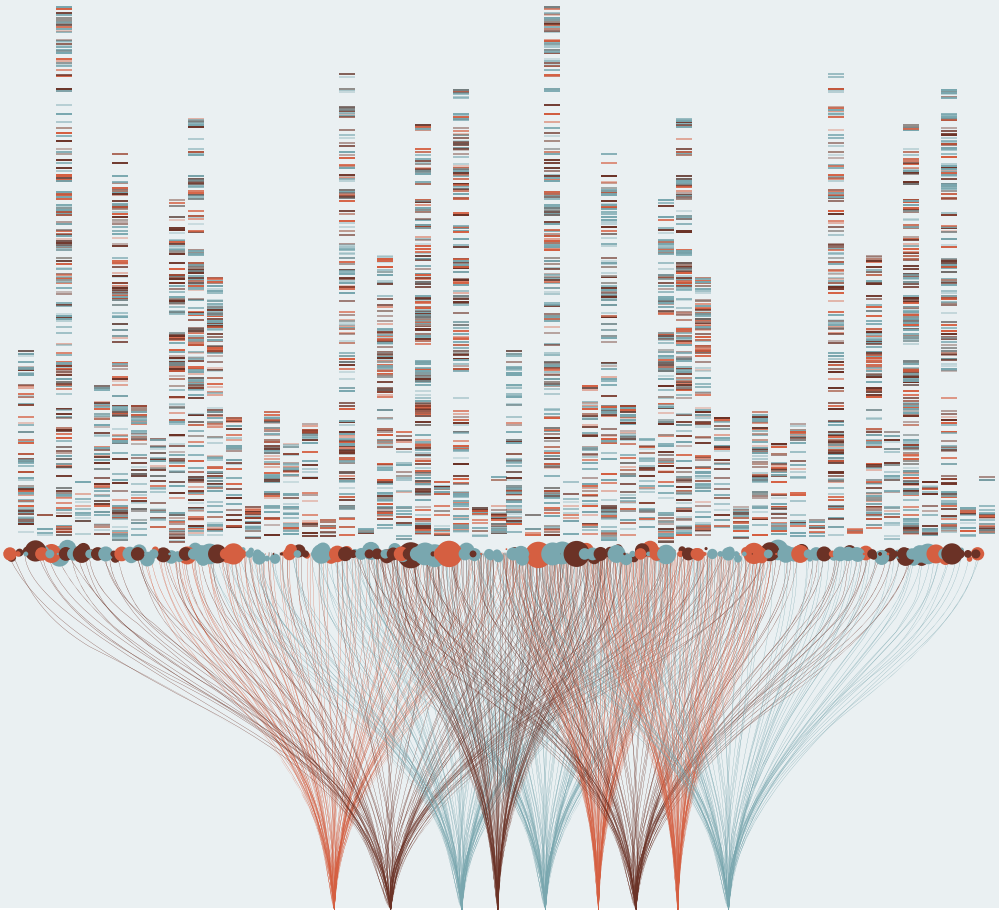


Cyfryzacja zdrowia

W INTERESIE SPOŁECZNYM

RAPORT | WARSZAWA 2023

Okręgowa Izba Lekarska w Warszawie
im. prof. Jana Nielubowicza.
ul. Puławska 18,
02-512 Warszawa

Raport zakończono w marcu 2023 roku.

Redakcja:
Maria Libura
Tomasz Imiela
Dagmara Głód-Śliwińska

Autorzy:
Michał Bedlicki
Michał Florczak
Maria Libura
Maciej Malenda
Marta Musidłowska
Artur Olesch
Anna Padiasek
Sebastian Sikorski
Jacek Sztajnke
Magdalena Władysiuk
Jan Zygmuntowski

Korekta:
Lidia Sadowska-Szlaga

Opracowanie graficzne:
Katarzyna Kapcia
Arkadiusz Galiński

Cytowanie raportu:
Libura M. (red.), Imiela T. (red.), Głód-Śliwińska D. (red.), *Cyfryzacja zdrowia w interesie społecznym*. Warszawa, Okręgowa Izba Lekarska w Warszawie, 2023.

ISBN 978-83-940620-7-1

OKRĘGOWA
IZBA LEKARSKA
W WARSZAWIE
im. prof. Jana Nielubowicza

Spis treści

Kluczowe pojęcia

Suwerenność cyfrowa	zdolność państw, organizacji międzynarodowych i każdego użytkownika i użytkowniczki z osobna do egzekwowania swoich praw oraz wpływania na platformy cyfrowe i firmy technologiczne zgodnie z własnymi potrzebami społecznymi i rozwojowymi.
Interoperacyjność (w zdrowiu)	zapewnienie możliwości wymiany informacji pomiędzy podmiotami realizującymi zadania z zakresu ochrony zdrowia, lub pomiędzy tymi podmiotami a ich klientami dzięki ujednoliconym standardom i procedurom stosowanym przez te podmioty w celu wspólnego użytkowania.[1] Dzielimy ją na silną i słabą: » **Interoperacyjność słaba** – wymiana informacji jedynie w obrębie sektora publicznego między systemami stosowanymi w publicznej ochronie zdrowia; » **Interoperacyjność silna** – wymiana informacji o charakterze międzysektorowym i powszechnym, między innymi z urządzeniami medycznymi, klinikami prywatnymi, narzędziami naukowców, aplikacjami czy inteligentnymi sensorami.
Dostępność danych	brak barier uniemożliwiających pełne wykorzystanie danych zawartych w bazach i pewien z góry wyznaczony zakres możliwości ich wykorzystania dla uprawnionych podmiotów.
Transparentność danych	udzielenie pacjentowi łatwo dostępnych i zrozumiałych informacji dotyczących tego, co z jego danymi będzie się działo od momentu ich udostępnienia.
Cyfrowe nierówności w zdrowiu	różnice w dostępie, korzystaniu i skuteczności wykorzystania technologii cyfrowych w celu monitorowania stanu zdrowia, diagnozowania i leczenia chorób między różnymi grupami społecznymi. Mogą one wynikać z różnic w dostępie do sprzętu i infrastruktury technologicznej, umiejętności korzystania z technologii cyfrowych, wiedzy i świadomości zdrowotnej, jak również z różnic w poziomie edukacji, dochodach, wieku, płci czy pochodzeniu etnicznym.
Wspólnica danych zdrowotnych	instytucja umożliwiająca bezpieczne współużytkowanie i analizę danych zdrowotnych w interesie publicznym.

[1] *Standardy Krajowych Ram Interoperacyjności (KRI).* Portal Interoperacyjności i Architektury 2022, https://www.gov.pl/web/ia/standardy-krajowych-ram-interoperacyjnosci-kri (dostęp: 12.02.2022).

Wstęp

Czwarta rewolucja przemysłowa, która dokonuje się na naszych oczach dzięki technologiom cyfrowym, w coraz większym stopniu przekształca system ochrony zdrowia. Sektor ten początkowo z trudem i nie bez oporów przyjmował rozwiązania teleinformatyczne, ale pandemia COVID-19 gwałtownie przyspieszyła szeroko rozumianą cyfryzację opieki medycznej. W czasie jej trwania w Polsce e-recepty i e-zwolnienia oraz porady zdalne przeszły przyspieszone wdrożenie, ujawniając swoje zalety i wady. Dzięki temu niszowe dotąd tematy, takie jak trudny do przeceniania potencjał innowacji cyfrowych, przykuły uwagę szerszej opinii publicznej. Jednocześnie jak nigdy dotąd uwidoczniły się ryzyka e-rozwiązań, w szczególności w zakresie bezpieczeństwa pacjenta i odpowiedzialności zawodów medycznych.

Cyfryzacja wpływa na każdy wymiar działania systemu ochrony zdrowia: zmienia sytuację pacjentów, pracę lekarzy i przedstawicieli innych zawodów medycznych, sposób realizacji świadczeń zdrowotnych, organizację pracy w szpitalach i poradniach, a także sposób kształtowania polityki zdrowotnej. Rośnie znaczenie danych i ich wykorzystania, co znajduje wyraz w upowszechnieniu elektronicznej dokumentacji medycznej i presji na tworzenie rejestrów medycznych. Coraz więcej danych o zdrowiu jest wytwarzanych i gromadzonych poza systemem ochrony zdrowia. Zarazem pojawia się pytanie o to, dla kogo i na jakich zasadach te informacje powinny być dostępne. Prywatność w czasach cyfryzacji nabiera nowego znaczenia, a jej ochrona wymaga nowych rozwiązań wypracowanych w ramach dialogu społecznego. W szczególności dotyczy to danych o zdrowiu, ze względu na ich szczególnie wrażliwy charakter.

Gromadzenie danych w formie cyfrowej otwiera szerokie możliwości ich zastosowania na wielu polach związanych z medycyną oraz organizacją opieki medycznej. Tworzenie rozwiązań cyfrowych prowadzi do powstania kompleksowych, integralnych rozwiązań systemowych, pozwalających na współpracę na linii pacjent – świadczeniodawca, z koordynacją na poziomie centralnym lub lokalnym. Cyfryzacja wymaga od władz publicznych wypracowania elastycznych strategii i planów rozwoju w ciągle zmieniających się warunkach, z uwzględnieniem potrzeb poszczególnych interesariuszy, ale przede wszystkim interesu społecznego.

Niniejszy raport powstał, by podkreślić wagę tego ostatniego w projektowaniu i wdrażaniu e-zdrowia. Żyjemy w społeczeństwie informacyjnym, w którym narzędzia cyfrowe i wirtualne środowisko są czynnikami, które należy uwzględniać w politykach społecznych. Testowane w systemach ochrony zdrowia na całym świecie, rozwiązania cyfrowe mają w zamyśle zwiększyć efektywność oraz poprawić jakość świadczeń medycznych. Dotychczasowe doświadczenia z wdrażaniem e-zdrowia wskazują jednak, że narzędzia te, wprowadzane bez odpowiedniego przygotowania, mogą generować skutki odwrotne od zamierzonych. Elektroniczna historia pacjenta nie powinna być dodatkowym obciążeniem administracyjnym, pochłaniającym czas lekarza przeznaczony dla pacjentów. Gromadzenie danych nie może być celem samym w sobie. Wartość danych zależy od ich wykorzystania w procesie podejmowania decyzji tak, by zmieniły na lepsze codzienną praktykę funkcjonowania opieki medycznej, czyniąc ją skuteczniejszą i bardziej przyjazną dla pacjentów i medyków. W przypadku inwestycji w infrastrukturę i oprogramowanie cyfrowe kapitalne znaczenie ma odpowiednia koordynacja wydatków na ten cel i ujednolicenie standardów, by zapewnić bezpieczeństwo i nie uzależniać się od jednego dostawcy. Algorytmy sztucznej inteligencji, trenowane na stronniczych lub niekompletnych bazach danych, pogłębiają istniejące nierówności w zdrowiu oraz wytwarzają nowe, często początkowo trudne do identyfikacji obszary wykluczenia i dyskryminacji. Także i w tym obszarze potrzebne są pilnie regulacje uwzględniające zupełnie nowy kontekst „nie-ludzkich" narzędzi wspomagających podejmowanie decyzji.

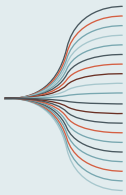
Mamy nadzieję, że niniejszy raport przesunie dyskusje nad cyfryzacją zdrowia z czysto technicznych rozważań o interoperacyjności w stronę refleksji nad konsekwencjami społecznymi podejmowanych przez władze publiczne wyborów. Technologie nas nie zbawią – one są narzędziem, które będzie na tyle użyteczne, na ile potrafimy się nim rozważnie posłużyć.

TOMASZ IMIELA

MARIA LIBURA

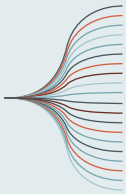
Rekomendacje

Kluczowym aspektem rozwoju społeczeństwa cyfrowego jest zaufanie obywateli do systemu publicznego, za który odpowiadają władze publiczne. Zależy ono od właściwie wytyczonych celów cyfryzacji, opisujących je ram prawnych, w szczególności mechanizmów ochrony prywatności danych zdrowotnych, które uważane są za szczególnie wrażliwe, a przede wszystkim od ich przestrzegania i rzeczywistego zastosowania. Zaufanie wymaga dialogu społecznego, szczególnie w okresie głębokiej transformacji systemu zdrowia, która czeka nas w najbliższej przyszłości.



1

Cyfryzacja ma służyć interesowi społecznemu: poprawie jakości opieki zdrowotnej, czyli uzyskiwaniu lepszych wyników opieki i poprawy bezpieczeństwa pacjentów, oraz sprawniejszej organizacji pracy personelu medycznego.

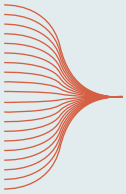


2

Gromadzenie danych nie może być celem samym w sobie. Kluczowe jest, by w oparciu o zgromadzone dane politycy, organizatorzy ochrony zdrowia i sami medycy podejmowali decyzje zmieniające codzienną praktykę funkcjonowania opieki medycznej.

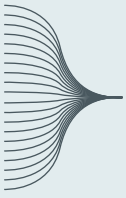
3

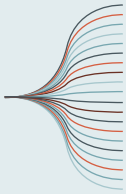
Cyfryzacja ochrony zdrowia musi się opierać na zasadach projektowania zorientowanego na użytkownika, a wdrażane rozwiązania powinny charakteryzować się wysokim poziomem użyteczności i wygody użytkownika.



