telefoniczny.

Niestety, jest on coraz bardziej wyrafinowany i przybiera coraz trudniejsze do rozpoznania formy. A wszystko dzięki AI. Do niedawna, pisane przez hakerów i masowo wysyłane wiadomości phishingowe, były stosunkowo łatwe do wykrycia. Zawierały błędy językowe, dziwne czcionki i podejrzane grafiki. Dzisiaj narzędzia oparte na sztucznej inteligencji są w stanie przygotować wiarygodne teksty w każdym języku, podszywające się pod różne instytucje. Trudno je odróżnić od prawdziwych wiadomości.

Drugą podatnością są luki w wykorzystywanym oprogramowaniu. Cyberprzestępcy cały czas monitorują dziury w systemach IT, by z ich pomocą dostać się do infrastruktury IT, zanim jeszcze producent wypuści odpowiednią łatkę, a użytkownik ją zainstaluje. Pomocne w monitorowaniu takich aktywności są narzędzia typu Cyberthreat Intelligence. Jak tylko zauważymy w raportach z monitoringu kampanii hakerskich, że jakiś system IT jest wykorzystywany w atakach, musimy tak szybko jak to możliwe zainstalować łatkę.

Wspomniał Pan o wiadomościach phishingowych, które mogą być trudne do rozpoznania. Nie wszystkie zostaną odsiane jako SPAM. I wtedy ostatnim ogniwem obrony jest personel. I tu kłaniają się regularne szkolenia z cyberbezpieczeństwa.

Proponuję, aby nie nazywać tego szkoleniami, ale kampanią budowania świadomości i edukacją pracowników. Szkolenie

za bardzo kojarzy się z jednorazowym wydarzeniem, czymś co ma początek i koniec. W Medicover podchodzimy do wzmacniania cyberbezpieczeństwa jako do ciągłego procesu.

Oprócz tego, że organizujemy klasyczne szkolenia dla pracowników – wymagane przepisami prawa albo naszymi wewnętrznymi standardami – prowadzimy regularne treningi phishingowe. Korzystamy ze specjalnych platform generujących kontrolowane wiadomości phishingowe. Sprawdzamy reakcje pracowników: nie tylko to, czy klikają w niechciane linki lub załączniki, ale przede wszystkim to, czy zgłaszają phishing. Do tego publikujemy w intranecie aktualne materiały dotyczące bezpieczeństwa danych.

Zgłaszanie zagrożeń jest kluczowe. To, co często obserwujemy w zarządzaniu incydentami cyberbezpieczeństwa, to nie tyle fakt, że użytkownicy dają się złapać na phishing – bo świadomość jest coraz większa – ale to, że ignorują phishing. Dostają wiadomość, rozpoznają, że to phishing i ją kasują. Tymczasem takie wiadomości powinny być zgłaszane, bo dzięki temu wewnętrzny zespół IT jest w stanie skorelować informacje i wykryć, że przykładowo prowadzona jest kampania wymierzona w naszych pracowników. Wtedy możemy podnieść alarm i uruchomić dedykowaną kampanię informacyjną.

Jeśli chodzi o budowanie świadomości i kultury organizacyjnej, edukacja jest kluczowa. Ale nie oszukujmy się: edukacja bez odpowiednich zabezpieczeń technologicznych nie będzie w stanie sprostać współczesnym zagrożeniom. Dlatego konieczne jest budowanie wielowarstwowego ekosystemu bezpieczeństwa zawierającego m.in. zapory sieciowe, kontrolę ruchu w sieci placówki, zaawansowane narzędzia ochrony poczty, ochronę stacji końcowych, systemy klasy EDR (red.: Endpoint Detection and Response, narzędzia do wykrywania i reagowania na podejrzaną aktywność na urządzeniach końcowych). Ochrona cybernetyczna jest ochroną wielowarstwową. Edukacja jest fundamentalna, ale musi być wsparta technologią.

Co zrobić, aby pracownicy nie bali się zgłaszać incydentów, również wtedy, gdy kliknęli w niebezpieczny link i myślą, że to ich wina?

To jest bardzo dobre pytanie i odpowiedź wcale nie jest prosta. Bardzo trudno jest zbudować kulturę organizacyjną w obszarze bezpieczeństwa, w której pracownicy wiedzą, że nawet jeśli kliknęli dziwny link nieumyślnie, to powinni to zgłosić. Oczywiście nie mówimy o sytuacjach, gdy ktoś klika na wiadomość phishing celowo – to zupełnie inny problem.

W ramach prowadzonych kampanii edukacyjnych stosujemy wewnętrzny system walidacji. Każda symulacja phishingu jest podsumowywana, a pracownik dostaje informację zwrotną – jak mu poszło, jak często klikał w wiadomości phishingowe albo czy je zgłaszał, jak radził sobie z quizami dotyczącymi bezpieczeństwa. Oprócz szkoleń prowadzimy regularne krótkie quizy, oparte na bardzo konkretnych sytuacjach związanych z cyberzagrożeniami, z prostymi pytaniami i dwoma wariantami odpowiedzi. Często są one wsparte formą graficzną, np. komiksem, żeby lepiej dotrzeć do pracownika.

Podczas każdego szkolenia jasno podkreślam, że każdy ma prawo się pomylić. Po to zarządzamy ryzykiem. Każdy może mieć swój słabszy dzień albo chwilę nieuwagi. Błąd popełniony nieumyślnie nie jest podstawą do karania pracownika. Wręcz przeciwnie – sytuacje, w których ktoś zgłasza, że zrobił coś nie tak, traktujemy jako zachowanie pożądane. Konsekwencje mogą pojawić się wtedy, gdy ktoś wie, że zrobił coś złe, i świadomie tego nie zgłasza. W takim przypadku dochodzi do złamania procedur.

Rozmawialiśmy o wielowarstwowej ochronie złożonej z zabezpieczeń technicznych i organizacyjnych. Czy cyberbezpieczeństwo w ochronie zdrowia jest drogą?

I tak, i nie. Na pewno jest to koszt – nie da się tego zrobić zupełnie bezkosztowo. Trzeba jednak mierzyć siły na zamiary.

» Chmura może być bardzo opłacalna, także pod względem bezpieczeństwa. «

Jeśli jesteśmy małą, jedno- czy kilkugabinetową placówką, prawdopodobieństwo ukierunkowanego ataku jest dużo mniejsze niż w przypadku dużej grupy kapitałowej działającej w ochronie zdrowia.

Nie każda placówka musi mieć etatowego specjalistę ds. cyberbezpieczeństwa. W mniejszych podmiotach często wystarczy dostęp do eksperta zewnętrznego, z którym można się konsultować. Dużą część bezpieczeństwa można też przenieść na usługodawcę. Coraz więcej usług IT jest świadczonych w modelu usługowym, bez konieczności utrzymywania własnej infrastruktury. Wtedy to dostawca odpowiada za jej zabezpieczenie.

Do tego dochodzi edukacja personelu, śledzenie portali branżowych, komunikatów CSIRT i zapisanie się do sektorewego CSIRT, aby otrzymywać ostrzeżenia o zagrożeniach. To wszystko można zrobić niskim kosztem lub bezkosztowo.

Wspomniał Pan o scedowaniu odpowiedzialności na zewnątrz. Czy dotyczy to też wyboru między serwerem lokalnym a chmurą?

Oczywiście, że tak. Chmura może być bardzo opłacalna, także pod względem bezpieczeństwa. Odpowiedzialności prawnej nie da się przenieść na dostawcę, ale można się nią w dużym stopniu podzielić, jeśli zadamy o odpowiednie umowy, certyfikaty i analizę ryzyka. Dla mniejszych podmiotów chmura bywa bardzo rozsądnym rozwiązaniem.

Parlament i Senat przyjęły już ustawę o Krajowym Systemie Cyberbezpieczeństwa adaptującą dyrektywę NIS2. Prezydent ją podpisał, ale jednocześnie skierował do Trybunału Konstytucyjnego. Czy Medcover już przygotowuje się na obowiązki z niej wynikające?

Nie tylko się przygotowujemy, ale w niektórych podmiotach już wdrożyliśmy wymagania wynikające z NIS2. Proszę pamiętać, że działamy również na rynkach zagranicznych,

jak w Rumunii czy Niemczech, gdzie NIS2 już obowiązuje. Wiemy od dawna, które podmioty w naszej grupie będą objęte nowymi przepisami, a dzięki centralizacji standardów bezpieczeństwa łatwiej jest nam nimi zarządzać. Od 2014 roku funkcjonujemy w oparciu o system zarządzania bezpieczeństwem informacji zgodny z ISO 27001 i te standardy przenosimy na kolejne spółki.

Jak wygląda typowy dzień pracy osoby, która odpowiada za bezpieczeństwo danych?

Bardzo rzadko ma on swój wyraźny początek i koniec. Oczywiście są pewne godziny pracy, w których intensywność i dyspozycyjność są największe, ale cyberprzestępcy nie patrzą ani na zegarek, ani na kalendarz. W sytuacji, w której pojawia się poważny incydent lub naruszenie bezpieczeństwa, inne zadania schodzą na dalszy plan i wszystkie ręce są na pokładzie, żeby zająć się tym, co jest w danym momencie najważniejsze.

Na co dzień odpowiadam również za tzw. governance w obszarze cyberbezpieczeństwa. Sprawdzam, jak wyglądamy pod kątem wskaźników bezpieczeństwa, ponieważ bardzo wiele obszarów monitorujemy na bieżąco. Analizuję, czy w którymś miejscu nie trzeba podjąć dodatkowych działań, z kimś się skontaktować albo zainicjować konkretną akcję.

Regularnie sprawdzam też, jak przebiegają projekty z zakresu cyberbezpieczeństwa, jak wdrażanie nowych standardów, technologii czy rozwiązań. Bardzo często trafiają do nas również umowy, wnioski i projekty do zaopiniowania, więc dużą częścią mojej pracy jest decydowanie i planowanie, w jaki sposób dany projekt lub system wdrożyć tak, aby był bezpieczny i zgodny z obowiązującymi wymaganiami.

Istotnym elementem mojej pracy jest także monitorowanie zmian, w szczególności legislacyjnych. Zajmuję się formalną i prawną stroną bezpieczeństwa informacji, a w ostatnich miesiącach – zwłaszcza na poziomie unijnym – zmian w przepisach jest bardzo dużo. To wymaga stałej uwagi.

Jeśli dzień jest spokojny i nie ma żadnych „pożarów”, staram się wygospodarować czas na przeglądanie komunikatów z instytucji branżowych, portali i źródeł, które subskrybuję, żeby sprawdzić, czy nie pojawiły się nowe zagrożenia, ostrzeżenia albo informacje, które mogłyby wymagać naszej reakcji w Medicover.

Ma Pan jedną główną dewizę dotyczącą cyberbezpieczeństwa?

Tak. Edukacja i budowanie świadomości wśród pracowników. Wierzę, że bezpieczeństwem trzeba pracowników zarazić. Jeśli zrozumieją, że bezpieczeństwo ich chroni, a nie tylko utrudnia pracę, to naturalnie będą je stosować. Chodzi o budowanie kultury bezpieczeństwa wokół pracownika. ●

reklama



SZTUCZNA INTELIGENCJA W OCHRONIE ZDROWIA

242 STRONY
Z PORADAMI
I NOWOŚCIAMI

↓ POBIERZ ZA DARMO



BLOG.OSOZ.PL



Hakerzy nie mają skrupułów, ale może ich zatrzymać „firewall z ludzi”

Naruszenia bezpieczeństwa danych często zaczynają się od chwili słabości, którą każdy doświadcza pod presją czasu albo z poczucia władzy – twierdzi Mark T. Hofmann, profiler kryminalny i wywiadowczy oraz psycholog biznesowy. Jego zdaniem ochrona danych to przede wszystkim wyzwanie psychologiczne.

Jest Pan profilerem kryminalnym zajmującym się cyberprzestępczością. Co to oznacza?

Zaglądam tam, gdzie inni nie zagląдают – do *Darknetu*, forów dla hakerów; analizuję rozmowy na Telegramie albo logi czatów, które wyciekły. Łącząc analizę behawioralną z bezpośrednimi badaniami w Darknecie, badam zachowania hakerów: Kim są? Jak myślą? Co ich motywuje? Jak się organizują? Cel jest zawsze ten sam: uczę się od „złych aktorów”, aby pokazać organizacjom i władzom, jak się chronić.

Na pierwszy rzut oka można pomyśleć, że cyberprzestępczość jest problemem technicznym. Jednak największe znaczenie mają aspekty psychologiczne, zarówno te po stronie ofiar ataków jak i hakerów.

Co powinniśmy wiedzieć o współczesnych hakerach?

Hakerzy są często młodzi, bardzo inteligentni i dobrze wykształceni. Kieruje nimi silna chęć rzucenia wyzwania systemowi. Wielu z nich określiłbym mianem „cyfrowych anarchistów” – lubią grę w kotka i myszkę z władzami i są dumni ze swoich umiejętności. Pieniądze są często tylko jednym z motywatorów; równie ważne są dreszczyk emocji, wyzwanie, chęć rozwiązania „zagadki” i prestiż. Nawet ci hakerzy, którzy już się wzbogacili, kontynuują swoją działalność cyberprzestępczą. Nie chodzi tylko o pieniądze, ale o status, przyciągnięcie uwagi i panowanie nad systemami IT.

Od lat wiemy, jak działa phishing i mimo to dajemy się na niego nabierać. Dlaczego?

Atakujący zawsze wykorzystują te same czynniki wyzwalające: emocje, presję czasu i nietypowe prośby. Najważniejsze są emocje. I ten schemat działania sprawdza się, ponieważ ludzie reagują odruchowo, zanim zaczną myśleć.

Sama świadomość często nie wystarcza, gdy w grę wchodzi stres, rutyna lub zaskoczenie. Nawet doświadczeni eksperci

» Pozostawienie komputera bez nadzoru na kilka minut to jak otwarte drzwi do danych. «

mogą dać się oszukać, zwłaszcza gdy haker wzbudza zaufanie, wykorzystuje emocje, autorytet lub presję czasu. Wyobraź sobie, że otrzymujesz dramatyczny telefon od córki, słysząc jej prawdziwy głos. Dzięki technologii deepfake jest to możliwe.

Hakerzy chętnie podszywają się pod autorytety: „Tu policja”, „Jest problem z Twoim kontem bankowym, musimy działać szybko”. Zawsze, gdy ktoś próbuje wyrzucić na nas presję, abyśmy zrobili coś nietypowego, na przykład ujawnili hasło lub przelali pieniądze na nieznane konto, powinniśmy wziąć głęboki oddech, zatrzymać się i pomyśleć: Czy mój bank zadzwoniłby do mnie i poprosił o hasło? Czy zadzwoniłby do mnie urząd skarbowy? Czy mój syn poprosiłby mnie o pieniądze przez telefon? Zastanów się, zanim zaczniesz działać, i słuchaj swojego doświadczenia.

Z psychologicznego punktu widzenia, co sprawia, że pracownicy służby zdrowia są szczególnie podatni na socjotechnikę?

Lekarze, pielęgniarki czy osoby na rejestracji pracują w warunkach dużego stresu i odpowiedzialności. Muszą działać szybko i pod presją. Atakujący wykorzystują to za pomocą socjotechniki: krótki telefon, e-mail lub wiadomość, które wywołują poczucie pilności i wyłączają racjonalne myślenie.

Ale są też inne często występujące luki bezpieczeństwa danych generowane przez ludzi: pozostawianie włączonych laptopów bez nadzoru, udostępnianie hasel przez telefon lub zapisywanie ich na karteczkach, otwieranie załączników bez weryfikacji lub głośne omawianie informacji o pacjentach w miejscach publicznych.

Każdy drobny, rutynowy błąd może stać się furtką dla atakujących. Pewnej nocy spacerowałem korytarzami jednego ze szpitali. Liczba odblokowanych i pozostawionych bez nadzoru komputerów mnie zaszokowała. Jeśli zalogowany użytkownik oddala się na chwilę, otwiera szeroko drzwi każdemu, kto chce wykraść dane.

» Techniczne środki bezpieczeństwa nie zawsze są w stanie zniwelować ryzyko wynikające z niebezpiecznych zachowań ludzi. «

Czyli szkolenia z ochrony zdrowia powinny obejmować także profilowanie behawioralne.

Tak, główna zasada bezpieczeństwa danych to „poznaj swojego wroga”. Lubię opisywać cyberprzestępczość jako grę w szachy behawioralne. Im lepiej zrozumiemy motyw i metody hakerów oraz wnिकniemy w ich umysły, tym lepiej możemy się bronić i przygotować. Jeśli zrozumiemy, w jaki sposób hakerzy wykorzystują sztuczną inteligencję i deepfake'i oraz jak ten trend się rozwija, będziemy mogli się odpowiednio przygotować.

Techniczne środki bezpieczeństwa nie zawsze są w stanie zniwelować ryzyko wynikające z niebezpiecznych zachowań ludzi. Jeśli ujawnisz hasło przez telefon, ponieważ ktoś podaje się za „wsparcie IT” i twierdzi, że ma miejsce sytuacja awaryjna, nawet najlepsza zaporę sieciową lub zespół ds. bezpieczeństwa nie pomogą. Nie jestem przeciwny technicznym środkom bezpieczeństwa. Długie, zróżnicowane hasła, firewall'e, zabezpieczenia sieciowe i uwierzytelnianie wieloskładnikowe są niezbędne. Potrzebujemy jednak zarówno technicznej, jak i ludzkiej zapory sieciowej. A to wymaga ciągłego szkolenia pracowników.

Jak stworzyć taką zaporę sieciową z ludzi?

Pod pojęciem „zapory sieciowej z ludzi” rozumiem sytuację, w której pracownicy organizacji nie są słabym punktem, ale stanowią pierwszą linię obrony przed hakerami. Chodzi o świadomość, krytyczne myślenie, rutynowe czynności i kulturę bezpieczeństwa.

Moim zdaniem cyberbezpieczeństwo musi stać się atrakcyjne i ciekawe. Zbyt często szkolenia z ochrony danych są nudne. W efekcie postrzegamy je jako przykry obowiązek i szybko zapominamy, o czym były. Ale nie musi tak być. Możemy zabrać uczestników w podróż do Darknetu, co jest tak samo fascynujące jak najlepszy serial na Netflixie. Możemy sprawić, że obrona przed hakerami będzie zabawna.

Zabawna?

Tak. Pod koniec mojego pierwszego wykładu TEDx „*Psychologia cyberprzestępczości*”, podeszła do mnie osoba z publiczności i zapytała: „To było zabawne, ale czy naprawdę uważasz, że tak poważny temat jak cyberprzestępczość powinien być zabawny?”. Nie, nie powinien być zabawny, ale musi być zabawny. To jedyny sposób, aby dotrzeć do osób, które nie interesują się tematami związanymi z IT i cyberbezpieczeństwem.

Dzięki AI, ataki phishingowe są coraz doskonalsze.

Wspomniał Pan jak hakerzy klonują głos, a nawet wizerunek zaufanej osoby. Co zrobić, żeby w takich sytuacjach zadziałały odpowiednie procedury ochrony danych?