4

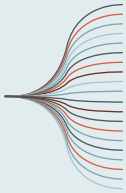
Konieczne jest uregulowanie kwestii odpowiedzialności za błędy i zdarzenia niepożądane wynikające z pracy urządzeń cyfrowych i algorytmów.





5

Potrzebne jest wypracowanie standardów technicznego rozwoju sztucznej inteligencji (AI), z równoczesnym dostosowaniem ram prawnych do nowych „nie-ludzkich" wzorców dyskryminacji generowanych przez algorytmy. Należy jednoznacznie podkreślić konieczność pozostawienia zawsze ostatecznej decyzji – poprzez wykonywany nadzór – w rękach człowieka.

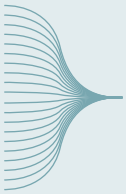


6

Utworzenie tzw. piaskownic regulacyjnych pozwoli stworzyć kontrolowane środowisko, w którym rozwiązania z dotyczące nowych wyzwań, takich jak AI i inne innowacyjne rozwiązania, będą bezpiecznie testowane. Ze względu na tempo postępu technicznego ważne jest monitorowanie wprowadzanych rozwiązań, aby prawodawca mógł w odpowiednim czasie reagować na nieznane dotąd wyzwania.

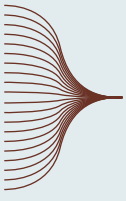
7

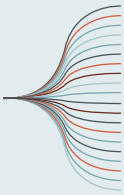
Należy uregulować zasady wykorzystania zasobów danych i wybierania dostawców chmurowych i oprogramowania, w tym przez zakupy grupowe. Obecnie dokonywanie wyborów infrastruktury i oprogramowania cyfrowego odbywa się często w sposób chaotyczny, a wydatki na cyfryzację ponoszone są na trzech różnych płaszczyznach: centralnej, regionalnej i lokalnej. Należy odpowiednio skoordynować wydatki na ten cel w taki sposób, by ujednolicić standardy, zapewnić bezpieczeństwo i uniezależnić się od jednego dostawcy (*vendor lock-in*).



8

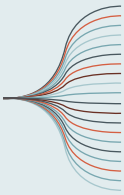
Należy utworzyć wspólnicę danych zdrowotnych. Rozwój nowoczesnych rozwiązań leczniczych jest uzależniony od dostępu do danych. W odpowiedzi na te potrzeby i presję ze strony regulatora (unijny projekt EHDS) konieczne jest stworzenie polskiej wspólnicy danych zdrowotnych – zaufanej przestrzeni współużytkowania i dostępu do danych zdrowotnych. Taka instytucja powinna powstać w modelu publicznym, jednak umożliwiając społeczną kontrolę nad dostępem do danych i korzystanie z praw obywateli do zarządzania danymi.





9

Dostęp do łączy szerokopasmowych oraz fizyczną i finansową dostępność urządzeń pozwalających na swobodne korzystanie z narzędzi cyfrowych należy uznać za prawa pacjenta i obywatela, gdyż cyfrowe uwarunkowania zdrowia nabierają coraz większego znaczenia.



10

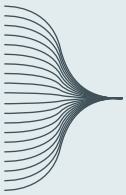
Obywatele powinni mieć możliwość dochodzenia praw w **ramach przejrzystych procedur antydyskryminacyjnych**, uwzględniających cyfrowe uwarunkowania zdrowia. Zwalczanie dyskryminacji cyfrowej wymaga też większej przejrzystości istniejących baz danych, gromadzenia dodatkowych danych, by nie dopuścić do nierównego traktowania grup defaworyzowanych, jak również monitorowania zbiorów swoich danych pod kątem ich stronniczości.

11

Konieczna jest rozbudowa systemu inwestycji w polskie firmy cyfrowe albo inicjatywy typu *start-up* (naukowe, informatyczne, szkoleniowe, konsultingowe) w celu wsparcia polskiej nauki i gospodarki.

12

Należy wypracować spójny proces refundacji, wdrażania oraz monitorowania rozwiązań i technologii cyfrowych w opiece zdrowotnej pod kątem skuteczności i bezpieczeństwa pacjenta oraz opłacalności.



Mapa raportu

1 Stan obecny

zobacz:
- **00** Wprowadzenie
- **01** Transformacja cyfrowa
- **02** Zastosowanie cyfryzacji w opiece zdrowotnej
- **03** Wyzwania rozwoju cyfryzacji w ochronie zdrowia

PRZEGLĄD SYTUACJI

Szanse i wyzwania związane z cyfryzacją zdrowia, możliwe kierunki rozwoju opieki cyfrowej, polityka zdrowotna oparta na danych

Rozwiązania cyfrowe w zakresie opieki zdrowotnej oraz społecznej są i będą jednym z głównych narzędzi (obok konwencjonalnych technologii medycznych) poprawy zdrowia obywateli

Od czego zależy zdrowie w społeczeństwie informacyjnym?

SZANSE, KTÓRE NIESIE CYFRYZACJI ZDROWIA

- wzrost efektywności i jakości opieki medycznej
- wsparcie decyzji klinicznych
- e-narzędzia samoopieki
- poprawa koordynacji opieki
- lepszy przepływ informacji

Jak cyfryzacja wpłynie na pracę lekarza i przedstawicieli innych zawodów medycznych?

stworzenie stabilnego publicznego ekosystemu cyfrowego

Kluczowym aspektem rozwoju społeczeństwa cyfrowego jest zaufanie obywateli do systemu publicznego

Jednym z najbardziej istotnych aspektów jest tworzenie bezpiecznego dostępu obywateli do danych dotyczących zdrowia oraz ich wymiana, a także rozwój narzędzi cyfrowych na rzecz wzmacniania pozycji obywateli i zapewnienia opieki skoncentrowanej na pacjencie

WYZWANIA CYFRYZACJI ZDROWIA

odpowiedzialność w erze automatyzacji decyzji

zagrożenia prywatności

zapewnienie równego dostępu do świadczeń zdrowotnych

Co zrobić, by pacjent był w centrum cyfrowej transformacji?

2 Suwerenność cyfrowa

zobacz:
- **04** Suwerenność cyfrowa w ochronie zdrowia
- **05** Zarządzanie danymi dotyczącymi zdrowia

Czym jest suwerenność cyfrowa i jak ją osiągnąć za pomocą polityki zamówień publicznych i odpowiedniego zarządzania danymi w ochronie zdrowia?

Suwerenność cyfrową można osiągnąć przez inwestowanie w promocję lokalnych rozwiązań chmurowych przez sektor publiczny oraz ułatwianie dostępu do informacji o modelach zarządzania danymi

- zasady tworzenia cyfrowej infrastruktury w opiece zdrowotnej
- zachowanie publicznej kontroli nad systemem
- minimalizacja ryzyka negatywnych zjawisk (uzależnienia od jednego dostawcy rozwiązań czy niekontrolowanego użycia danych przez podmioty komercyjne)

ZARZĄDZANIE DANYMI

Aby efektywnie zarządzać danymi w sektorze medycznym, konieczne jest zapewnienie współistnienia trzech komponentów:

- interoperacyjności
- dostępności
- transparentności

W jaki sposób zbierać, przetwarzać i udostępniać dane dotyczące zdrowia przekazywane podmiotom świadczącym prywatnie/publicznie usługi medyczne aby zapewnić ich dostępność, interoperacyjność i transparentność oraz aby maksymalizować użyteczność danych w podejmowaniu decyzji?

Interoperacyjność (w zdrowiu) – zapewnienie możliwości wymiany informacji pomiędzy podmiotami realizującymi zadania z zakresu ochrony zdrowia lub pomiędzy tymi podmiotami a ich klientami dzięki ujednoliconym standardom i procedurom stosowanym przez te podmioty w celu wspólnego użytkowania (Portal Interoperacyjności i Architektury, 2022)

3 Społeczny wymiar cyfrowej transformacji

zobacz:
- **06** Cyfryzacja a bezpieczeństwo opieki medycznej
- **07** Cyfrowe nierówności w zdrowiu
- **08** Sztuczna inteligencja w ochronie zdrowia oraz standardy telemedyczne

Jak w dobie informatyzacji dbać o bezpieczeństwo danych w ochronie zdrowia? Jak cyfrowa transformacja wpływa na równość w dostępie do opieki? Jakie szanse i zagrożenia niesie ze sobą sztuczna inteligencja?

Szybko wprowadzane cyfrowe technologie zdrowotne zakładają powszechność dostępu do Internetu i urządzeń mobilnych, marginalizując osoby, które mają trudności w korzystaniu z nowych technologii

Z perspektywy praw pacjenta niezwykle istotne jest, aby systemy oparte na AI gwarantowały prawo do informacji oraz respektowały wolę pacjenta w zakresie dostępu do informacji

Około 50% czasu wizyty pacjenta lekarz spędza przed komputerem, wprowadzając dane i generując dokumentację. Aby system IT pomagał w pracy zamiast prowadzić do frustracji, trzeba przyjrzeć się z bliska elementom wpływającym na efektywność i płynność jego obsługi

4 Innowacje

Jak powinien być zaprojektowany system i dlaczego innowacje są ważne? Jakie korzyści niesie Paszport Pacjenta z chorobą rzadką?

zobacz:
- **09** Wygoda użytkownika
- **10** Cyfryzacja ochrony zdrowia a innowacje
- **11** Paszport Pacjenta z chorobą rzadką

01

Transformacja cyfrowa

MAGDALENA WŁADYSIUK

Prezes Stowarzyszenia CEESTAHC oraz wiceprezes firmy HTA Consulting, lekarz (Akademia Medyczna w Lublinie), absolwent ekonomii i manager (MBA na WSPiZ im. L. Koźmińskiego w Warszawie), Departament Epidemiologii i Medycyny Prewencyjnej UJ

Społeczeństwo informacyjne a transformacja cyfrowa

Społeczeństwo informacyjne to społeczność opierająca swój rozwój gospodarczy oraz wpływ na rzeczywistość na informacjach (danych) i wiedzy. Rozwój cywilizacyjny i nowoczesne rozwiązania techniczne pozwoliły na przestawienie gospodarki z produkcyjnej na opartą na usługach, w tym cyfrowych. Technikę wykorzystuje się do automatyzacji czynności, komunikacji, magazynowania oraz przekształcania informacji, a także wspierania procesów, również decyzyjnych. Pozwala to na poprawę wygody i funkcjonalności wielu z nich.[2] Jednocześnie transformacja ta stwarza nowe wyzwania gospodarcze i społeczne, które wymagają wypracowania odpowiednich ram prawnych, zaangażowania społeczeństwa obywatelskiego w kształtowanie powstającego na naszych oczach cyfrowego środowiska, a także pogłębionego zrozumienia i redefinicji roli instytucji publicznych stojących na straży interesu społecznego.

W Polsce w 2022 r. odsetek osób w wieku od 16 do 74 lat zamawiających przez Internet towary lub usługi do użytku prywatnego w ciągu ostatnich 12 miesięcy wyniósł 64,6%, i jest to o 3,4 p. proc. więcej niż w roku poprzednim.[3] Jednocześnie ma to prowadzić do poprawy komunikacji i ochrony środowiska. W 2022 r. blisko połowa przedsiębiorstw zapewniała swoim pracownikom zdalny dostęp do służbowych dokumentów. Aż 55% przedsiębiorstw stosowało procedury mające na celu redukcję zużycia papieru, a 43% ograniczało zużycie energii. **Wartość gospodarki opartej na danych jest w Polsce szacowana na 6,2 mld euro (1,2 proc. udziału w PKB), a w 2025 r. może już wynieść między 7,9 a 12 mld euro.**[4] Pomimo to Polska jest zaliczana do krajów o niskim poziomie cyfryzacji, plasując się dopiero na 24. miejscu spośród 27 ocenianych krajów UE. W Polsce wydatki na e-biznes stanowiły zaledwie 4,1% PKB, w porównaniu z 6–8% w Wielkiej Brytanii, Danii lub Szwecji.

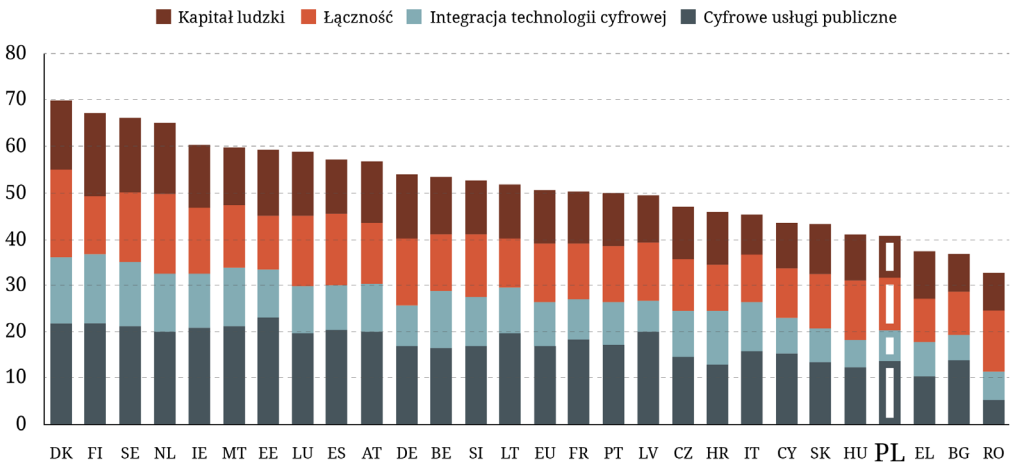
---

[2] Internetowe Konto Pacjenta – e-recepta https://pacjent.gov.pl/internetowe-konto-pacjenta/erecepta (dostęp: 1.05.2022).