Sztuczna inteligencja i deepfake'i przenoszą inżynierię społeczną na nowy, dużo wyższy poziom, a podszywanie się pod znane osoby pracujące w organizacji i ataki na tożsamość stają się znacznie skuteczniejsze.

W służbie zdrowia mieszanka presji czasu, stresu i wielozadaniowości sprawia, że łatwiej jest manipulować ludźmi, aby dostać się do systemu IT. Do tego trzeba stworzyć odpowiednią kulturę ochrony danych, personel musi wiedzieć, kiedy powinno się zapalić czerwone światło, jak działają strategie „zatrzymywania się i weryfikacji” oraz jakie są procedury w przypadku nietypowych sytuacji. Każdy pracownik musi mieć świadomość, że przykładowo najpierw należy zadzwonić pod numer wybrany z telefonu, a nie oddzwaniać, zadawać pytania weryfikujące tożsamość lub używać wcześniej uzgodnione hasła. Świadomość w połączeniu z kulturą i rutyną pozostaje najskuteczniejszą formą obrony.

Pracownicy muszą wiedzieć, że każdy człowiek reaguje odruchowo pod wpływem emocji i stresu. Atakujący systematycznie to wykorzystują, a sztuczna inteligencja zwiększa zarówno ilość, jak i jakość tych ataków. Po drugie, autorytet i poczucie pilności są potężnymi narzędziami oddziaływania

na zachowania i nawet osoby dobrze wyszkolone mogą dać się oszukać. I po trzecie, większość cyberataków zaczyna się od błędu ludzkiego, ale ludzie mogą być również najsilniejszą obroną, jeśli są przeszkoleni, zmotywowani i mają odpowiednie uprawnienia.

Co o cyberbezpieczeństwie powinien wiedzieć każdy menedżer szpitala?

Moim zdaniem trzeba skończyć z traktowaniem cyberbezpieczeństwa w charakterze wyzwania czysto technicznego i zacząć postrzegać ludzi jako najważniejszy element pierwszej linii obrony przed hakerami. Jasne procedury, podnoszenie świadomości w tematach związanych z ochroną danych – to elementy, które muszą wniknąć w codzienną pracę. Szkolenie organizowane raz na jakiś czas nie wystarczy.

Drugim priorytetem jest normalizacja procedur weryfikacji. Personel powinien czuć się zachęcany do sprawdzenia źródła informacji przed podjęciem działania, nawet pod presją.

Zabezpieczenia jak podwójna autoryzacja muszą być postrzegane jako pomoc, a nie wyraz nieufności lub biurokracji.

I wreszcie, zachęcam do szkoleń, podczas których omawiane są elementy psychologii. Kiedy ludzie dowiadują się, dlaczego ataki są skuteczne, w jaki sposób celowo wykorzystuje się poczucie pilności, autorytet i strach oraz jakie błędy poznawcze są słabymi punktami każdej osoby, znacznie lepiej rozpoznają wczesne sygnały ostrzegawcze i nie dają się tak łatwo zmanipulować. ●

Hakerzy czasami kradną dane, aby się popisać i wzbudzić respekt u innych hakerów.





5 sposobów, jak uniknąć kary Urzędu Ochrony Danych Osobowych

W 2025 roku UODO nałożył rekordowe kary za naruszenie ochrony danych osobowych. Ich wysokość była prawie 5-krotnie wyższa niż w 2024 roku i przekroczyła 64 mln zł. Wśród nich była też grzywna dla podmiotu medycznego w kwocie 1,1 mln zł. Paradoksalnie, większości z nich można było uniknąć.

» Trudno w to uwierzyć, ale część podmiotów nadal nie spełniła podstawowego obowiązku RODO, jakim jest wyznaczenie Inspektora Ochrony Danych. «

Nie jest tajemnicą, za co można dostać karę od UODO, bo wszystkie sprawy podawane są do opinii publicznej na stronie www organu nadzorczego. Najważniejszy wniosek jest taki, że jeszcze nigdy UODO nie nałożył grzywny za to, że hakerzy wykradli dane – to może zdarzyć się każdej firmie posiadającej nawet najlepsze zabezpieczenia. Po kary sięga się wtedy, gdy uchybienia są rażące albo gdy podmiot odmawia współpracy lub utrudnia wyjaśnienie sprawy.

– Kary Prezesa UODO często mają związek z naruszeniami ochrony danych osobowych, ale są nakładane nie za to, że doszło do konkretnego incydentu, ale za nieprzestrzeganie przepisów o ochronie danych osobowych – mówi w rozmowie z OSOZ Mirosław Wróblewski, Prezes UODO.

Przeanalizowaliśmy wszystkie administracyjne kary pieniężne nałożone w ostatnich 5 lat. Które powtarzają się najczęściej?

Liczba i wysokość kar nakładanych przez UODO w latach 2020–2025

Rok	Liczba decyzji	Kwota kar
2020	10 decyzji	3,5 mln zł
2021	14 decyzji	2,2 mln zł
2022	13 decyzji	6,1 mln zł
2023	30 decyzji	1,2 mln zł
2024	20 decyzji	13,9 mln zł
2025	19 decyzji	64 mln*

* dane do listopada 2025

Wysokość kary w zależności od naruszenia (średnia dla lat 2020–2025)

Kategoria naruszenia	Przedział kar (PLN)
Brak zgłoszenia naruszenia	20 000 – 250 000
Niedostateczne zabezpieczenia	30 000 – 500 000+
Brak współpracy z UODO	10 000 – 150 000
Brak / błędy IOD	10 000 – 50 000
Transfery danych niezgodne z prawem	100 000 – kilka mln

Niezgłoszenie naruszenia ochrony danych i niepowiadomienie poszkodowanych osób

Jedna z najczęstszych kar (około 25% wszystkich) dotyczy sytuacji, w której administratorzy nie zgłosili naruszenia organowi nadzorczemu „bez zbędnej zwłoki”, czyli 72 godziny od zidentyfikowania problemu, albo nie powiadomili osób poszkodowanych w sytuacji, gdy naruszenie miało wysokie ryzyko. To twarda zasada, w przypadku której rzadko kiedy udało się uniknąć kary poprzez odwołanie decyzji do sądu administracyjnego.

A można się przed nią ustrzec w banalnie prosty sposób, wdrażając procedurę wykrywania i raportowania incydentów (*Incident Response*), określając, kto jest odpowiedzialny za zgłoszenie naruszenia i kontakt z osobami poszkodowanymi, przygotowując gotowe szablony zgłoszeń i komunikatów dla osób, których dane dotyczą.

Za takie niedociągnięcia dotąd nałożone kary były bolesne i sięgały 250 tys. zł, nawet w przypadku podmiotów publicznych.

Niedostateczne środki techniczne i organizacyjne w zakresie bezpieczeństwa danych

RODO obowiązuje w Polsce już od 7 lat i pomimo to nadal wiele podmiotów nie wprowadziło podstawowych jego zapisów. Na początku UODO pobłażliwie traktowało uchybienia, ale teraz twardo karze za brak zabezpieczeń, takich jak niezaszyfrowane bazy danych, brak regularnego testowania mechanizmów bezpieczeństwa danych, nieodpowiednie zabezpieczenia urządzeń mobilnych. Kary w tym obszarze dotyczą ok. 35% wszystkich nałożonych kar administracyjnych, a ich wysokość przekraczała nawet 500 000 zł.

Pierwszym krokiem jest przeprowadzenie rzetelnej oceny ryzyka, wdrożenie polityki szyfrowania danych w spoczynku i w transzycie, zarządzanie aktualizacjami, segmentacja sieci (różne sieci dla różnych systemów), wielopoziomowe logowanie i regularne zmiany haseł, tworzenie i testowanie kopii zapasowych oraz przygotowanie procedur odzyskiwania danych.

Brak współpracy z organem nadzorczym i nieprzekazywanie informacji

Ukrywanie naruszenia i liczenie na to, że „nikt nie zauważy”, to wysoce ryzykowna strategia, bo UODO najczęściej dowiaduje się o sprawach od samych poszkodowanych. UODO karze też wtedy, gdy administrator danych osobowych odmawia udostępnienia dokumentów lub danych niezbędnych do kontroli albo opóźnia realizację analizy sprawy. Ten powód nałożenia kary dotyczy co dziesiątej sprawy, a można byłoby go zminimalizować do zera. Jak?

Stwórz kulturę kładącą nacisk na jawne komunikowanie incydentów w zakresie ochrony danych osobowych, wyznacz dedykowaną do kontaktu osobę, przeprowadź szkolenia dla pracowników ze współpracy z UODO i innymi organami, jak CSIRT CeZ i Policją. Na ukrywaniu można stracić podwójnie, bo takie sprawy najczęściej odbijają się szerokim echem w mediach.

Nieprawidłowości w wyznaczaniu lub brak Inspektora Ochrony Danych (IOD)

Trudno w to uwierzyć, ale część podmiotów nadal nie spełniła podstawowego obowiązku RODO, jakim jest wyznaczenie Inspektora Ochrony Danych. W tym przypadku kara jest jednoznaczna, a odwołanie się do sądu administracyjnego – bezskuteczne. To uchybienie najczęściej dotyczy jednostek publicznych. Przy dobrej współpracy z UODO sprawa kończy się upomnieniem, ale w przeszłości były i kary wynoszące od 10 do 150 tys. zł.

Niwelowanie ryzyka otrzymania tej kary też jest proste: sprawdź obowiązki w zakresie IOD w przepisach RODO, wyznacz jego obowiązki, opublikuj dane kontaktowe.