[3] https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2022-roku,2,12.html

[4] *Analiza danych przyspieszy rewolucję w ochronie zdrowia*, 2020, https://biotechnologia.pl/technologie/analiza-danych-przyspieszy-rewolucje-w-ochronie-zdrowia,19459

WYKRES 1. RANKING INDEKSU GOSPODARKI CYFROWEJ I SPOŁECZEŃSTWA CYFROWEGO NA 2021 R.



W ostatnich pięciu latach, szczególnie w czasie pandemii COVID-19, doszło do znaczącego przyspieszenia procesu transformacji cyfrowej, także w zdrowiu. Według raportu Global Market Insights z 2018 r., do 2024 rynek cyfrowych technologii medycznych przekroczy 379 mld dol.[5] Szacowany przyrost wartości do 2030 r. może wynosić 17,9 proc. rocznie. Łączną ilość danych tworzonych na całym świecie prognozowano na 79 zetabajtów w 2021 r., z podwojeniem tej wartości do 2025 r.[6] Sama branża opieki zdrowotnej generuje już obecnie około 30 proc. światowego wolumenu danych.[7] Ta branża będzie sektorem o najszybszym wzroście ilości danych, ze skumulowaną roczną stopą wzrostu wynoszącą 36 proc. do 2025 r., czyli o 6 proc. szybszym niż w produkcji, o 10 proc. szybszym niż w usługach finansowych i o 11 proc. szybszym niż w obszarze mediów i rozrywki. W Polsce tylko w 2021 r. w systemie e-zdrowie zaraportowano 30 mln zdarzeń medycznych. W sumie do 2021 r. zostało zaraportowanych 91,5 mln zdarzeń medycznych, a każdego dnia generowany jest kolejny milion.[8]

Wraz z rozwojem społeczeństwa informacyjnego rozwój infrastruktury cyfrowej, zwiększenie potencjału wykorzystania zbieranych danych i dzięki temu poprawa funkcjonalności systemu staje się krytycznym obszarem opieki zdrowotnej, a szerzej – państwa.

---

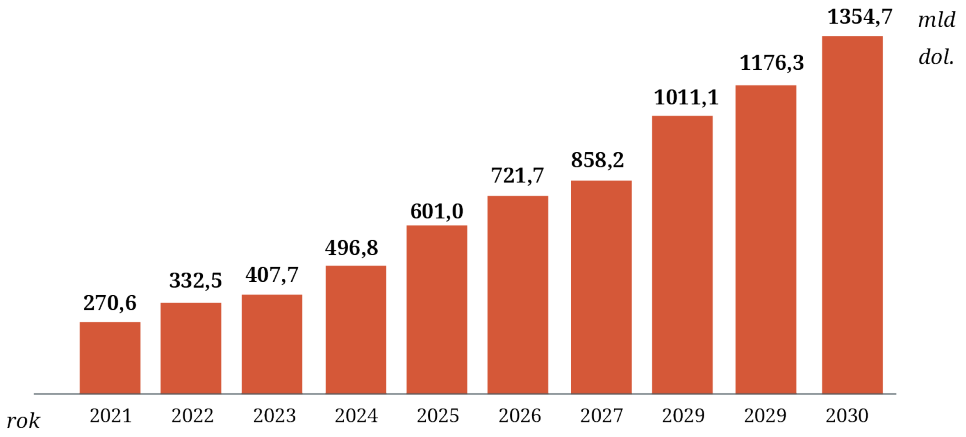
[5] Global Digital Health Market Growth Rate of 17.9 % over the Forecast Years 2022, https://www.biospace.com/article/global-digital-health-market-growth-rate-of-17-9-percent-over-the-forecast-years-2021-2030-/ (dostęp: 17.11.2022).

[6] https://www.harmonyhit.com/health-data-volumes-skyrocket-legacy-data-archives-rise-hie/

[7] The healthcare data explosion. Capital Markets, https://www.rbccm.com/en/gib/healthcare/episode/the_healthcare_data_explosion

[8] J. Dziekoński, *EDM – cyfrowa kopalnia wiedzy*, 2021, https://www.mp.pl/ezdrowie/baza-wiedzy/286226,edm-cyfrowa-kopalnia-wiedzy (dostęp: 17.11.2022).

WYKRES 2. PROGNOZOWANY WZROST CYFROWEGO RYNKU ZDROWIA W LATACH 2021–2030 (W DOL.)[9]



W celu osiągniecia niezależności i samowystarczalności technologicznej kraju oraz stworzenia przestrzeni dla cyfrowego zdrowia kluczowe jest zbudowanie stabilnego publicznego ekosystemu cyfrowego: strategicznego, politycznego, legislacyjnego, infrastrukturalnego, naukowego i edukacyjnego (dla utrzymania wysokiego poziomu skolaryzacji i alfabetyzmu funkcjonalnego społeczeństwa) oraz ochrony zasobów (w tym intelektualnych), co umożliwi dalszy rozwój i tworzenie innowacji. Priorytetem rozwoju społeczeństw, także w Polsce, staje się więc stworzenie takiego ekosystemu, prowadzącego do samodzielnej kontroli oraz decyzyjności w zakresie aspektów technologicznocyfrowych, który doprowadzi do suwerenności cyfrowej.

Obowiązek zapewnienia odpowiedniego standardu i dostępności świadczeń finansowanych ze środków publicznych (m.in. w oparciu o rozwiązania cyfrowe) spoczywa na władzach publicznych, które swoimi regulacjami obejmują także rynek prywatny. Zastosowanie mechanicznego i cyfrowego zapisu i rejestrowanie stanu fizycznego oraz doświadczeń pacjenta przygotowało grunt pod rewolucyjny postęp w możliwościach utrzymania zdrowia, samoopieki i leczenia na poziomie indywidualnym, strategiach zdrowotnych dla całej populacji oraz zintegrowanym generowaniu nowej wiedzy i spostrzeżeń w czasie rzeczywistym. Te rozwijające się zdolności, uzyskane dzięki rozwojowi technologii cyfrowych, nazywane są **zdrowiem cyfrowym. Cyfrowe zdrowie ewoluowało i dzisiaj**

[9] Digital Health Market Size, Growth, Trends, Report 2022–2030, https://www.precedenceresearch.com/digital-health-market.

jest szerokim pojęciem, obejmującym elektronicznie uzyskane dane z infrastrukturą oraz aplikacjami w ekosystemie opieki zdrowotnej. Rewolucyjne postępy w cyfrowym zdrowiu zmieniają medycynę i nauki biomedyczne oraz redefiniują i prowadzą do konstruowania narzędzi potrzebnych do zapewnienia zdrowszej przyszłości społeczeństwa. Polityka zdrowotna nakierowana powinna być więc nadal na osiąganie lepszych efektów zdrowotnych, jednak z zachowaniem określonego bezpieczeństwa zdrowotnego, m.in. przez zwalczanie nierówności w dostępie do opieki, błędów czy zagrożeń wynikających z funkcjonowania systemu w oparciu o integrację danych (np. duplikowanie, błędy zapisów lub działanie alertów). Wdrożenie określonych modeli cyfryzacji w obszarze zdrowia może sprzyjać suwerenności państwa w tym zakresie lub osłabiać ją. Przetwarzanie danych w chmurze, sztuczna inteligencja, uczenie maszynowe, blockchain, cyfrowa diagnostyka i leczenie, telezdrowie oraz mobilne aplikacje zdrowotne przeznaczone dla pacjentów są obecnie coraz częściej rutynowo wykorzystywane w opiece zdrowotnej i naukach biomedycznych.[10] Przy odpowiednich umiejętnościach cyfrowych (tzw. alfabetyzmie cyfrowym) zarówno kadry medycznej, jak i zarządzających, które są podstawowym fundamentem rozwoju, można poprawić wyniki zdrowotne przez zwiększenie zaangażowania pacjentów w dbanie o zdrowie na co dzień.

Przywództwo polityczne w dobie cyfryzacji nie obejmuje jedynie zapewnienia i rozdzielenia środków dla sektora ochrony zdrowia. Wręcz przeciwnie – dobra polityka zdrowotna polega na ustaleniu ram działalności i napędzaniu rozwoju w stabilnych warunkach politycznych, prawnych i finansowych oraz transparentności podejmowanych działań. Droga w kierunku cyfrowej transformacji jest jednak długa, obejmie nawet kilka dekad, co wprowadza konieczność koncentrowania się na pośrednich etapach rozwoju systemu. Pozwoli to ocenić wartość wdrażanych rozwiązań, a możliwości transformacji cyfrowej wciąż rosną. Transformacja cyfrowa w zdrowiu ma często charakter regionalny, a scentralizowane formy wdrażania cyfrowych rozwiązań w ochronie zdrowia występują w niewielu krajach. Wyważenie kapitalnej roli inicjatyw lokalnych i oddolnych z potrzebą wprowadzenia jednolitych standardów, interoperacyjności oraz uniknięcia pułapek związanych z niekorzystnym uzależnieniem od dostawców technologii stanowi kolejne wyzwanie cyfryzacji zdrowia.

W świetle prognozowanych zmian demograficznych,[11] Polska będzie coraz bardziej narażona także na deficyty kadry medycznej, zarówno w systemie publicz-

[10] McGinnis i in., 2021.

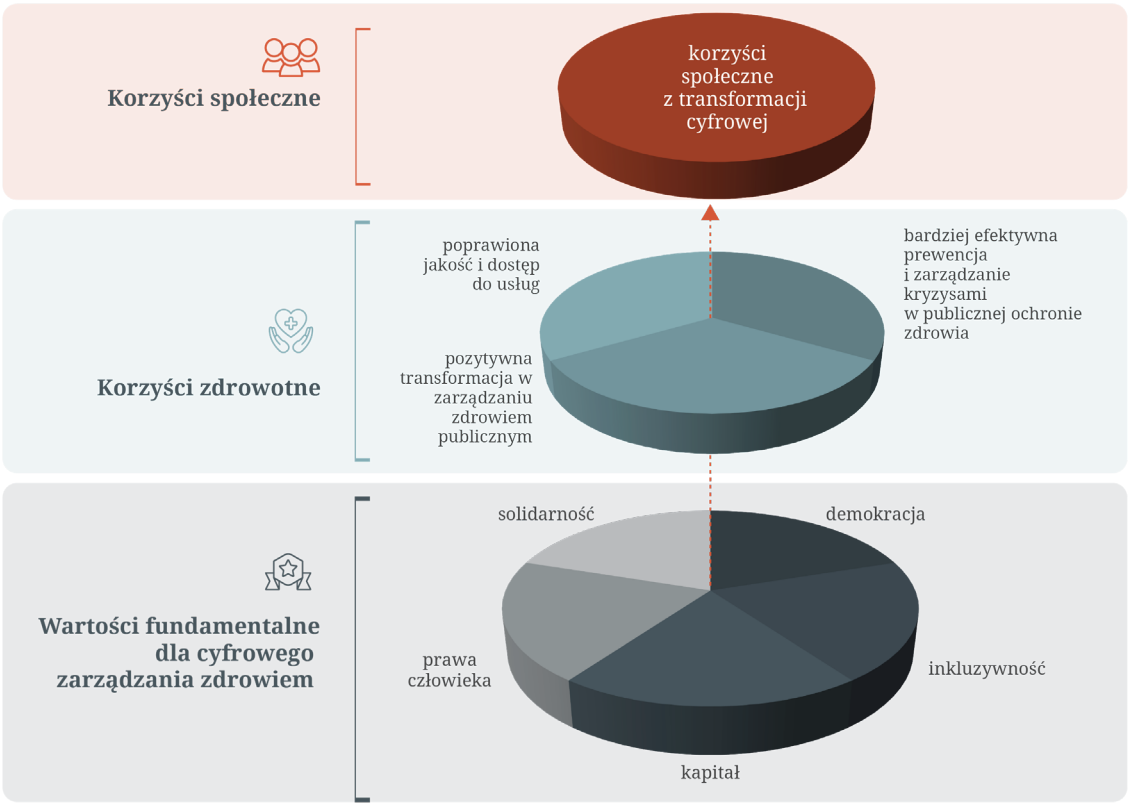
[11] GUS – prognozy demograficzne.

nym, jak i poza nim. Kluczowe jest także rozwinięcie zasobów związanych z informatyką medyczną oraz postępem nauki w tym obszarze, obok rozwoju infrastruktury, metod implementacji rozwiązań cyfrowych i metod ich finansowania.

Zaspokojenie zróżnicowanych potrzeb możliwe jest jedynie metodą ciągłej analizy funkcjonalności systemu, regulacji i zmian w zakresie świadczeń lub technologii w ramach koszyka świadczeń gwarantowanych, z zachowaniem zasad powszechności, solidaryzmu i równości.