Uchybienia w przekazywaniu danych poza EOG

Statystycznie co szósta kara UODO dotyczy przekazywania danych do krajów znajdujących się poza Europejskim Obszarem Gospodarczym bez wymaganych umów powierzenia. Należy dokładnie przeanalizować ryzyko po stronie dostaw-

ców i to czy dane osobowe lub medyczne nie są przetwarzane na serwerach w np. USA (wiele e-usług koncernów zagranicznych jest opartych na chmurach danych znajdujących się właśnie w USA, np. call center).

Jak uniknąć kar UODO? Poradnik

Odpowiadaj na każde pismo UODO

Brak odpowiedzi na pisma organu nadzorczego jest najkrótszą drogą do otrzymania kary. Niezależnie od oceny zasadności zarzutów, każda korespondencja z UODO wymaga reakcji w wyznaczonym terminie.

Szyfruj nośniki danych i stosuj kontrolę dostępu

Zagubiony niezasyfrowany laptop czy pendrive z danymi pacjentów – za to już UODO nakładał kary. Szyfrowanie dysków twardych i nośników przenośnych, polityka czystego biurka, kontrola dostępu do systemów IT to minimum wymagań wynikających z art. 32 RODO.

Wdrożenie procedury 72 godzin

Każda organizacja musi mieć procedurę zgłaszania naruszeń, regularnie ją testować i komunikować pracownikom. Obejmuje m.in. metody identyfikacji naruszenia, szablon zgłoszenia do UODO oraz kryteria oceny, czy konieczne jest również powiadomienie osób fizycznych.

Weryfikuj podmioty przetwarzające

Wiele kar wynikało z faktu, że administrator nie sprawdził, czy jego podwykonawcy – przykładowo firma IT, dostawca systemu HIS, operatorzy call center – zapewniają właściwy poziom bezpieczeństwa. Umowa powierzenia przetwarzania to absolutne minimum.

Wyznacz IOD

W 2024 roku jedną z kar nałożono na podmiot, który nie wyznaczył Inspektora Ochrony Danych po 6 latach od wejścia w życie RODO. To obowiązek ustawowy.

Kary dla podmiotów medycznych

Choć kary na podmioty medyczne nadal stanowią tylko niewielką część wszystkich kar UODO, to czasami są one bardzo wysokie i rzucają się cieniem na zaufaniu pacjentów do placówki zdrowia.

Oto kilka przykładów. W 2025 roku Centrum Medyczne Ujastek zostało ukarane kwotą ponad 1,1 mln zł za niezgodny z prawem monitoring na salach neonatologii oraz brak odpowiednich zabezpieczeń technicznych i organizacyjnych danych osobowych. W 2024 roku spółka American Heart of Poland otrzymała karę 1,5 mln zł za naruszenie bezpieczeństwa danych około 21 000 osób. Powodem był atak hakerów, będący następstwem błędnej oceny ryzyka i nieprzestrzegania polityki bezpieczeństwa.

Również w 2024 roku SPZOZ w Pajęcznie dostał karę 40 000 zł za niewystarczające środki ochrony danych po ataku ransomware oraz niewypełnienie obowiązku powiadomienia osób dotkniętych incydem. W 2025 roku Uniwersytecki Dziecięcy Szpital Kliniczny w Białymstoku otrzymał karę 66 500 zł za nieprawidłową analizę ryzyka oraz brak odpowiednich technicznych i organizacyjnych środków po ataku ransomware. Z kolei Gyncentrum otrzymało karę 40 000 zł za niepowiadomienie o naruszeniu danych pacjentów po wysłaniu dokumentu zawierającego dane do niewłaściwej osoby.

Na koniec warto zaznaczyć, że polityka bezpieczeństwa danych w podmiocie medycznym nie powinna mieć na celu uniknięcia kary UODO albo innego organu nadzorczego, ale ochronę danych pacjentów. Jeśli to będzie priorytetem, o kary nie trzeba się martwić. ●

SALMED CONNECT

MEDYCYNĄ. EKSPOZYCJĄ. DIALOG

19-20 MAJA 2026

Poznań Congress Center

SALMED 2026 – tu rozwija się przyszłość medycyny!

Dlaczego warto odwiedzić targi?

- Zobacz nowości i innowacje w sprzęcie medycznym, wyposażeniu placówek i technologii dla ochrony zdrowia
- Poznaj liderów branży i porozmawiaj bezpośrednio z producentami, dystrybutorami i ekspertami
- Sprawdź sprzęt w praktyce podczas prezentacji, pokazów i demonstracji urządzeń
- Rozwiń swoją wiedzę dzięki konferencjom, wykładom i warsztatom prowadzonym przez uznanych specjalistów
- Zainspiruj się nowymi trendami w diagnostyce, rehabilitacji, opiece szpitalnej i technologii medycznej
- Nawiąż wartościowe kontakty z profesjonalistami i decydentami w sektorze zdrowia

www.salmed.pl

ORGANIZATORZY:



**Zarejestruj się
i odbierz bilet**





Ochrona danych w indywidualnej praktyce lekarskiej. „Już za ok. 1200 zł rocznie można uchronić się przed 90 proc. ataków”

Kiedy duże szpitale nadrabiają zaległości w cyberbezpieczeństwie, między innymi dzięki środkom z KPO, małe, indywidualne praktyki lekarskie stają się łatwym łupem dla hakerów. Ale dobra ochrona danych to kwestia prostych zabezpieczeń za ok. 100 zł miesięcznie.

1400 zł – tyle biorą hakerzy za ukradzioną kartotekę medyczną pacjenta

Szacuje się, że 8 na 10 lekarzy doświadczyło próby ataku hakerskiego. Złamanie zabezpieczeń jest znacznie łatwiejsze niż w przypadku coraz lepiej chronionych dużych placówek, przy czym wartość danych i obietnica szybkiego zarobku – takie same albo większe. Lekarz, który przez lata pracował na zaufanie swoich pacjentów, może je stracić w ułamku sekundy. Hakerzy o tym dobrze wiedzą.

Nawet 1400 zł kosztuje w darknecie skradziona kartoteka medyczna. To znacznie więcej niż dane karty kredytowej, które można zdobyć już za 25 zł. Chętnych, żeby je kupić, nie brakuje, bo to łatwe narzędzie wywierania przez przestępców presji okupu na lekarzy. W przypadku ataku ransomware, w panice wiele osób woli przelać w bitcoina kilka tysięcy złotych, aby szybko odblokować komputer. Według statystyk, robi to ok. 20–50% ofiar. Zapłata nie gwarantuje jednak, że haker nie wykradł dodatkowo danych, potem ktoś je kupi i w krótkim czasie pojawiają się kolejne szantaże i groźby. Ataków phishingowych przybywa, a hakerzy coraz lepiej podszywają się pod NFZ i ZUS, aby przekonać do kliknięcia w zainfekowany link.

Brak zabezpieczeń przed hakerami to ryzykowna gra, która może źle się skończyć. A wystarczy nieco ponad 100 złotych miesięcznie, aby spać spokojniej.

Menedżer haseł dla całego gabinetu

Najczęstszą przyczyną włamania do komputera, a następnie do systemu gabinetowego, są słabe hasła. Eksperti zalecają stosowanie menedżerów haseł, które generują długie, unikalne hasła złożone z różnych kombinacji liter, cyfr i znaków specjalnych oraz przechowują je w zaszyfrowanej bazie. Menedżer haseł jest dostępny za darmo m.in. w przeglądarce internetowej Chrome od Google i Edge od Microsoft. Mają go też popularne systemy antywirusowe w wersjach premium, jak np. Avast. Użytkownik musi pamiętać tylko hasło główne do menedżera.

Dwuskładnikowe uwierzytelnianie

Nawet jeśli haker zdobędzie hasło, nie dostanie się do systemu zabezpieczonego tzw. 2FA, czyli metodą dwuetapowego uwierzytelniania. Logowanie trzeba wówczas potwierdzić kodem wysłanym na aplikację w telefonie. 2FA znacząco redukuje ryzyko skutecznego ataku i stało się standardem zabezpieczenia danych.

2FA można włączyć za darmo m.in. w poczcie internetowej. Jest też wymagane podczas logowania do platform ZUS i NFZ. Wspierają go np. bezpłatny Microsoft Authenticator albo Google Authenticator oraz niektóre aplikacje mobilne dla lekarzy i pielęgniarek.

Chmurowe kopie zapasowe z wersjonowaniem

Kiedy lekarz kliknie przez nieuwagę na link albo załącznik w wiadomości phishingowej, na komputerze zostanie zainstalowane złośliwe oprogramowanie ransomware. Szyfruje ono dane, a na ekranie pojawia się żądanie okupu. Komputer zostaje zablokowany. Jedynym wyjściem jest ponowna instalacja Windows, co oznacza utratę danych. W tym czarnym scenariuszu lekarz traci w jednej chwili dostęp do wszystkich kartotek swoich pacjentów, terminów, kontaktów – danych zbieranych przez kilka, kilkanaście lat.

Jedynym ratunkiem jest kopia zapasowa na innym nośniku danych, a najlepiej w innej lokalizacji, bo dane można stracić też w wyniku np. poważnej awarii komputera, pożaru, kradzieży itd. Najwygodniejszą i nie wymagającą żadnych dodatkowych czynności (oprócz jednorazowej konfiguracji) jest kopia w chmurze danych. Taki backup jest coraz tańszy.

» Lekarz może w jednej chwili stracić dostęp do wszystkich kartotek swoich pacjentów, terminów, kontaktów – danych zbieranych przez kilka, kilkanaście lat. «

Przykładowo, w systemie KS-PPS firmy KAMSOFIT kosztuje ok. 600 zł netto rocznie za jeden serwer. Systemy gabinetowe mają też inne opcje bezpieczeństwa danych, jak np. moduł ułatwiający spełnienie wymagań RODO (cena także ok. 600 zł za pierwszy rok).

Szyfrowanie dysków i urządzeń mobilnych

System Windows 10 lub 11 Pro oraz macOS oferują wbudowane szyfrowanie dysku, tzw. BitLocker (Windows) oraz FileVault (Apple). Jego aktywacja jest bezpłatna.

Po co szyfrować dyski? Jeśli urządzenie zostanie skradzione lub zgubione, dostęp do danych pacjentów – w przypadku lokalnej bazy danych – będzie znacznie utrudniony. Szyfrowanie jest też kluczowe w kontekście RODO. W przypadku urządzeń mobilnych, jak smartfon albo tablet, szyfrowanie najczęściej aktywowane jest automatycznie, np. poprzez FaceID (rozpoznawanie twarzy) lub TouchID (odcisk palca).

Szkolenie z cyberbezpieczeństwa i phishingu

Lekarze regularnie uczestniczą w konferencjach oraz szkoleniach, aby zaktualizować swoją wiedzę medyczną. Warto je uzupełnić o przynajmniej jedno szkolenie rocznie na temat bezpieczeństwa danych. Te organizowane przez Akademię Centrum e-Zdrowia są bezpłatne. Aby być na bieżąco, polecamy newsletter ezdrowie.gov.pl. Dużo dostawców IT organizuje też własne kursy albo webinary on-line, za które nie trzeba płacić.

Powyższe opcje powinny wystarczyć, aby być na bieżąco z cyberzagrożeniami. Zainteresowani wiedzą na poziomie zaawansowanym, łatwo znajdą szkolenia z cyberbezpieczeństwa za ok. 200–1000 zł od osoby. Te z NIS2, które choć nie dotyczą gabinetów lekarskich to mogą się przydać, kosztują od 2000 zł w górę.

Antywirus i firewall

Kiedyś to komputery Apple uchodziły za dużo bezpieczniejsze niż Windows, ale najnowsze wersje systemu firmy Microsoft

też mają bardzo dobre zabezpieczenia przed wirusami. Ochrona zdrowia wymaga aktualnego systemu operacyjnego, bo hakerzy często wykorzystują luki w zabezpieczeniach w nieaktualnym oprogramowaniu. Dlatego pod żadnym pozorem nie można wyłączać automatycznych aktualizacji systemów operacyjnych. Update trzeba przeprowadzić natychmiast po tym, jak na ekranie pojawi się informacja o nowej wersji i prośba o restart komputera.

W systemie iOS oraz w usłudze Windows 365 dane są gromadzone w chmurze (tylko dane systemowe i tworzone przez użytkownika pliki, teksty i obrazy, ale nie baza danych systemu gabinetowego), co ułatwia ich odzyskanie po awarii lub blokadzie systemu przez cyberprzestępców.

Antywirus nadal warto mieć, gdy w grę wchodzi dane medyczne. Programy takie jak Avast, Norton 360 czy Bitdefender, oprócz firewalla mają też wbudowane narzędzia rozpoznawania zagrożeń w czasie rzeczywistym (np. podczas odwiedzania stron www), zarządzania hasłami, wykonywania skanowania dysków albo konserwacji komputera. Roczna licencja kosztuje ok. 150–250 zł.

Na koniec jeszcze jedna rada: na komputerze z systemem gabinetowym nie powinno się instalować żadnych innych programów albo, co gorsza, korzystać z prywatnej poczty, odwiedzać prywatnie strony internetowe, robić zakupy online. To idealne okazje dla hakerów, aby wykraść nasze dane.

Zestawienie rocznych kosztów podstawowych zabezpieczeń

Rodzaj zabezpieczenia	Zakres	Koszt roczny (PLN)
Chmurowa kopia zapasowa (np. system KS-PPS – KAMSOFI)	Backup w chmurze	ok. 600
Moduł zgodności z RODO	Wsparcie spełnienia wymagań ochrony danych osobowych	ok. 600 za pierwszy rok i 300 zł za kolejny
Oprogramowanie antywirusowe + firewall (wersja premium)	Ochrona w czasie rzeczywistym	150–250
Szkolenie z cyberbezpieczeństwa	W ramach Akademii Centrum e-Zdrowia	0
Menedżer haseł (np. Chrome – Google/Edge – Microsoft)	Generowanie i przechowywanie haseł	0
Dwuskładnikowe uwierzytelnianie 2FA (np. Microsoft Authenticator/Google Authenticator)	Dodatkowa warstwa logowania	0
Szyfrowanie dysku (BitLocker/FileVault)	Ochrona danych w przypadku kradzieży sprzętu	0
Razem (rocznie)		1350–1450 zł

OCHRONA DANYCH W GABINECIE LEKARSKIM

Używaj menedżera haseł.

Generuj długie i unikalne hasła zamiast powtarzać te same w różnych systemach.



Włącz uwierzytelnianie dwuskładnikowe 2FA.

Kod wysyłany na telefon skutecznie blokuje kradzież danych, nawet jeśli haker zna hasło.



Twórz automatycznie kopie zapasowe w chmurze.

Szybko odzyskasz dane po ataku ransomware. Nie musisz myśleć o codziennym robieniu back-upów.



Szyfruj dyski i urządzenia mobilne.

W przypadku kradzieży sprzętu dane pacjentów pozostaną niedostępne.



Szkol się z cyberbezpieczeństwa.

Znajomość socjotechnik i nowych metod hakerów zmniejsza ryzyko kliknięcia w zainfekowany link albo nabrania się na ataki z wykorzystaniem AI.

WWW

Włącz automatyczne aktualizacje systemu operacyjnego.

Luki w Windows są częstą drogą ataku.

Nie trać czasu na szukanie leków po aptekach

- skorzystaj z serwisu

 **KtoMaLek.pl**



1 Podaj lokalizację
Powiedz nam gdzie jesteś, poszukamy leku w Twojej okolicy.

Wpisz miasto lub adres (np.: Katowice, 1 Maja 133)

Miasto, ulica

lub udostępnij lokalizację

2 Wskaż lek
Wykaż lek, a następnie wybierz aptekę.

3 Zarezerwuj lek
360 rezerwacji w wybranej aptece.

4 Odbierz lek
Odbierz lek w aptece i zapłać przy odbiorze.

**Sprawdzamy
dostępność
leków w ponad
11 000 aptek!**

➤ Oszczędzaj czas

Dowiedz się, w której najbliższej aptece dostępny jest potrzebny Ci lek. Zarezerwuj go on-line.

➤ Uzyskaj wsparcie Farmaceuty on-line

Jeśli masz pytania dotyczące leku, sposobu zażywania, interakcji - zapytaj farmaceutę.

➤ Miej KtoMaLek zawsze pod ręką

Pobierz bezpłatną aplikację KtoMaLek lub VisiMed, wyszukuj i rezerwuj leki kiedy chcesz.





W jakich sprawach pacjenci zwracają się do AI?

Dużo mówi się o tym, że AI często jest stosowana do diagnozowania chorób. Ale o wiele częściej pacjenci pytają AI o błahe sprawy organizacyjne – wynika z nowego badania opublikowanego w prestiżowym Journal of the American Medical Informatics Association (JAMA).

AI od prostych zadań

W styczniu br. ukazał się raport OpenAI, twórcy ChatGPT, w którym autorzy sugerują, że najczęściej poruszonymi w rozmowach z AI tematami zdrowotnymi są te dotyczące spraw administracyjnych: ubezpieczenia zdrowotnego, poruszania się po systemie zdrowia. AI jest pomocne szczególnie wtedy, gdy zaniepokojeni pacjenci szukają porady poza godzinami pracy gabinetów lekarskich.

Potwierdza to badanie “What patients want from healthcare chatbots: insights from a mixed-methods study” przeprowadzone przez zespół badaczy z University of Colorado Anschutz Medical Campus. Według niego, pacjenci zwracają się do AI wtedy, gdy oczekują szybkiej pomocy i życzą sobie dyskretnego rozwiązania problemu bez oceniania przez człowieka.

W ankiecie wzięło udział 617 osób, a 46 osób uczestniczyło w wywiadach pogłębionych. Warto wspomnieć, że mieli oni dostęp do chatbota zintegrowanego z elektroniczną dokumentacją medyczną (EDM). Pacjenci używają chatbotów głównie do spraw administracyjnych, jak umawianie wizyt, sprawdzanie wolnych terminów, odnawianie recept, przegląd wyników badań laboratoryjnych, pytania o rozliczenia (89 proc.). Według nich, AI dostępna jest o każdej porze i nie wymaga angażowania lekarza ani personelu. Prawie połowa badanych wskazała, że wybrała chatbota, bo szukała natychmiastowej odpowiedzi dotyczącej sprawy związanej ze zdrowiem, a sprawa była zbyt prozaiczna, aby od razu pytać lekarza. Co piąta osoba tak zrobiła, bo nie była pewna, czy uda się dodzwonić do lekarza lub pielęgniarki.

» Dla większości pacjentów chatbot AI jest dyskretnym i neutralnym asystentem, który uzupełnia lukę w systemie zdrowia.«

W wywiadach powtarzała się odpowiedź „nie chcę zwracać głowy lekarzowi”. Chatbot ma nieograniczony czas, nie jest zmęczony, nie ma złego dnia. W świecie przeciążonych poradni to wartość sama w sobie.