Transformacja cyfrowa, jako element wspierający dostęp, realizację i zarządzanie świadczeniami medycznymi, musi podlegać ścisłym regulacjom prawnym, jednak równolegle ich stosowanie jest zależne od dojrzałości społeczeństwa i kultury organizacji, w tym liderów w opiece zdrowotnej. Wymaga to myślenia i planowania działań w dłuższej perspektywie, jako elementu zrównoważonego rozwoju kraju, a także odejścia od rozwiązań w oparciu o podejście projektowe.

RYSUNEK 1. KORZYŚCI Z ROZWOJU INFRASTRUKTURY CYFROWEJ W OCHRONIE ZDROWIA[12]



[12] The Lancet and Financial Times Commission on governing health futures 2030: growing up in a digital world 2021, https://www.thelancet.com/article/S0140-6736%2821%2901824-9/fulltext (dostęp: 22.11.2022).

Kluczowe trendy transformacji cyfrowej

Celem transformacji cyfrowej jest stworzenie inteligentnego systemu opieki zdrowotnej „Smart Health". Koncepcja inteligentnej opieki zdrowotnej wywodzi się z koncepcji „Smart Planet", zaproponowanej po raz pierwszy w 2009 r. przez IBM. Cyfryzacja staje się podstawą podejścia skoncentrowanego na pacjencie, optymalizuje procesy związane z opieką zdrowotną, usprawnia operacje i przyczynia się do budowania wzajemnego zaufania wszystkich interesariuszy opieki zdrowotnej. Idea inteligentnej opieki zdrowotnej wykorzystuje technologie informacyjne nowej generacji, w tym sztuczną inteligencję i duże zbiory danych.

Bez wątpienia jednym z najważniejszych osiągnięć współczesnych systemów opieki zdrowotnej jest wykorzystywanie transformacji cyfrowej jako drogi do poprawy funkcjonowania instytucji publicznych, świadczeniodawców i wsparcia pacjentów. Kadra medyczna z powodzeniem wykorzystuje elektroniczną dokumentację medyczną, rejestry, najnowsze technologie, oprogramowanie medyczne (m.in. *digital therapeutics*, modele predykcyjne), a nawet – coraz częściej – sztuczną inteligencję w podejmowaniu krytycznych decyzji medycznych. Cyfryzacja daje szansę na poprawę operacyjności systemu, przepływu informacji między jego interesariuszami, analizę danych oraz ich wizualizację. Podniesie to efekty zdrowotne oraz bezpieczeństwo pacjenta, a także ułatwi tworzenie cyfrowych technologii medycznych w celu diagnozowania, monitorowania i leczenia pacjentów (więcej w Rozdziale 2. Zastosowanie cyfryzacji w opiece zdrowotnej). Wśród trendów rozwoju rozwiązań cyfrowych na rynku, poza narastają liczbą aplikacji na smartfony, wskazać można rozwój tzw. medtechów (obejmujących wszystkie zdobycze techniki, które można zastosować do ratowania życia, profilaktyki czy też leczenia różnorodnych dolegliwości; MedTech to zarówno nowoczesne urządzenia diagnostyczne, jak i proste wyroby medyczne[13]), wprowadzających rozwiązania mające zastosowanie nie tylko w Polsce, ale i zagranicą.

Zarówno tworzenie zasobów *big data*, jak i coraz powszechniejsze, bardziej wszechstronne ich wykorzystywanie w opiece zdrowotnej jest jednym z głównych trendów w operowaniu na już zgromadzonych i przyszłych danych medycznych. Może to prowadzić do rzeczywistej poprawy jakości opieki medycznej, m.in. przez odchodzenie od modeli opieki doraźnej i jednorazowej na rzecz podejścia zorientowanego na łańcuch pomocy zintegrowanej i ciągłej, w tym medycyny

[13] M. Gołąbek, *MedTech, czyli technologia w służbie medycyny*, 2019, https://lifescience.pl/aktualnosci/medtech/ (dostęp: 23.11.2022).

zapobiegawczej. Duża liczba osób zgłaszających się na izbę przyjęć to powracający pacjenci. Mogą stanowić nawet 28 proc. trafiających tam osób. Analiza dużych zbiorów danych pozwoli ich zidentyfikować i stworzyć plany zapobiegawcze, aby powstrzymać pacjentów przed powrotem. Istotnym celem jest również zmniejszenie wskaźników błędów w opiece nad pacjentem. Dzięki analizie danych pacjentów oprogramowanie może oznaczać wszelkie nieprawidłowości w stanie zdrowia pacjenta, a także prowadzić analizę stosowanych leków czy technologii, a następnie wykorzystać systemy ostrzegające (alerty) dla pracowników służby zdrowia i pacjentów do przekazywania tych informacji. Wsparcie decyzyjne personelu i poprawa jakości opieki to również analizy predykcyjne dużych zbiorów danych, które umożliwią szpitalom i klinikom oszacować m.in. przyszłe wskaźniki przyjęć, co pozwoli tym placówkom przydzielić odpowiedni personel do obsługi pacjentów. Pozwala to zredukować koszty i skrócić czas oczekiwania na izbie przyjęć z powodu braku personelu. Dodatkowo analizy te mogą wspierać decyzje kliniczne kadry medycznej, także w oparciu o analizę danych genetycznych.

Urządzenia i aplikacje do monitoringu stanu zdrowia, m.in. *wearable medical device*, należą do najdynamiczniej rozwijających się cyfrowych rozwiązań na świecie. Szacuje się, że rynek urządzeń medycznych do noszenia przekroczy w 2023 r. wartość 27 mln dol., co stanowi spektakularny skok z niespełna 8 mln dol. w 2017. Zdalny monitoring stanu zdrowia, dzięki coraz nowocześniejszym urządzeniom domowego użytku, umożliwia zarówno wstępną diagnozę medyczną, jak i monitorowanie przebiegu chorób, także przewlekłych. Wspiera także rozwój medycyny spersonalizowanej. Dzięki takim urządzeniom w epoce cyfrowej pacjenci mają szansę koncentrować się na utrzymaniu stanu zdrowia i prewencji rozwoju choroby przez kontrolowanie np. aktywności fizycznej czy diety. *Wearable medical device* pozwalają również na właściwe reakcje kadry medycznej w odpowiednim czasie. Coraz większe zainteresowanie budzą technologie dotyczące oszacowania u pacjentów prawdopodobieństwa wystąpienia poważnego zdarzenia zdrowotnego. Jednocześnie rozwój tych technologii jest uważany za jeden z głównych kierunków poprawy wydajności systemu. Jedno z badań wykazało, że aplikacje zdrowotne i urządzenia ubieralne do opieki profilaktycznej mogą zaoszczędzić systemowi opieki zdrowotnej w USA blisko 7 mld dol. rocznie.

Równolegle z rozwojem *big data* oraz możliwości zbierania danych bezpośrednio od pacjenta dochodzi do **rozwoju sztucznej inteligencji.** Z założenia zadaniem AI jest doprowadzenie do przyspieszenia procesów i uproszczenia obsługi

świadczeń dla pacjentów, lekarzy i administracji, aby przebiegały szybciej i generowały niższe koszty.[14] Szerokie zastosowanie AI ma miejsce obecnie głównie w obszarze diagnostyki obrazowej (m.in. obrazowania nowotworów), badań nad nowymi lekami, genetyki/genomiki, wirtualnej komunikacji (np. wirtualni asystenci pacjenta i lekarza czy chatboty) oraz robotyzacji. Chatboty mogą pełnić wiele ról, od obsługi klienta po narzędzia diagnostyczne, a nawet zastępować terapeutów. Ich wszechstronność przekłada się na duże inwestycje. Już dzisiaj, dzięki zaawansowanemu rozpoznawaniu wzorców przez sztuczną inteligencję, pacjenci mogę mieć dostęp do spersonalizowanych terapii dostosowanych do ich genów i stylu życia. Co więcej, firmy farmaceutyczne i biotechnologiczne wykorzystują algorytmy uczenia maszynowego, aby skrócić cykl opracowywania leków. Już obecnie szacuje się, że sztuczna inteligencja skróci czas wczesnego odkrywania leków o cztery lata w stosunku do średniej w branży i wygeneruje oszczędności na poziomie 60 proc. Oczekuje się, że rynek narzędzi opartych na sztucznej inteligencji w opiece zdrowotnej do 2025 r. przekroczy 34 mld dol., co oznacza, że ta technologia będzie kształtować prawie wszystkie aspekty branży. Sam światowy rynek chatbotów opieki zdrowotnej zwiększy się z 122 mln dol. w 2018 r. do 314,3 mln dol. do 2023, a liczba aktywnych start-upów AI wzrosła już (od 2000 r.) 14-krotnie.

Elektroniczna dokumentacja medyczna (EHR) jest w zasadzie cyfrową wersją karty medycznej i zawiera wszystko, od danych osobowych, historii medycznej i diagnoz pacjenta po plany leczenia, daty szczepień i wyniki badań, również dane genetyczne. Dane zdrowotne są kluczowym zasobem zarówno obywatela, jak i państwa, a dokumentacja medyczna stanowi ich podstawę. To właśnie sprawia, że EHR są tak atrakcyjnym celem dla hakerów, a także coraz częściej przedmiotem zakusów rynku komercyjnego. Kluczowym elementem systemów staje się nie tylko sposób zbierania danych, ale również zarządzania nimi przez świadczeniodawców. Dane medyczne są obecnie zapisywane w nieustrukturyzowanych formatach i gromadzone w wielu systemach i bazach. Celem rozwoju EHR staje się nie tylko zmniejszenie obciążeń kadry medycznej związanych z ręcznym wprowadzaniem danych, lecz także eliminacja błędów wynikających z duplikacji dokumentacji medycznej, co pozwoli na zmniejszenie liczby błędnych diagnoz, zredukuje opóźnienia w leczeniu i ryzyko zgonu. **Stąd również zainteresowanie blockchainem, jako skomputeryzowaną formą zapisu danych transakcyjnych,**

[14] D. Żochowska, *Najważniejsze trendy w e-zdrowiu*, 2021, https://www.medonet.pl/magazyn-digital-health/digital-innovation,najwazniejsze-trendy-w-e-zdrowiu-2021,artykul,64860646.html (dostęp: 17.11.2022).

związanych z elektroniczną dokumentacją medyczną. Dzięki zdecentralizowanej sieci komputerów, które obsługują blockchain i jednocześnie rejestrują każdą transakcję, automatycznie wykrywane są błędy zapisu. Niektóre kraje, takie jak Australia, Litwa czy Wielka Brytania, zaczęły eksperymentować z technologią blockchain w celu zarządzania dokumentacją medyczną i przepływem dokumentacji między pacjentami, świadczeniodawcami, a także firmami ubezpieczeniowymi. Jednym z potencjalnych kierunków rozwoju jest kontrolowanie EHR przez pacjenta z poziomu aplikacji i udostępnianie jej kadrze medycznej oraz innym interesariuszom. W opiece zdrowotnej blockchain okazał się już skutecznym narzędziem zapobiegania naruszeniom bezpieczeństwa danych, poprawiania dokładności dokumentacji medycznej i obniżania kosztów. Może być też rozwiązaniem problemu fragmentarycznej dokumentacji medycznej. Wartość rozwiązań blockchain na rynku opieki zdrowotnej ma osiągnąć do 2023 r. 890,5 mln dol.

Wszystkie te rozwiązania prowadzą do wdrażania nowego modelu opieki medycznej na żądanie (*on-demand health care*). Placówki opieki zdrowotnej stoją w obliczu zarządzania ogromną ilością danych pacjentów i zwiększonego zapotrzebowania na dostęp do danych, najlepiej w czasie rzeczywistym, przede wszystkim dotyczących indywidualnego pacjenta. W związku z tym portfele aplikacji cyfrowych powinny być wciąż usprawniane, a starsze rozwiązania wycofywane. Jednocześnie przyspieszona adaptacja rozwiązań cyfrowych przez interesariuszy systemu opieki zdrowotnej, napędzana głównie przez rosnące oczekiwania w stosunku do rynku e-commerce, a także długotrwałą pandemię, rodzi nowe oczekiwania w zakresie dostarczania świadczeń zdrowotnych. Rozwój opieki na żądanie pacjentów, czyli w oparciu o ich własny harmonogram, ma na celu wygodę pacjenta i poprawę dostępności świadczeń medycznych. Innowacje cyfrowe umożliwiają komunikację i monitorowanie pacjenta pośrednio (telekonsultacje, telemonitorowanie) za pomocą choćby ich własnych smartfonów. Oczekuje się, że nasilające się wykorzystanie urządzeń mobilnych i opracowywanie coraz to nowych aplikacji związanych ze zdrowiem na całym świecie będzie kluczowym czynnikiem napędzającym wzrost rynku. Zwiększenie się akceptacji tych rozwiązań zarówno przez administrację publiczną, jak i społeczeństwo, pozwala na dokonanie przełomu w cyfryzacji systemu opieki zdrowotnej, także w zakresie jej finansowania. Dodatkowo pacjenci już obecnie szukają w sieci odpowiedniego lekarza, placówki medycznej czy ośrodków prowadzących badania naukowe, coraz częściej też umawiają się online na wizyty lekarskie. Teleporada stała się normą i elementem koszyka świadczeń gwaran-

towanych także w Polsce, nie tylko w kardiologii, lecz także w innych obszarach (POZ, geriatrii, pulmonologii). Prowadzi to do konieczności przekształcenia filozofii zarządzania zasobami ludzkimi również w zakresie kadry medycznej. Nowe formy komunikacji cyfrowej pozwalają na zwiększenie elastyczności zatrudnienia profesjonalistów medycznych (co już widoczne jest choćby w radiologii), zarówno na rynku publicznym, jak i prywatnym.[15]

W niniejszym dokumencie chcemy przedstawić znaczenie możliwości zastosowania cyfryzacji w ochronie zdrowia, a także najważniejsze zagrożenia i bariery w transformacji cyfrowej w Polsce. W kolejnych rozdziałach omówiono obecny stan rozwoju ekosystemu cyfrowego i jego wpływ na suwerenność cyfrową Polski. Wdrożenie rozwiązań cyfrowych do współczesnych modeli opieki zdrowotnej pozwala na identyfikację najważniejszych wyzwań rozwoju społeczeństwa informacyjnego, także w świetle dokumentów dotyczących polityki zdrowotnej EU i Polski. Następnie przedstawiamy wpływ cyfryzacji na bezpieczeństwo pacjentów i nierówności w dostępie do opieki zdrowotnej, w kontekście polskiej transformacji cyfrowej. Ma ona nie tylko wymiar centralny, ale jest mocno związana z dość rozproszonym (szczególnie w zakresie nauki) testowaniem i wdrażaniem cyfrowych rozwiązań u świadczeniodawców, na poziomie lokalnym czy też w ramach inicjatyw europejskich. Wnioski te mogą być podstawą wypracowania szczegółowych rozwiązań cyfrowej strategii zdrowia w Polsce.

[15] M. Reddy, *Digital Transformation in Healthcare in 2022: 7 Key Trends*, 2022, https://www.digitalauthority.me/resources/state-of-digital-transformation-healthcare/ (dostęp: 17.11.2022).

02

MAGDALENA WŁADYSIUK

Prezes Stowarzyszenia CEESTAHC oraz wiceprezes firmy HTA Consulting, lekarz (Akademia Medyczna w Lublinie), absolwent ekonomii i manager (MBA na WSPiZ im. L. Koźmińskiego w Warszawie), Departament Epidemiologii i Medycyny Prewencyjnej UJ

Zastosowanie cyfryzacji w opiece zdrowotnej

Typy danych zdrowotnych

Transformacja cyfrowa, jako jeden ze strategicznych kierunków działania wyznaczonych przez Radę Europejską, jest w Polsce realizowana przez tworzenie nowych rozwiązań i modeli. Rozwiązania cyfrowe w zakresie opieki zdrowotnej oraz społecznej są i będą jednym z głównych narzędzi (obok konwencjonalnych technologii medycznych) poprawy zdrowia obywateli. Maksymalne wykorzystanie możliwości cyfrowych może prowadzić do radykalnej zmiany zarówno zakresu, jak i sposobu świadczenia usług medycznych oraz społecznych, o ile opracowane będą w sposób celowy i zgodnie ze strategicznymi kierunkami rozwoju systemów zdrowia. A przede wszystkim będą poddawane ewaluacji pod kątem efektywności i opłacalności. Ze względu na koszty transformacji cyfrowej, a także wysokie koszty wycofywania się (deinwestycji) z obecnych rozwiązań, powinna być ona przeprowadzona kompleksowo, z uwzględnieniem poziomu umiejętności cyfrowych całego społeczeństwa, a przede wszystkim interesariuszy systemu. Dzięki cyfryzacji możliwe jest wykorzystanie zbieranych danych – medycznych, finansowych, infrastrukturalnych i wielu innych, w zależności od potrzeb systemowych (centralnych czy lokalnych samorządów) i potrzeb indywidualnego pacjenta.

RYSUNEK 2. INTERESARIUSZE SYSTEMU OPIEKI ZDROWOTNEJ

RZĄD/MINISTERSTWO ZDROWIA

wykorzystujący dane w celu kreowania i centralnego zarządzania, w ramach realizacji polityki zdrowotnej państwa.

INSTYTUCJE PUBLICZNE I DECYDENCI

którzy chcą wspierać swoje decyzje w oparciu o dane dotyczące pacjentów, świadczeniodawców, funkcjonowania systemu opieki zdrowotnej czy szerzej – wykorzystywać je w ochronie zdrowia w celu kreowania polityki zdrowotnej państwa na poziomie centralnym i lokalnym.

ŚWIADCZENIODAWCY

którzy dzięki analizie danych, poprzez dostęp do danych zarówno klinicznych, jak i tych dotyczących struktury i procesu, czyli aspektów jakości, mogą poprawiać zarządzanie placówkami zdrowia w celu podniesienia jakości opieki nad pacjentem, od profilaktyki przez leczenie po profilaktykę wtórną.

SEKTOR PRYWATNY E-ZDROWIA

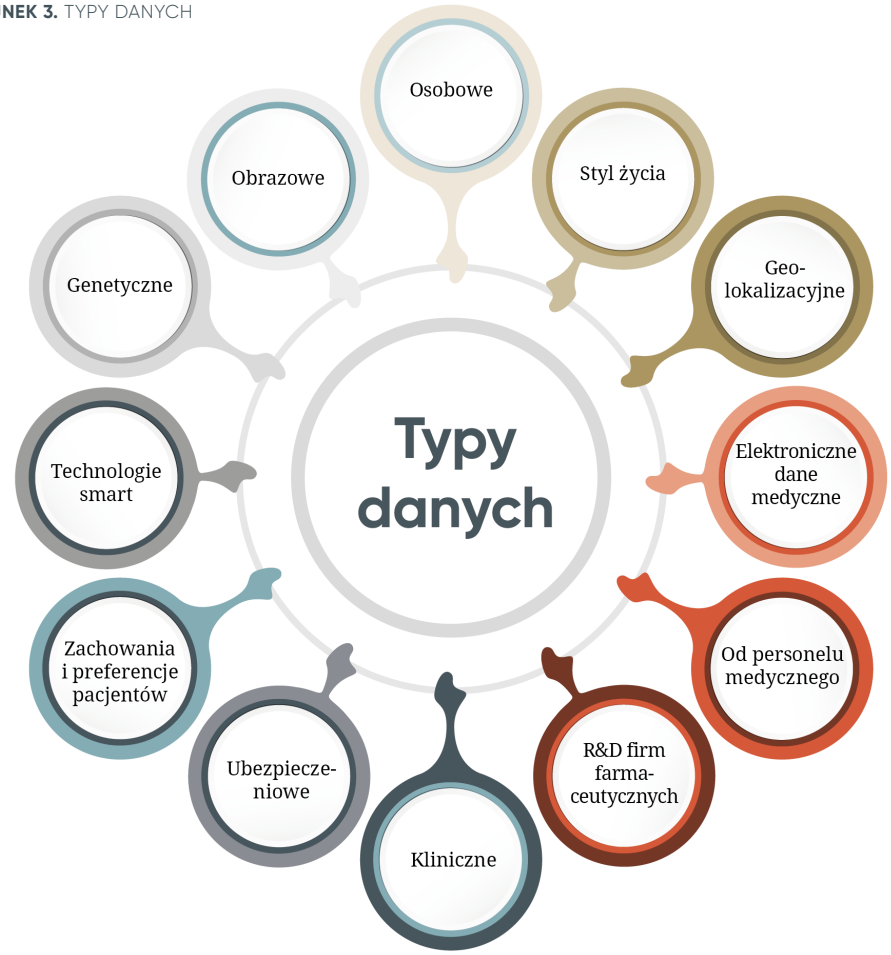
firmy farmaceutyczne/sprzętowe i firmy IT odpowiedzialne za wdrażanie rozwiązań czy technologii medycznych, w tym w oparciu o cyfryzację na poziomie pacjenta, świadczeniodawcy, instytucji publicznych czy całego systemu opieki zdrowotnej.

PACJENCI/ORGANIZACJE PACJENTÓW

oraz ich przedstawiciele, dzięki danym pozyskiwanym przez organizacje pozarządowe oraz fundacje i stowarzyszenia, otrzymają łatwiejszy dostęp do uporządkowanej wiedzy na temat diagnostyki i dostępnych opcji terapeutycznych, będą mogli również bardziej świadomie podejmować decyzje dotyczące wyboru ośrodka, lekarza czy leczenia. Dla ośrodków naukowo-badawczych, firm farmaceutycznych i technologicznych dostęp do danych medycznych to przede wszystkim szansa na przyspieszenie prowadzonych badań i łatwiejsze wdrażanie innowacji.

Dane dobrej jakości są kluczowym czynnikiem umożliwiającym transformację cyfrową. Wykorzystanie danych z różnorodnych źródeł zapewnia ich dalszą dogłębną analizę i wyciąganie wniosków dla wszystkich interesariuszy w systemie opieki zdrowotnej. Dane zdrowotne rozumiane są jako wyniki obserwacji chorego/zdrowego w jego codziennym funkcjonowaniu lub w czasie obserwacji klinicznej (dane medyczne), pozyskiwane bezpośrednio od niego lub jego najbliższego otoczenia. Głównymi interesariuszami – zarówno w zakresie generowania danych, ich zbierania, przetwarzania oraz ostatecznie korzystania z nich – są decydenci (rząd/Ministerstwo Zdrowia, inne instytucje publiczne), świadczeniodawcy jako realizatorzy świadczeń, pacjenci oraz szeroko pojęty sektor prywatny. Wraz z rozwojem możliwości cyfryzacji pojawiają się nowe metody pozyskiwania (np. social media i Internet rzeczy – ang. IoT, *Internet of things*) oraz zapisu danych, co pozwala na poszerzanie zakresu wykorzystywanych źródeł danych, których wciąż przybywa. Dane dotyczące zdrowia mogą występować w różnych formach (dane prospektywne lub z archiwów), a sposób zarządzania nimi jest różny w różnych krajowych systemach opieki zdrowotnej (scentralizowanym, zdecentralizowanym, mieszanym).

RYSUNEK 3. TYPY DANYCH



Kolejny istotny podział danych jest związany z miejscem ich pochodzenia, tu rozróżniamy dane **publiczne i prywatne**. Jest to szczególnie istotne ze względu na kwestie prawne dotyczące bezpieczeństwa gromadzenia, przetwarzania i możliwości wykorzystania danych albo dostępu do nich. Dane mogą być podzielone także w zależności od obszaru ich przetwarzania na: pierwotne – generowane i wykorzystywane bezpośrednio przez kadrę medyczną, lub wtórne – wykorzystywane w monitorowaniu zdrowia populacji, a także w kształtowaniu polityki i rozwoju usług publicznych albo prywatnych w dziedzinie zdrowia. Przetwarzanie danych oraz analityka okazują się kluczowe dla możliwości dalszego rozwoju tej dziedziny.

Zastosowanie danych w opiece zdrowotnej w dobie cyfryzacji

Cyfryzacja zmienia wszystkie aspekty życia człowieka, a metody zbierania danych, ich przetwarzania i zastosowania są olbrzymie i wciąż rozwijane w Polsce i na świecie. Gromadzenie danych w formie cyfrowej otwiera szerokie możliwości ich wykorzystywania na wielu polach związanych z medycyną oraz w kształtowaniu systemu opieki zdrowotnej. Jednocześnie tworzenie rozwiązań cyfrowych prowadzi do powstania zarówno pojedynczych technologii medycznych, jak i kompleksowych, integralnych rozwiązań systemowych, pozwalających na współpracę na linii pacjent – świadczeniodawca, z koordynacją na poziomie centralnym lub lokalnym. Skoordynowanie działań w zakresie cyfryzacji wymaga opracowania strategii i planów rozwoju w ciągle zmieniających się warunkach, z uwzględnieniem potrzeb poszczególnych interesariuszy.

Digital Health Interventions – cyfrowe interwencje zdrowotne, rozwijane na podstawie danych medycznych (szerzej: zdrowotnych), stanowią rosnący zbiór rozwiązań wdrażanych w systemach opieki zdrowotnej. Jeśli chodzi o funkcje cyfrowych interwencji, przygotowana przez WHO klasyfikacja pozwala na skategoryzowanie wciąż dynamicznie rozwijającego się zastosowania technologii cyfrowych i mobilnych do wspierania ochrony zdrowia i rozwiązań systemowych w czterech obszarach:

1. pacjenci/obywatele,
2. świadczeniodawcy,
3. zarządzający systemem ochrony zdrowia,
4. odrębnie usługi związane z zarządzaniem danymi.[16]

Potrzeby i oczekiwania pacjentów wobec organizacji opieki zdrowotnej ewoluują. Pacjenci chcą być poinformowani, zaangażowani i mieć możliwości kontaktu z kadrą medyczną na każdym etapie opie-

[16] *WHO guideline: recommendations on digital interventions for health system strengthening. Executive summary*, World Health Organization, Geneva 2019 (WHO/RHR/19.8). Licence: CC BY-NC-SA 3.0 IGO, https://apps.who.int/iris/bitstream/handle/10665/311977/WHO-RHR-19.8-eng.pdf?ua=1 (dostęp: 21.11.2022).