AI do intymnych rozmów

Cześć pacjentów docenia anonimowość rozmów z chatbotem, a takiej oczekują w rozmowach o problemach psychicznych i seksualnych oraz uzależnieniach. Nie sądzą przy tym, że chatbot jest lepszy od lekarza, ale priorytetem jest zaufana rozmowa w zaciszu domowym, bez wstydu towarzyszącego rozmowie z drugim człowiekiem. 36 proc. respondentów obawia się, że lekarz może ich ocenić lub „źle o nich pomyśleć”. W przypadku chatbota ten odsetek wynosi tylko 25 proc. Chatbot dobrze sprawdza się jako narzędzie pierwszego kontaktu w sprawach intymnych. Pacjent może bez obaw zadać każde pytanie, sprawdzić opcje leczenia, a dopiero potem zdecydować, czy chce umówić wizytę.

Trzeci wniosek dotyczy uprzedzeń i równego traktowania. 80 proc. uczestników badania zadeklarowało, że chatbot wydaje im się mniej stronniczy niż człowiek w kwestii np. pochodzenia. 75 proc. respondentów doceniło, że chatbot traktuje wszystkich tak samo, niezależnie od płci czy rasy.

AI sprawdza się świetnie, gdy problem nie jest pilny. Ale kiedy pacjenci szukają pewnej diagnozy, kontakt z lekarzem pozostaje na pierwszym miejscu. W wywiadach powtarzał się argument, że diagnoza, decyzje terapeutyczne i rozmowa o poważnych problemach powinny należeć do lekarza. Tylko 29 proc. badanych zgodziło się ze stwierdzeniem, że chatbot może podejmować decyzje kliniczne, które do tej pory zarezerwowane są dla personelu medycznego.

AI jako pierwszy kontakt z systemem zdrowia

Badanie daje ciekawy wgląd w to, jak AI może uzupełniać kompetencje lekarzy. Najlepszy z punktu widzenia pacjentów jest model hybrydowy – połączenie dostępu do chatbota z wizytą lekarską. Chatbot może przejąć wiele zadań admini-

stracyjnych i zachęcić do kontaktu z lekarzem w przypadku chorób i problemów wstydlivych. Ale ostateczna diagnoza i leczenie są już w rękach lekarza.

To, że obawy o ocenę ze strony lekarza często powstrzymują pacjentów przed wizytą, wiadomo od dawna. AI świetnie zaspokaja potrzebę intymnej rozmowy w zaciszu domowym. Wiele innych badań sugeruje, że osoby regularnie korzystające z chatbotów często traktują je w charakterze dobrych wirtualnych przyjaciół. Emocje odgrywają ważną rolę w zaufanej komunikacji z pacjentem – jeśli tej nie uda się zbudować, pacjent nie powie lekarzowi wszystkiego, co negatywnie wpływa na diagnozę i efekty leczenia.

Wniosek z badania jest optymistyczny: pacjenci wcale nie idealizują technologii, a AI stosują do uzyskiwania szybkich odpowiedzi, często zbyt prozaicznych, aby od razu dzwonić do lekarza. Znają jej ograniczenia, traktując ją jako zaufanego doradcę oraz nowe narzędzie pozwalające na pierwszy kontakt z systemem zdrowia. ●

reklama

OPIEKA KOORDYNOWANA

W PODSTAWOWEJ OPIECE ZDROWOTNEJ

AKTUALNE WYDANIE!
Staw na września 2023.

PRZEWODNIKI PO CYFROWEJ OCHRONIE ZDROWIA
KLUS-OSOZ.PL

SIEMET
5 kroków do wdrożenia
Opieki Koordynowanej w POZ

PODSTAWY
Czym jest POZ, jakiej
pomoc, PPM, usługi,
opieki koordynowanej

OPINIA EKSPERTA
Marek J. G. G. G.
Agencja Medyczna Migan

RAJNY LECZKAJA
Pracownicy wdrożenia
wieloletni Tomasz Górecki

ECHEKA PACJENTA
Marek J. G. G. G.
wydanie koordynowanej

ODRODZENIE IT
Wdrożenie, integracja, modernizacja
systemu koordynowania

CIĘTYSTWA
Marek J. G. G. G. G.
Pracownicy koordynowanej

POMOCY MENEDŻERA
Marek J. G. G. G. G.
Pracownicy koordynowanej

NOWE NARZĘDZIA
Opracowanie, wdrożenie,
wdrożenie koordynowanej

PROJEKTOWANIE I WYKONANIE
KAMSOFT S.A.

PORADNIK WDRAŻANIA OPIEKI KOORDYNOWANEJ W POZ.

ZAWIERA BEZPŁATNY WEBINAR

POBIERZ ZA DARMO

BLOG.OSOZ.PL



Nowe roboty z Chin tańczą i popisują się Kung-Fu. Efektowny show czy powód do zmartwienia?

Film z tańczącymi i walczącymi robotami podczas chińskiej Spring Festival Gala 2026 zachwyca i przeraża. Jeszcze rok temu podobne maszyny jedynie machały chusteczkami, chwiejnie stąpając w miejscu. Czy Chiny właśnie wygrały wojnę o dominację w robotyce?

Noworoczna Gala Festiwalu Wiosny to w Chinach wydarzenie tak samo ważne jak Super Bowl w USA, oglądane przez miliony ludzi na całym świecie. W tym roku, 16 lutego, na scenie pojawiły się roboty, które wykonywały akrobatyczne sztuczki i salta, symulowały walkę, tańczyły.

Barwne i dynamiczne widowisko to mocny sygnał polityczny i gospodarczy z Pekinu: Chiny są liderem robotyki i innowacji AI, zostawiając w tyle amerykańskie firmy.

Cztery nowe klasy robotów już do kupienia

Podczas Gali można było zobaczyć humanoidy czterech chińskich spółek: Unitree Robotics, MagicLab, Noetix oraz Galbot. W głównym widowisku humanoidy Unitree wykonywały trzymetrowe salta, przeskakiwały przez przeszkody, wywijają kijami i mieczami używanymi we wschodnich sztukach walki, celowo upadały i podnosiły się na nogi. Ten ostatni element jest istotny, bo zdolność do odzyskiwania równowagi po upadku, tzw. fault recovery, jest jednym z kluczowych wskaźników dojrzałości systemów sterowania ruchem robotów.

MagicLab zaprezentował modele robotów MagicBot Gen1 i Z1, które tańczyły synchronicznie z dziećmi, utrzymując identyczny rytm, tempo obrotów i precyzję ruchów. Noetix pokazał bionicznego robota z twarzą przypominającą do złudzenia znaną chińską aktorkę. Wyposażono go w 32 mikrosilniki sterujące mimiką, w tym 12 – ruchami ust. Humanoid G1 firmy Galbot chwalił się zdolnościami manualnymi, obracając orzechy w dłoni i składając ubrania.

W czasie transmisji Gali na żywo można było kupić online wybrane modele robotów obecnych na scenie, w tym dwa roboty Galbot G1 za ok. 325 000 zł za sztukę. W kilka minut sprzedano wszystkie egzemplarze.

Według oficjalnych danych, w 2024 r. w Chinach zarejestrowanych było ponad 451 tys. firm zajmujących się robotyką. Rozwój AI i robotyki to główne priorytety polityki Chin, zapisane w bieżącym planie pięcioletnim. Mówi się w nim o tzw. „embodied intelligence”, czyli inteligencji ucieleśnionej. Bank Morgan Stanley prognozuje, że sprzedaż humanoidów w Chinach przekroczy w 2026 r. 28 tys. sztuk.

Pstryczek w ambicje USA czy jedynie świetna propaganda?

Pokaz odbił się szerokim echem w mediach w USA i Europie oraz stał się okazją do dyskusji nad tym, czy Chiny właśnie zapewniły sobie globalną dominację technologiczną. Niektórzy mówią wprost, że widowisko to kompromitacja Elona Muska, który od lat rozwija swojego humanoida o nazwie Optimus. Jak na razie nie może się pochwalić tak efektownymi postępami jak maszyny” made in China”, starając się wzbudzać zainteresowanie Optimusem kontrowersyjnymi wypowiedziami. Przykładowo, w wywiadzie ze stycznia 2026 r. stwierdził, że w okresie 3 lat jego robot prześcignie umiejętności najlepszych chirurgów.

Mimo że synchroniczne walki i tańce robotów zapierają dech w piersi, część ekspertów od robotyki uspokaja: występy sceniczne są efektem wielokrotnego trenowania konkretnej sekwencji ruchów w kontrolowanym środowisku. Roboty od początku do końca poruszają się zgodnie z programem. To nie to samo co praca w fabryce albo w szpitalu.

Ale mimo to postęp w umiejętnościach ruchowych jest ogromny. Na ewolucję robotyki czeka też ochrona zdrowia mierząca się z wyzwaniem zapewnienia opieki starzejącemu się społeczeństwu. Roboty domowe są nadzieją na jej przesunięcie z domów starców do domów. Z kolei szpitale i przychodnie, którym coraz bardziej doskwiera niedobór personelu pilnie potrzebują wsparcia w prostych czynnościach logistycznych, jak transport materiałów z magazynu, sprzątanie sal operacyjnych i przygotowanie oddziałów na przyjęcie nowych pacjentów. ●



Kliknij tutaj, aby zobaczyć
spektakl chińskich robotów



Diagnoza po konsultacji z Chatem GPT. "Byłam kompletnie zszokowana"

Zadała pytanie dla zabawy. ChatGPT uratował jej życie

Chat GPT uratował ją przed rakiem. Lekarze pomylili diagnozę

Śmierć 16-letniego Adama. Rodzice pozywają twórcę programu ChatGPT



Lekarze postawili chorej złą diagnozę. ChatGPT uratował jej życie

Pacjenci chwalą się jak „ChatGPT uratował im życie”. Ale to nie cała prawda

W mediach społecznościowych mnoży się od opowieści pacjentów, jak ChatGPT albo inne narzędzia AI zdiagnozowały chorobę, której nie wykrył lekarz. Rzadko kiedy czytamy, że ChatGPT źle doradził.