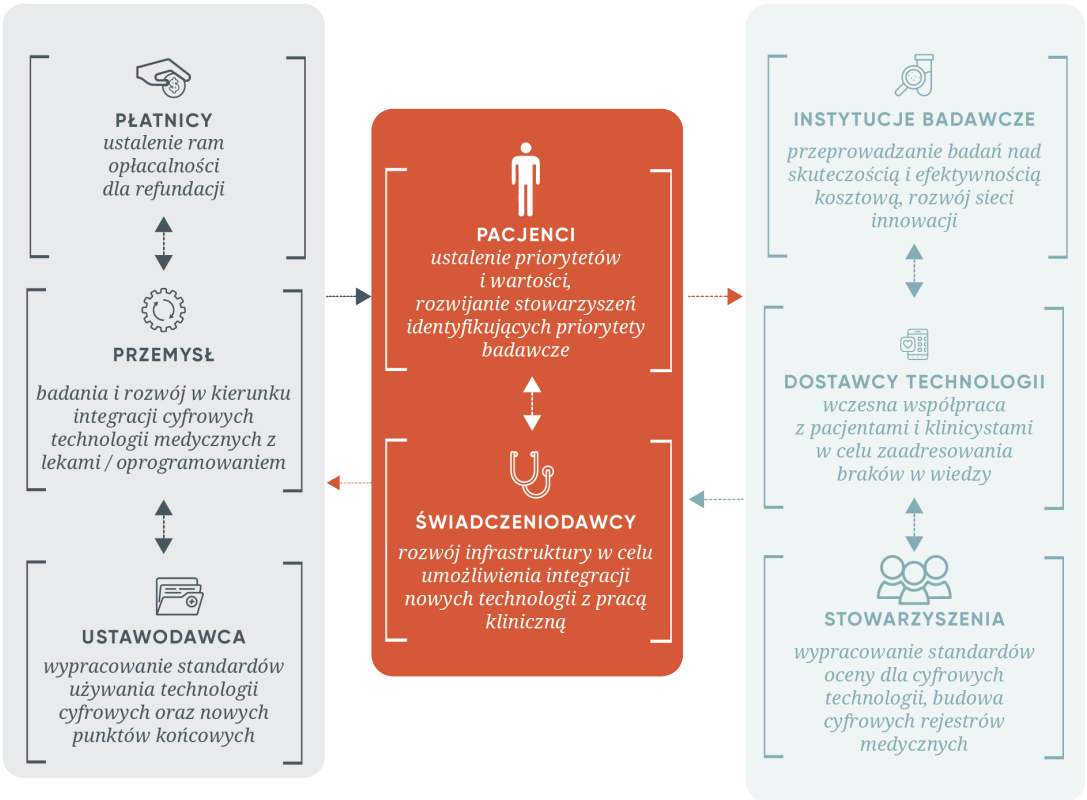
ki. Dlatego nie tylko integracja świadczeń medycznych, komunikacja i wspieranie pacjenta w poprawie jego umiejętności radzenia sobie z chorobą, lecz i rozwój umiejętności cyfrowych staje się podstawą opieki skoncentrowanej na pacjencie. Mobilny i szerzej rozumiany Internet rzeczy (IoT) będzie odgrywać kluczową rolę, podobnie jak smartfon, w samodzielnym zarządzaniu zdrowiem, zwiększając zaangażowanie pacjentów i tworząc warunki do partnerstwa w opiece zdrowotnej.

Trzy główne grupy interesariuszy są obecnie najczęstszymi użytkownikami analiz danych w opiece zdrowotnej:

» **Praktycy kliniczni** – analiza danych klinicznych ma na celu skrócenie czasu oczekiwania pacjentów na świadczenie przez ulepszenie planowania i zwiększenie liczebności personelu, zapewnienie pacjentom większej liczby opcji podczas planowania wizyt i leczenia oraz zmniejszenie wskaźników ponownych przyjęć za pomocą modeli predykcyjnych, szacujących ryzyko;

» **Płatnicy opieki zdrowotnej** – ubezpieczyciele (prywatni lub publiczni) wykorzystują analitykę danych w celu monitorowania prawidłowości procesów zachodzących w systemie pod względem prawnym, monitorowania stanu ludności w celu zwalczania powszechnych dolegliwości zdrowotnych, opracowania systemów oceny wskaźników jakości z monitorowaniem kosztów;

RYSUNEK 4. ZALEŻNOŚCI MIĘDZY INTERESARIUSZAMI UŻYWAJĄCYMI TECHNOLOGII CYFROWYCH W OCHRONIE ZDROWIA I BADANIACH KLINICZNYCH



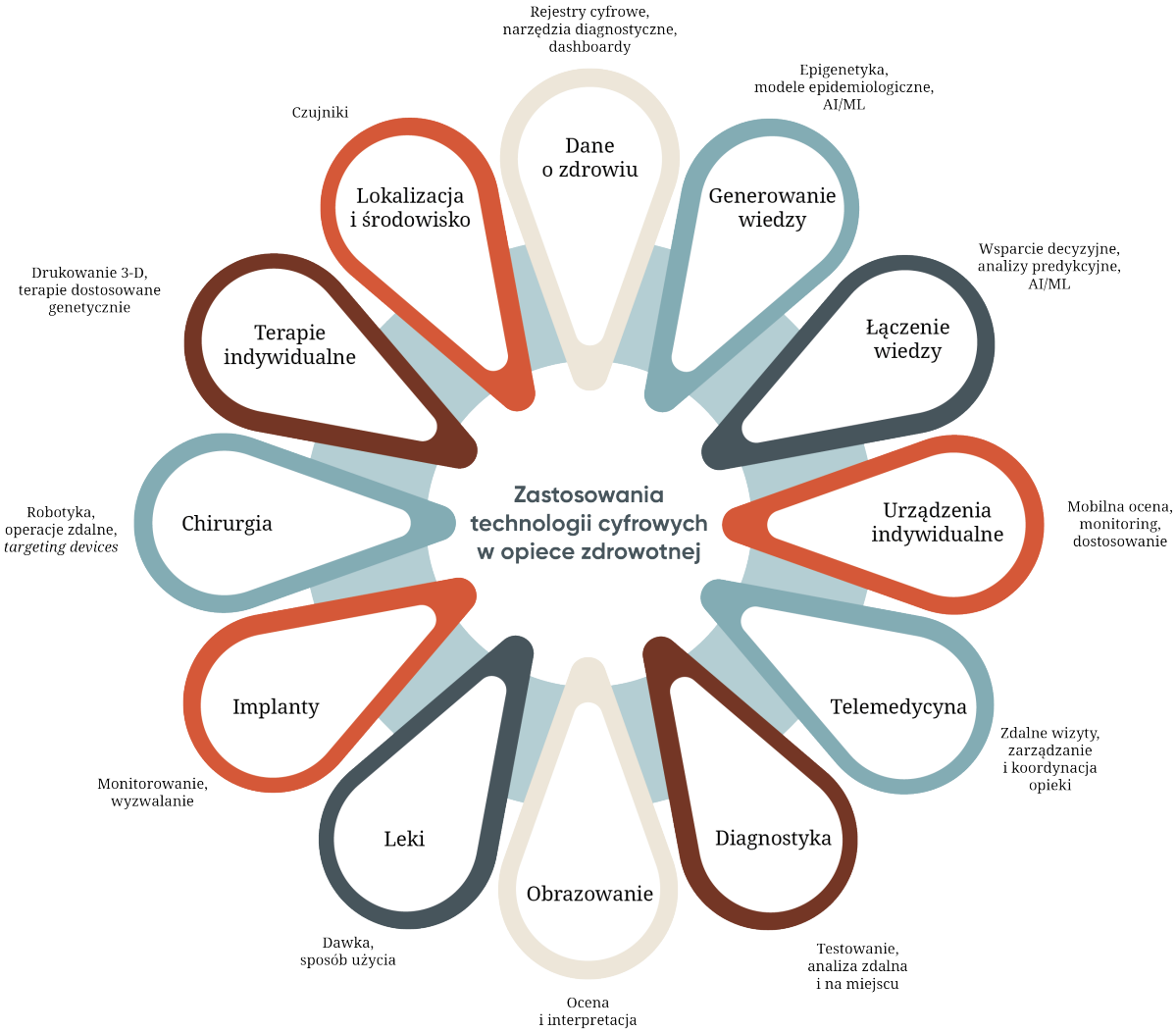
» **Decydenci** – zarządzający opieką zdrowotną. Przedmiotem zainteresowania decydentów jest przewidywanie zdarzeń medycznych i zapobieganie im na podstawie analiz predykcyjnych, m.in. dzięki identyfikacji pacjentów o najwyższym ryzyku choroby przewlekłej w jej wczesnych stadiach. Analiza badań laboratoryjnych i danych generowanych przez pacjentów wraz z analizą czynników ekonomiczno-społecznych zmniejsza ryzyko długotrwałej choroby, co obniża ogólne koszty opieki zdrowotnej i poprawia wyniki pacjentów.

Gromadzone dane mogą obejmować bardzo szeroki zakres, od danych medycznych na temat diagnostyki, stanu klinicznego, leczenia, rekonwalescencji pooperacyjnej po zachowania pacjenta i jego zaangażowanie w terapię. Obecnie, w celu szerszego wykorzystania zbieranych informacji, dokonuje się przekształcania danych nieustrukturyzowanych. Wraz z transformacją cyfrową modele leczenia ulegają zmianie, a wiele z tych zmian wynika właśnie z danych. Lekarze chcą jak najwięcej dowiedzieć się o konkretnej osobie, rozpocząć jej monitorowanie na jak najwcześniejszym etapie, aby wykryć ostrzegawcze objawy poważnej choroby, bo leczenie każdej choroby na wczesnym etapie jest znacznie prostsze i tańsze.

Zwiększenie potencjału cyfryzacji jest możliwe przez wdrażanie nowych narzędzi i infrastruktury cyfrowej, których utrzymanie oraz dalszy rozwój zależy od zarządzających danymi. Szpitale i inne jednostki ochrony zdrowia uzyskują dziś dostęp do innowacyjnych technologii gromadzenia dużych ilości danych za pośrednictwem elektronicznej dokumentacji medycznej, spersonalizowanych aplikacji mobilnych dotyczących zdrowia lub telemedycyny. Pełne wykorzystanie zebranych danych przez lekarzy, czy szerzej: świadczeniodawców, oparte jest na tworzeniu wizualizacji danych oraz rozwiązań typu *low code*, no code (obejmujących technikę programowania z wykorzystaniem prostego kodu, do którego nie jest wymagana zaawansowana wiedza z zakresu języków programowania). W rezultacie użytkownicy *low code* mogą tworzyć procesy i aplikacje bez pomocy ekspertów w zakresie programowania.

Usługi cyfrowe to szansa na poprawę profilaktyki i leczenia chorób przewlekłych oraz umożliwienie pacjentom przekazywania informacji zwrotnej świadczeniodawcom. Systemy ochrony zdrowia skorzystają również na innowacyjnych modelach opieki, w których telemedycyna i m-zdrowie służą do zaspokajania rosnącego zapotrzebowania zdrowotnego pacjentów. Na bazę składają się dostępne publicznie aplikacje, zawierające informacje z poszczególnych dziedzin medycyny i obszarów opieki zdrowotnej, m.in. dane w zakresie: demografii, epi-

RYSUNEK 5. ZASTOSOWANIA TECHNOLOGII CYFROWYCH W OPIECE ZDROWOTNEJ[17]



demiologii, prognozy epidemiologicznej oraz czynników ryzyka i profilaktyki. Różne zakresy analiz obejmują takie obszary jak podstawowa opieka zdrowotna, leczenie szpitalne, opieka domowa, zastosowanie sprzętu medycznego.[18,19]