AI ma czas na sprawdzenie wszystkich opcji, lekarz nie

„Jako osoba autystyczna używam ChatGPT, aby zrozumieć, co ludzie myślą, co czuję, jak mogę sobie z czymś poradzić. Absolutnie ratuje mi życie i zawsze czuję się o wiele lepiej,

» Ok. 5–7% wszystkich zapytań w Google dotyczy zdrowia. Często odpowiada AI.«

ponieważ AI usuwa niepokój z mojego codziennego życia” – pisze na forum dyskusyjnym Reddit jeden z użytkowników.

Podobne historie systematycznie pojawiają się w prasie. Ostatnio NPR opisał sprawę Bethany Crystal z Nowego Jorku. Po pojawieniu się czerwonych plam na nogach, pacjentka zapytała ChatGPT o możliwe przyczyny. AI zasugerowała „natychmiastową ocenę pod kątem ryzyka krwawienia”. Po trzech dniach badań u pacjentki rozpoznano rzadką chorobę autoimmunologiczną – *Immune thrombocytopenic purpura* – która prowadzi do spadku liczby płytek krwi i zwiększonego ryzyka krwotoków. Bez rekomendacji AI, pacjentce groziłaby śmierć.

Z kolei na portalu Medium pojawiła się historia osoby z myślami samobójczymi, która po podzieleniu się nimi z ChatGPT rozpoczęła długi dialog z AI. Ostatecznie sztuczna inteligencja w empatyczny sposób przekonała do tego, że warto żyć.

1 miliard zapytań o zdrowie każdego dnia

Według raportu OpenAI ze stycznia br., już 40 milionów osób korzysta codziennie z ChatGPT w poszukiwaniu porad dotyczących zdrowia. Dotyczy ich ok. 5–7% wszystkich zapytań w Google, co przelicza się na 70 000 zapytań na minutę. Odpowiedzi mają najczęściej formę podsumowań AI, które Google wprowadził w 2025 roku.

Pacjenci chwalą AI za dogłębną analizę ich problemu medycznego i nieograniczony czas. AI zadaje kolejne pytania, analizuje możliwe scenariusze, jest cierpliwa i empatyczna. Takie podejście nie jest możliwe w przeciążonej ochronie zdrowia.

W medycynie przyjęło się powiedzenie „jeśli słyszysz odgłos kopyt, myśl o koniach, nie o zebrawach”, które oznacza, że diagnoza często polega na przyporządkowaniu objawów do najbardziej prawdopodobnego lub popularnego schorzenia. Lekarze rzadko kiedy mają czas, aby wykluczyć inne choroby. Wielu pacjentów musi czekać miesiącami na wizytę u spe-

cialisty. Z kolei AI jest zawsze pod ręką i potrafi wychwycić niuanse, które odróżniają rzadkie choroby od powszechnie występujących dolegliwości.

Badania naukowe sugerują, że duże modele językowe osiągają dokładność diagnoz porównywalną z ludźmi. W przypadku rzadkich schorzeń, AI często jest lepsza niż człowiek.

Czarne statystyki, gdy AI wprowadza w błąd

ChatGPT, Geminie, Perplexity, Claude czy Microsoft Pilot to produkty konsumenckie, które nie podlegają żadnym regulacjom. Nie są one walidowane jak urządzenia medyczne, ale mimo to przez pacjentów traktowane jako wiarygodne źródło danych. Według dostępnych badań, 1 na 5 pacjentów bardziej ufa rekomendacjom AI niż zaleceniom lekarzy.

Nieproporcjonalnie rzadziej pacjenci dzielą się historiami, jak AI wprowadziła ich w błąd. Takie teksty nie przyciągają jednak tak dużej uwagi, jak te o AI ratującej życie.

Mało kto wie, że przykładowo OpenAI zostało już wielokrotnie pozwane do sądu w związku ze szkodami psychicznymi wyrządzonymi pacjentom szukającym pomocy. Pod koniec 2025 roku głośna była sprawa 23-latka z Teksasu, którego ChatGPT miał zachęcić do popełnienia samobójstwa. W podobnym przypadku 16-latka z Kalifornii, OpenAI argumentował, że przyczyną było nieprawidłowe korzystanie z ChatGPT.

Na forach internetowych pojawiają się relacje o błędnych sugestjach prowadzących do napadów paniki czy hospitalizacji. Jeden z użytkowników przez osiem miesięcy codziennie sprawdzał objawy, przekonany przez AI o chorobie zwyrodnieniowej kręgosłupa. Błędne diagnozy to jedno. Drugie to wywoływanie niepokoju oraz generowanie niepotrzebnych wizyt u lekarza.

„The Guardian” przeprowadził śledztwo, które wykazało, że generowane przez AI podsumowania wyświetlane w wyszukiwarce Google w ramach funkcji AI Overview zawierają fałszywe i wprowadzające w błąd informacje zdrowotne, a w nie-

» OpenAI ma kilka spraw sądowych w związku ze szkodami psychicznymi lub zdrowotnymi wyrządzonymi pacjentom szukającym pomocy.«

których przypadkach mogą być niebezpieczne. Dziennikarze zidentyfikowali m.in. „całkowicie błędne” porady żywieniowe dla chorych na raka trzustki, które eksperci określili jako „bardzo niebezpieczne” i niezgodne z zaleceniami klinicznymi. Błędne informacje dotyczyły także badań przesiewowych w kierunku nowotworów u kobiet oraz interpretacji testów wątrobowych, co mogło prowadzić do fałszywego poczucia bezpieczeństwa i zniechęcać do konsultacji lekarskiej.

Google w odpowiedzi podkreślił, że „zdecydowana większość” podsumowań jest rzetelna i że firma stale poprawia jakość systemu. Także OpenAI wie, że jego narzędzie nie jest idealne. Firma powołała nawet *Global Physician Network*, zrzeszającą 300 lekarzy i psychologów, aby zwiększać bezpieczeństwo swoich modeli.

Ale to, że AI nie jest narzędziem diagnostycznym, nie ma znaczenia. Użytkownicy widzą w AI magiczne narzędzie, które wie wszystko. Jego moc rośnie wraz z tym, jak systemy zdrowia pogrążają się w coraz większym kryzysie – kolejki do lekarzy rosną, lekarze muszą przyjmować coraz więcej chorych, brakuje czasu na rozmowę i empatię. AI robi dużo dobrego, dając pacjentom do rąk narzędzie samoleczenia. Ale nadal wyrządza też krzywdę. ●

reklama

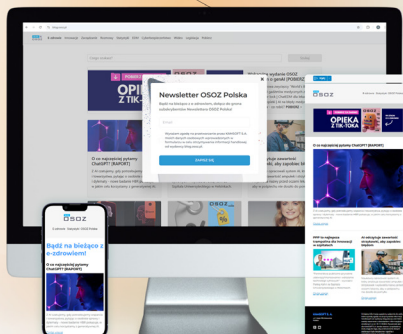
Newsletter OSOZ Polska

BLOG
OSOZ

Nie przegap nowości z blog.OSOZ.pl!

Bądź na bieżąco z e-zdrowiem.
Dołącz do grona subskrybentów
i dowiedz się, co ważnego dzieje
się w cyfryzacji ochrony zdrowia
w Polsce.

DOŁĄCZ DO NAS!



blog.osoz.pl



KAMSOFTESTUJE NOWY Portal Pacjenta. „Skorzysta personel rejestracji i pacjenci”

Rejestracje w podmiotach zdrowia toną w pracy administracyjnej i telefonach od pacjentów. Tymczasem wiele spraw pacjenci mogliby załatwić samodzielnie przez internet. KAMSOF zaprezentował nowy Portal Pacjenta, który ma zmniejszyć obciążenia organizacyjne, przenosząc proste czynności związane z obsługą pacjentów do kanału online i umożliwiając wygodną interakcję z podmiotem zdrowia.

Łatwiejszy i szybszy kontakt pacjenta z placówką bez konieczności zwiększania etatów

Portal Pacjenta umożliwia intuicyjne korzystanie z usług medycznych bez konieczności kontaktu telefonicznego czy osobistej wizyty w przychodni. Dzięki Portalowi Pacjenta pacjent może samodzielnie:

- umówić lub odwołać wizytę u lekarza. System prezentuje dostępne terminy zgodnie z aktualnym grafikiem placówki;
- zamówić receptę na leki na kontynuację leczenia, stosowane w chorobach przewlekłych. Pacjent składa wniosek online; lekarz go akceptuje bez udziału rejestracji i bez konieczności wizyty stacjonarnej;
- sprawdzić wyniki badań. Wyniki publikują się automatycznie po ich zatwierdzeniu w placówce;
- uzyskać dostęp do historii wizyt i dokumentacji medycznej. Wszystkie informacje są dostępne w jednym miejscu, bez potrzeby dzwonienia z pytaniami.

Odciążenie personelu i oszczędność czasu

Wdrożenie Portalu Pacjenta to nie tylko korzyści dla pacjentów, ale także dla placówek zdrowia. Wśród nich są m.in.:

- mniejsza liczba połączeń telefonicznych dotyczących zapisów czy przepisania recept,
- mniej wizyt „po receptę”, które generowały kolejki i zajmowały czas lekarzom,
- mniejsza liczba tzw. *no-shows*, czyli wizyt niezrealizowanych z powodu niestawienia się pacjenta, dzięki automatycznym powiadomieniom oraz możliwości łatwego odwołania terminu jednym kliknięciem.

Przeniesienie części procesów na pacjenta i umożliwienie mu wygodnej samoobsługi odciażają personel placówki z trzech najczęściej powtarzających się czynności: rejestracji wizyt, obsługi wizyt „po receptę” oraz udzielania podstawowych informacji, np. o wynikach badań.

– Dla coraz większej grupy pacjentów cyfrowe kanały obsługi są standardem, a nie dodatkiem. Nowy Portal Pacjenta

» Dzięki Portalowi Pacjenta chorzy mają łatwy dostęp do swoich danych medycznych – wizyt, recept, wyników badań i zaleceń – zgromadzonych w jednym miejscu.«

odpowiada na te oczekiwania, jednocześnie realnie odciążając personel. To narzędzie, które pozwala placówkom budować nowoczesną, zorientowaną na pacjenta obsługę – mówi Tomasz Latko, Dyrektor Techniczny Wydziału Rozwoju KAMSOF S.A.

Portal Pacjenta buduje pozytywny wizerunek placówki

Cyfryzacja w ochronie zdrowia to, oprócz usprawnienia pracy, także ważny element przewagi konkurencyjnej. Placówki oferujące pacjentom nowoczesne narzędzia online są postrzegane jako lepiej zorganizowane, dostępne i dbające o czas i wygodę swoich pacjentów.

Dzięki Portalowi Pacjenta chorzy mają łatwy dostęp do swoich danych medycznych – wizyt, recept, wyników badań i zaleceń – zgromadzonych w jednym miejscu. To buduje poczucie bezpieczeństwa, większą kontrolę nad procesem leczenia i wrażenie indywidualnej troski. W efekcie pacjenci czują się lepiej „zaopiekowani”, co przekłada się na większe zaangażowanie i lojalność wobec placówki.

Nowy wygląd, większe możliwości

Opracowując nową wersję Portalu Pacjenta, postawiono na przejrzystość, nowoczesność oraz możliwość dopasowania narzędzia do specyfiki konkretnej placówki. Wśród nowych funkcjonalności i cech znajdują się:

- odświeżona, intuicyjna szata graficzna,
- rozszerzone możliwości konfiguracji – moduły i usługi można dostosować do oferty placówki (np. opcja sprzedaży usług komplementarnych),
- personalizacja elementów wizualnych,
- większy nacisk na ergonomię i łatwość obsługi zarówno dla pacjenta, jak i administratorów (proste i szybkie wdrożenie rozwiązania).

Trwa pilotaż, wkrótce premiera

Wybrane placówki testują nowe funkcje Portalu Pacjenta, a ich opinie pomogą dopracować narzędzie przed szerszym wdrożeniem. To ważny etap, który pozwala rozwijać Portal

w oparciu o realne potrzeby użytkowników oraz codzienne doświadczenia pracy personelu i pacjentów.

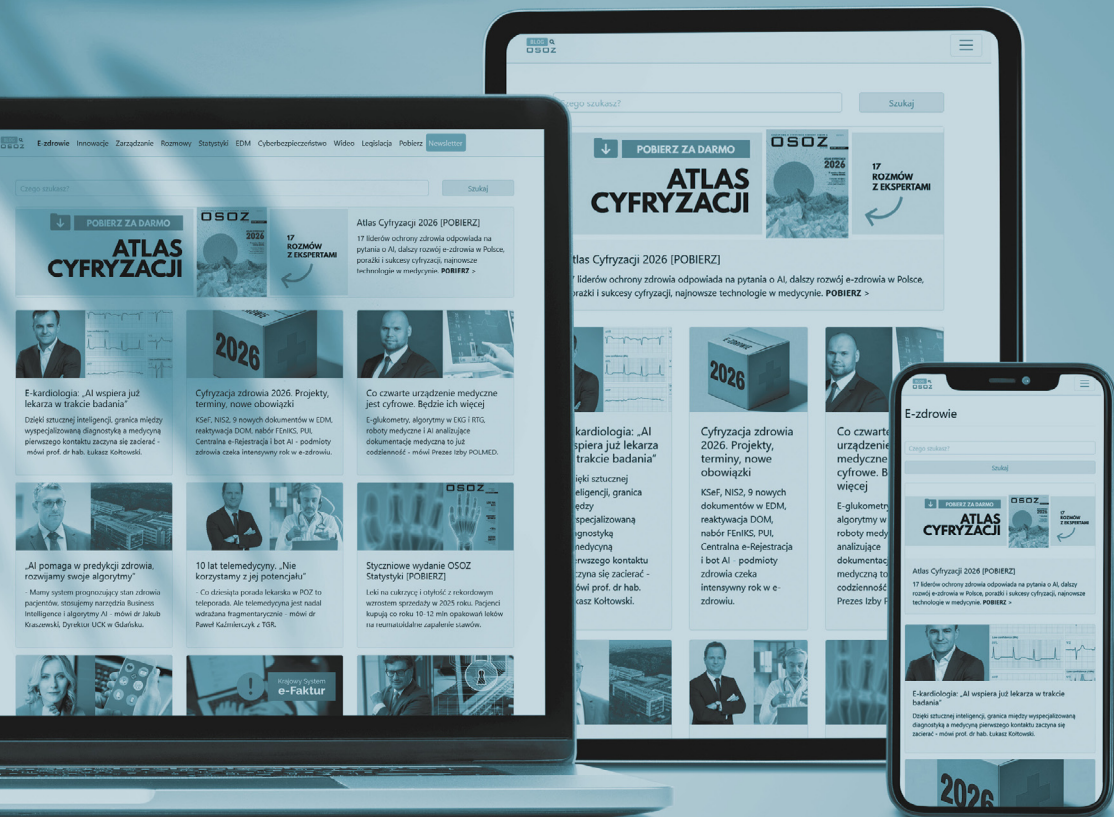
Portal Pacjenta będzie dostępny jako moduł dla placówek korzystających z systemów KAMSOF, a jego uruchomienie po stronie podmiotu medycznego nie będzie wymagało dodatkowych nakładów pracy ani czasochłonnych zmian organizacyjnych.

Portal Pacjenta jest kolejnym elementem ekosystemu OSOZ, którego centrum stanowi pacjent. Rozwiązanie uzupełnia znaną i cenioną przez pacjentów aplikację mobilną VisiMed, dzięki której pacjenci mogą załatwiać sprawy zdrowotne również z poziomu smartfona. VisiMed tym głównie różni się od Portalu Pacjenta, że daje dostęp do wielu placówek jednocześnie, zaś Portal Pacjenta pozwala na uzyskanie danych medycznych, które nie są w tak szerokim zakresie możliwe do udostępnienia w VisiMed. Obie aplikacje tworzą spójny duet, uzupełniając się nawzajem.

Zarówno w Portalu Pacjenta, jak i aplikacji VisiMed, dostęp 24/7 sprawia, że pacjent załatwia swoje sprawy wtedy, kiedy najbardziej mu wygodnie, bez ograniczeń czasowych, czekania w kolejkach czy konieczności kontaktu z rejestracją. ●

Testowy widok Portalu
Pacjenta KAMSOF-u

The screenshot displays the 'Zaplanuj wizytę' (Book appointment) section of the KAMSOF Patient Portal. At the top, there are navigation links: 'O nas', 'Kontakt', and 'Rejestracja on-line'. A 'Zaloguj się' (Log in) button is in the top right corner. Below the navigation bar is a banner image showing a person using a laptop. The main section is titled 'Zaplanuj wizytę' and includes search filters for 'Lekarz / Gabinet' (set to 'MALINA ANDRZEJ'), 'Usługa' (set to 'PRZYCHODNIA MOBILNA'), and 'Lokalizacja' (set to 'PRZYCHODNIA MOBILNA'). A 'Szukaj' (Search) button is on the right. Below the filters, a card for 'MALINA ANDRZEJ, LEKARZ - SPECJALISTA PSYCHIATRII, LEKARZ - SPECJALISTA MEDYCZNY RODZINNEJ' is shown. Underneath, 'Najbliższe wolne terminy' (Next available times) are listed in three columns: 'Wizyta prywatna' (Private visit), 'Wizyta na NFZ' (Visit on NFZ), and 'Wizyta abonencka' (Subscription visit). Each column shows the date 'poniedziałek, 9 lutego 2026' and the time '13:30' or '16:00'. There are 'Zarezerwuj' (Book) and 'W więcej' (See more) buttons for each time slot. At the bottom, there are icons for 'Telewizja', 'Porada telefoniczna', and 'Porada stacjonarna'. A footer section contains contact information for 'PRZYCHODNIA MOBILNA' and a 'Kontakt' (Contact) button.



Wszystko o e-zdrowiu

Praktyczne porady
Informacje z rynku zdrowia
Inspirujące wywiady



ZESKANUJ KOD,
aby przejść do bloga



OTWARTY SYSTEM OCHRONY ZDROWIA

OSOZ

Wydawca:
KAMSOF S.A.
40-235 Katowice, ul 1 Maja 133
tel. +48 32 209-07-05
fax +48 32 209-07-15
e-mail: czasopismo@osoz.pl

Redaktor naczelny: Artur Olesch



Jesteśmy partnerem
European Connected Health Alliance

Zespół redakcyjny:
Zygmunt Kamiński,
Agnieszka Golec,
Aleksandra Kurowska,
Katarzyna Płoskonka,
Bożena Wojnarowicz-Głuszek.

Współpracownicy:
Mark Hoffmann,
Patrik Kuchta.

Skład i łamanie: Piotr Chamera

Przedruk, kopiowanie, skracanie, wykorzystanie
tekstów (lub ich fragmentów) publikowanych
w czasopiśmie OSOZ bez zgody wydawcy
KAMSOF S.A. jest zabronione.

Redakcja nie odpowiada za treść reklam,
ogłoszeń i artykułów sponsorowanych.