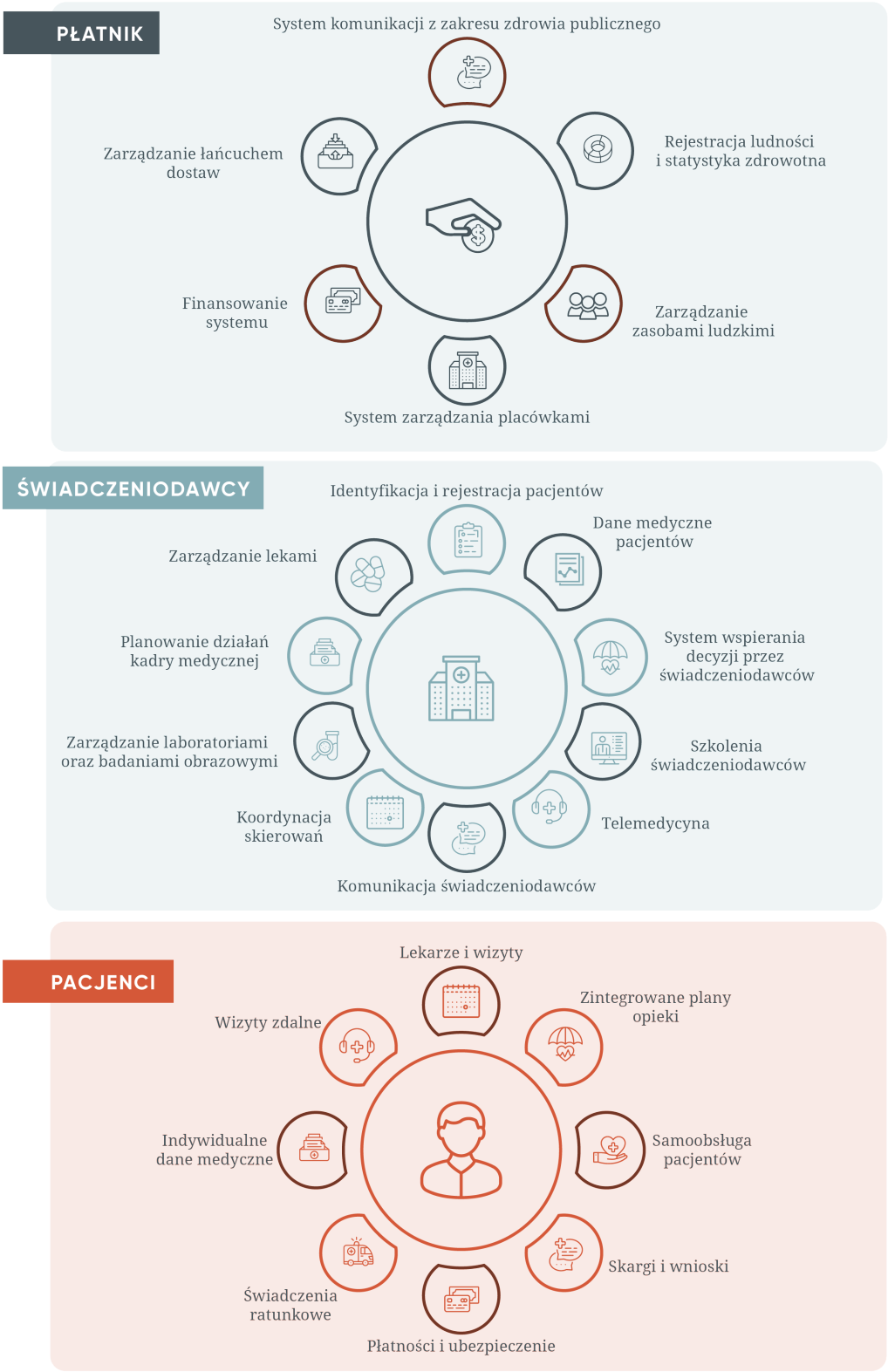
---

[17] National Academy of Medicine, Digital Health Action Collaborative, a NAM Leadership Consortium, 2019.

[18] N. Hanson, V. Matyi, J. Sarmiento, D. Wimble, Redefine your digital health strategy with behavioral engagement patterns, 2020, https://www.zs.com/insights/redefining-your-digital-health-strategy (dostęp: 23.11.2022).

[19] A. Abernethy, L. Adams, M. Barrett, C. Bechtel, P. Brennan, A. Butte, J. Faulkner, E. Fontaine, S. Friedhoff, J. Halamka, M. Howell, K. Johnson, P. Lee, P. Long, D. McGraw, R. Miller, J. Perlin, D. Rucker, L. Sandy, L. Savage, L. Stump, P. Tang, E. Topol, R. Tuckson, K. Valdes, *The Promise of Digital Health: Then, Now, and the Future. NAM Perspectives*. Discussion Paper, National Academy of Medicine, Washington 2022, DC. https://doi.org/10.31478/202206e. https://nam.edu/the-promise-of-digital-health-then-now-and-the-future/ (dostęp: 23.11.2022).

RYSUNEK 6. ROZWIĄZANIA ZDROWIA CYFROWEGO DLA POSZCZEGÓLNYCH INTERESARIUSZY SYSTEMU[20]



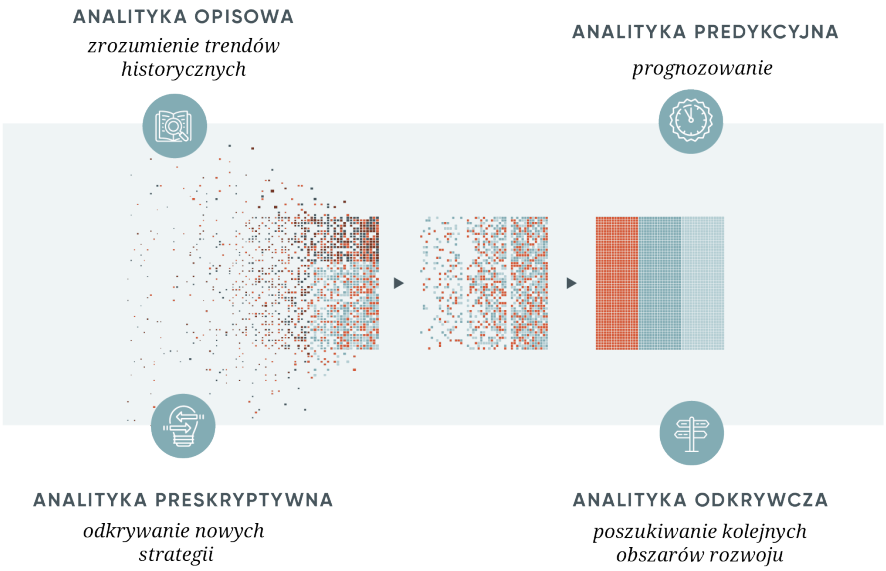
[20] Opracowanie własne na podstawie: IQVIA. Mobile and Home Health Tech Solutions, 2022, https://www.iqvia.com/locations/middle-east-and-africa/solutions/provider-solutions/mobile-and-home-health-tech-solutions.

Dzięki rosnącym możliwościom współczesnej analityki, opartej na dużych zbiorach danych (*big data*) oraz sztucznej inteligencji, dane gromadzone w medycznych systemach informatycznych mogą zostać wykorzystane m.in. do:

- badania i przewidywania chorób,
- personalizacji opieki nad pacjentem,
- wczesnego wykrywania choroby,
- zapobiegania niepotrzebnym wizytom lekarskim,
- monitorowania leczenia pacjentów,
- bardziej efektywnego udostępniania danych pacjentów,
- odkrywania nowych leków,
- automatyzacji procesów administracyjnych szpitala.

Oczywiście, w zakresie analityki danych potężne moce obliczeniowe i modele analiz są opracowywane i wykorzystywane przez firmy farmaceutyczne lub sprzętowe, przy wsparciu firm data science wraz z rozwojem ich produktów. Istotne jest, żeby dane różnego pochodzenia móc zintegrować, co dzięki odpowiednim modelom analitycznym pozwoli na pozyskanie wiedzy wspierającej podejmowanie decyzji w ramach opieki zdrowotnej. Pierwszym z takich rozwiązań w Polsce jest opracowanie „Mapa potrzeb zdrowotnych", realizowane przez Departament Analiz i Strategii Ministerstwa Zdrowia[21,22] i nadal rozwijane. Planuje się wdrożenie nowych narzędzi w zakresie e-recept i e-skierowań oraz Zintegrowanej Platformy Analitycznej[23] (w celu podniesienia skuteczności działań administracji w wybranych obszarach problemów społecznych i gospodarczych przez wsparcie procesów decyzyjnych za pomocą informacji analitycznej).

RYSUNEK 7. CZTERY RODZAJE ANALIZY DANYCH W OPIECE ZDROWOTNEJ[24]

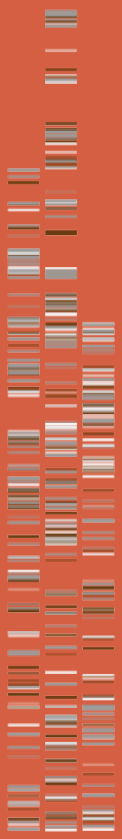


[21] https://basiw.mz.gov.pl/index.html#/visualization?id=3304.

[22] https://basiw.mz.gov.pl/index.html#/visualization?id=3304.

[23] https://www.gov.pl/web/zdrowie/zintegrowana-platforma-analityczna.

[24] A. Abernethy, L. Adams, M. Barrett, C. Bechtel, P. Brennan, A. Butte, J. Faulkner, E. Fontaine, S. Friedhoff, J. Halamka, M. Howell, K. Johnson, P. Lee, P. Long, D. McGraw, R. Miller, J. Perlin, D. Rucker, L. Sandy, L. Savage, L. Stump, P. Tang, E. Topol, R. Tuckson, K. Valdes... op.cit. (dostęp: 23.11.2022).



03

MAGDALENA WŁADYSIUK

Prezes Stowarzyszenia CEESTAHC oraz wiceprezes firmy HTA Consulting, lekarz (Akademia Medyczna w Lublinie), absolwent ekonomii i manager (MBA na WSPiZ im. L. Koźmińskiego w Warszawie), Departament Epidemiologii i Medycyny Prewencyjnej UJ

Wyzwania w rozwoju cyfryzacji w ochronie zdrowia

Dostęp i powszechność (*universal coverage*) systemów opieki zdrowotnej są sukcesami cywilizacyjnym państw europejskich w XX w. Mają na celu zapewnienie zdrowia obywateli przez poprawę jakości opieki zdrowotnej, a transformacja cyfrowa ma ten postęp wspierać. Dane naukowe oraz badania wskazują, że chociaż podmioty świadczące usługi opieki zdrowotnej korzystają z coraz większej liczby rozwiązań opartych na technologiach cyfrowych, skala wdrażania tych rozwiązań oraz rodzaje i możliwości technologii cyfrowych różnią się znacznie w poszczególnych krajach UE. Komisja Europejska zainicjowała w całej UE liczne działania związane zarówno ze stworzeniem odpowiednich strategii, jak i integracji już działających w państwach członkowskich rozwiązań. Jednak mimo że kraje europejskie zainicjowały transformację cyfrową, nadal znacznie różnią się dojrzałością w zakresie jej implementacji w opiece zdrowotnej zarówno między sobą, jak i na własnym terenie.

W dobie nowych wyzwań cyfryzacja to jedyna droga do poprawy wydajności systemów opieki zdrowotnej.[25,26] W związku z rosnącą długością życia w UE oraz starzeniem się populacji coraz większym wyzwaniem staje się wydajność systemu opieki zdrowotnej. Oznacza to najczęściej nieustanną potrzebę poprawy efektywności, najlepiej bez wzrostu wydatków publicznych lub z jak najmniejszym ich wzrostem. Polityka zdrowotna, stanowiąca domenę państw członkowskich, jest w tym obszarze rozwijana wraz z polityką Unii Europejskiej, która dąży do większej spójności w obszarach, w których kraje członkowskie mogłyby przygotowywać się na ewentualne kryzysy zdrowotne i wspólnie na nie reagować. Pandemia uwypukliła też znane już wcześniej wyzwania, którym muszą sprostać systemy ochrony zdrowia, lecz znaczenie cyfryzacji jeszcze bardziej wzrosło m.in. na skutek nasilenia się problemów z dostępnością kadry medycznej, z komunikacją między pacjentami a świadczeniodawcami, a także między poszczególnymi służbami, co wpłynęło na jakość opieki medycznej i różnice między sytuacją w krajach Unii. Nadało to nowe znaczenie planom budowy ściślejszej Europejskiej Unii Zdrowotnej.

Jednym z najbardziej istotnych aspektów wzmacniania pozycji obywateli i zapewniania opieki skoncentrowanej na pacjencie jest tworzenie bezpiecznego dostępu obywateli do danych dotyczących zdrowia oraz ich wymiana, a także rozwój narzędzi cyfrowych. Cyfryzacja, jako złożone zjawisko, szczególnie w systemach opieki zdrowotnej, jest wielką szansą na zmianę kształtu systemu, lecz niesie ze sobą liczne zagrożenia – zarówno dla pojedynczego pacjenta, jak dla całego społeczeństwa. Jednocześnie słabe zarządzanie transformacjami cyfrowymi już

---

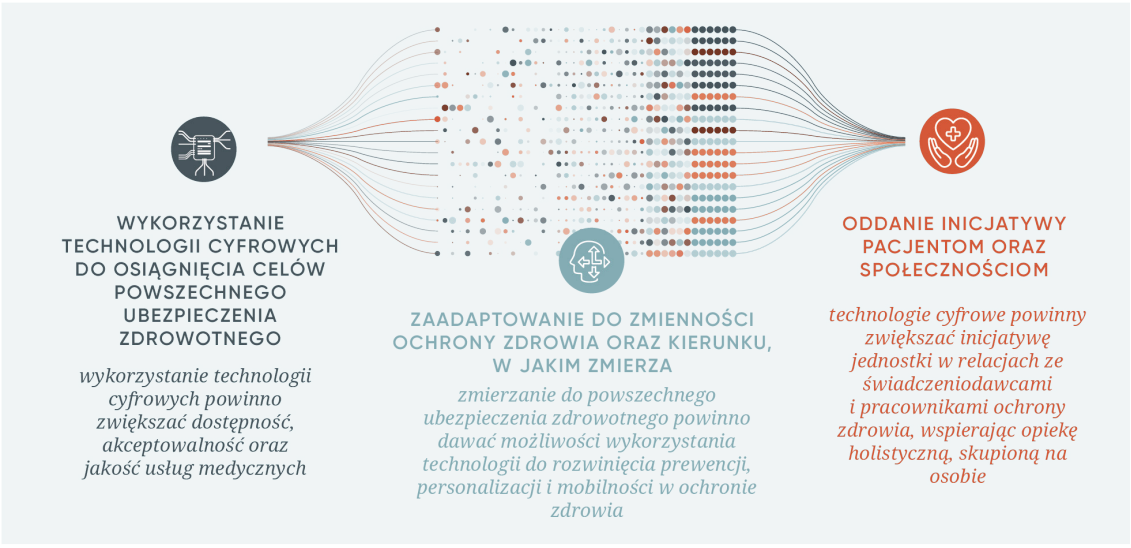
[25] PAHO, *8 Principles for Digital Transformation of Public Health*, https://www.paho.org/en/is4h-project/8-principles-digital-transformation-public-health.

[26] *Digital transformation. Shaping the future of European healthcare*, Deloitte 2020, https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/life-sciences-health-care/deloitte-uk-shaping-the-future-of-european-healthcare.pdf.

dzisiaj prowadzi do nieprzewidzianych skutków na całym świecie, od zagrożeń demokracji i praw człowieka w ochronie zdrowia po ograniczenie podmiotowości pacjentów i społeczności, a tym samym do nierówności w ochronie zdrowia i podważania zaufania publicznego do jej systemu. Ochrona zdrowia od wielu lat na całym świecie jest motorem innowacji i przedmiotem rosnącej aktywności biznesowej firm i platform technologicznych. Kluczowe staje się stworzenie systemu opartego na wartościach, także w zarządzaniu, w celu wsparcia integracji z technologiami cyfrowymi zarówno w sektorze publicznym, jak i prywatnym.

W ciągu ostatnich kilkudziesięciu lat przyspieszony postęp technologii cyfrowej spowodował zmiany w praktycznie wszystkich aspektach ludzkich działań. Pozytywne i negatywne skutki tych zmian były i pozostaną przedmiotem gorących dyskusji. Transformacje cyfrowe są osadzone w ekosystemie szerszych procesów politycznych, społecznych oraz gospodarczych i w nich negocjowane. Rozwijane modele biznesowe, oparte na ekstrakcji danych i ich koncentracji, wraz z szerzeniem się dezinformacji reprezentują cechy definiujące obecną fazę transformacji cyfrowej. I podmiotom prywatnym, i rządom narzędzia cyfrowe umożliwiają bezprecedensowy dostęp do informacji o codziennym życiu ludzi i są wykorzystywane w wielu krajach do różnych celów politycznych, także w polityce zdrowotnej. W ramach tych szerszych procesów transformacji cyfrowej ochrona zdrowia szybko staje się dziedziną o wysokim poziomie ryzyka ze względu na dynamikę, rosnące znaczenie gospodarcze danych dotyczących zdrowia i zapotrzebowanie na

RYSUNEK 8. DYNAMIKA PRZEMIAN POWSZECHNEGO UBEZPIECZENIA ZDROWOTNEGO[27]



[27] Opracowanie własne na podstawie: The Lancet and Financial Times Commission on governing health futures 2030: growing up in a digital world 2021, https://www.thelancet.com/article/S0140-6736%2821%2901824-9/fulltext (dostęp: 22.11.2022).

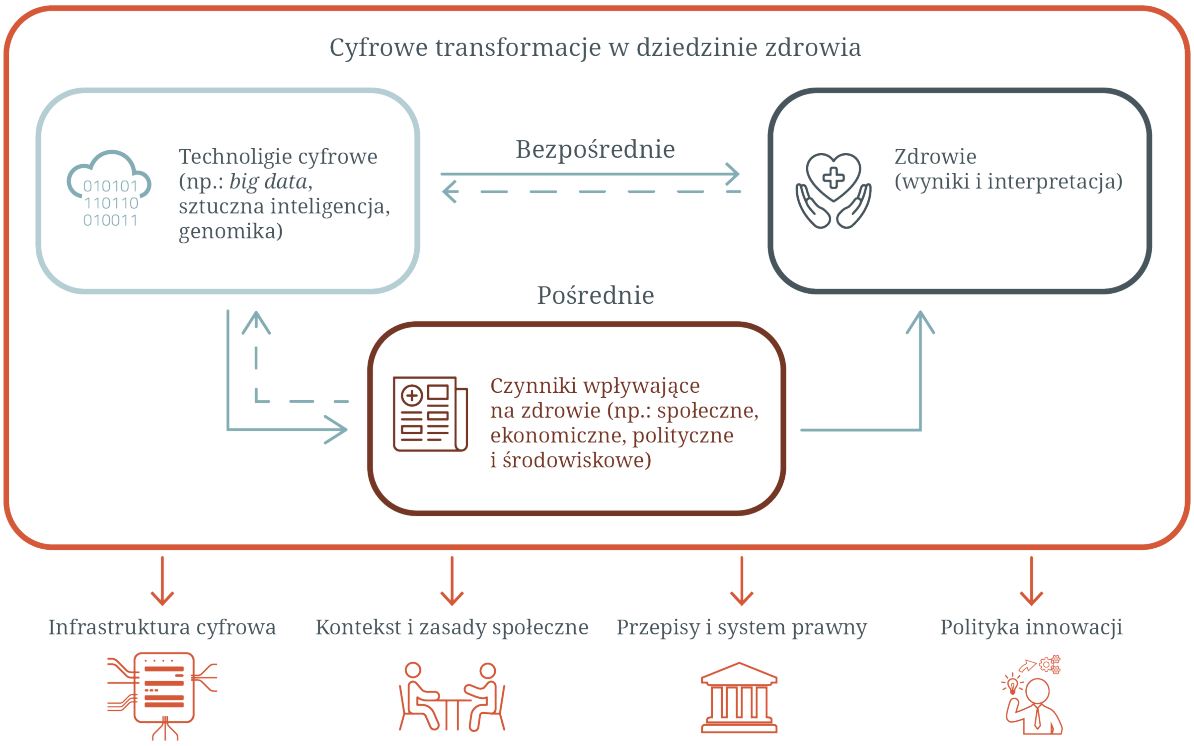
rozwiązania cyfrowe w sektorze opieki zdrowotnej.

Kierunki wskazane w europejskiej i polskiej strategii cyfryzacji są spójne i zawierają długofalowe cele strategiczne dla Polski. Z drugiej strony działania w naszym kraju wymagają nowych kompetencji w zakresie zarządzania w celu skoordynowania działań w ramach stabilnego, lecz niedofinansowanego sektora, jakim jest ochrona zdrowia. Przede wszystkim jednak konieczna jest ewaluacja skutków wdrożonych kompleksowych działań operacyjnych, które w ochronie zdrowia mogą być mierzone na poziomie centralnym, w określonych sektorach zdrowia lub obszarach zdrowotnych. Poniżej przedstawimy historię transformacji cyfrowej w UE oraz w Polsce jako zapis podjętych działań, ale także jako realizację wizji przyszłości w zdrowiu. W tym rozdziale zostaną przedstawione także najważniejsze wyzwania oraz zagrożenia wynikające z transformacji cyfrowej opieki zdrowotnej.

Cyfryzacja a polityka europejska

Europejska strategia dotycząca przyszłości cyfrowej mocno podkreśla rolę danych w sektorze zdrowia.[29] Zdigitalizowana

RYSUNEK 9. EKOSYSTEM CYFROWYCH TRANSFORMACJI[28]



[28] The Lancet and Financial Times Commission on governing health futures 2030: Growing up in a digital world, 2021, https://www.thelancet.com/article/S0140-6736%2821%2901824-9/fulltext (dostęp: 22.11.2022).

[29] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów Cyfrowy kompas na 2030 r.: europejska droga w cyfrowej dekadzie, COM(2021) 118 final/2 z 9.03.2021.

dokumentacja medyczna, gromadzona we wspólnej europejskiej przestrzeni, ma wspierać lepszą wymianę różnych rodzajów danych dotyczących zdrowia (elektronicznych kart zdrowia, danych genomowych, danych z rejestrów pacjentów itp.) nie tylko do celów związanych z opieką zdrowotną (czyli celów tzw. podstawowego wykorzystania danych), ale także z badaniami naukowymi i kształtowaniem polityki zdrowotnej (wtórne wykorzystanie danych). Ma to prowadzić do poprawy leczenia schorzeń generujących największe obciążenia zdrowotne, m.in. chorób cywilizacyjnych, nowotworów oraz chorób rzadkich, a także do zrównania dostępu do wysokiej jakości usług zdrowotnych dla wszystkich obywateli w państwach członkowskich. Wprowadzenie tego śmiałego planu zależeć będzie od poziomu zaufania obywateli do mechanizmów ochrony prywatności danych zdrowotnych, które uważane są za szczególnie wrażliwe.

Wprowadzenie dyrektywy 2011/24/UE, obok stworzenia mechanizmów przestrzegania praw pacjentów w transgranicznej opiece zdrowotnej, po raz pierwszy doprowadziło do postępu w digitalizacji zdrowia. W 2012 r. powstała europejska grupa e-zdrowia składająca się z przedstawicieli organizacji/stowarzyszeń patronackich i organizacji o zasięgu europejskim, przedstawicieli stowarzyszeń reprezentujących interesariuszy (pacjentów, specjalistów, usługodawców itp.). Liczy 30 członków, a jej mandat wygasł pod koniec 2022 r.

9 marca 2021 r. Komisja Europejska przyjęła „Cyfrowy kompas na 2030 r.: europejska droga w cyfrowej dekadzie". W komunikacie w sprawie „cyfrowego kompasu"[30] przedstawiono wizję, cele i możliwości przeprowadzenia do 2030 r. udanej transformacji cyfrowej całej Unii Europejskiej. Ambicją UE jest suwerenność cyfrowa w otwartym świecie oraz prowadzenie polityki cyfrowej, która zapewni obywatelom i przedsiębiorstwom wykorzystanie ukierunkowanej na człowieka, zrównoważonej i bardziej dostatniej cyfrowej przyszłości. Cele cyfrowe na 2030 r. dotyczą czterech głównych kierunków: umiejętności cyfrowych, infrastruktur cyfrowych, cyfryzacji przedsiębiorstw i cyfryzacji usług publicznych. Ostatecznym celem jest stworzenie do 2030 r. Unii Cyfrowej. Dodatkowo wypracowano Strategię bezpieczeństwa cyfrowego UE oraz Kodeks Usług Cyfrowych (ang. *Digital Services Act*). Oba dokumenty są zdecydowanie ukierunkowane na cyfrową suwerenność Unii w obliczu rosnących wyzwań krajowych, europejskich i globalnych.

Polityka europejska pozwala wytyczać kierunki rozwoju także w dziedzinie e-zdrowia i uczestniczyć w kształtowaniu polityki dotyczącej interoperacyjno-

[30] Komunikat Komisji..., op.cit.

ści i normalizacji. W 2018 r. zainicjowano wspólne działanie wspierające sieć e-zdrowie pod nazwą eHAction, powiązane z rozwojem sieci eZdrowia na lata 2018–2021. eHAction zakładało opracowywanie strategicznych ram współpracy między państwami UE i Komisją w czterech priorytetowych obszarach: przez wzmacnianie pozycji jednostek, rozwój innowacji w zastosowaniu danych dotyczących zdrowia, usprawnienia ciągłości opieki oraz rozwiązywanie problemów z wdrażaniem rozwiązań cyfrowych. Głównym celem eHAction było wsparcie naukowe i techniczne sieci eZdrowie, ułatwianie świadczenia transgranicznej opieki zdrowotnej w całej UE oraz zapewnianie niezbędnego wsparcia politycznego dla europejskiej infrastruktury usług cyfrowych w dziedzinie e-zdrowia. Rozpoczęto zatem budowę infrastruktury, która umożliwia wymianę e-recept i kartotek pacjentów między świadczeniodawcami. Pierwsze wymiany transgraniczne nastąpiły w 2019 r., a do 2025 r. mają objąć wszystkie kraje UE. W perspektywie długoterminowej Komisja pracuje nad utworzeniem formatu wymiany europejskich kartotek elektronicznych dostępnego dla wszystkich obywateli Unii.[31]

Najnowsze kierunki tego rozwoju zostały zawarte w programie EU4Health[32] na lata 2021–2027.[33] W programie wyznaczono główne cele w zakresie opracowania i wdrożenia norm prawnych dotyczących:

1. opracowywania ogólnounijnych norm jakości, wiarygodności i cyberbezpieczeństwa danych,
2. ogólnounijnej normalizacji elektronicznej dokumentacji medycznej,
3. e-interoperacyjności przez otwarte formaty wymiany.

Oprócz dokumentów strategicznych wprowadzane są konkretne rozwiązania w zakresie rozwoju wyrobów medycznych,[34] ochrony danych,[35] identyfikacji elektronicznej[36] oraz bezpieczeństwa sieci i systemów informatycznych,[37] oferujące szereg możliwości służących ułatwieniu odpowiedzialnego wykorzystania cyfrowych technologii w zakresie opieki zdrowotnej i społecznej w ramach współpracy krajów członkowskich UE.

---

[31] E-Zdrowie – rozwiązania cyfrowe w ochronie zdrowia, Public Health, Komisja Europejska, https://ec.europa.eu/health/ehealth-digital-health-and-care/overview_pl (dostęp: 6.05.2022).

[32] Regulation (EU) 2021/522.

[33] Regulation (EU) 2021/522 establishing a Programme for the Union's action in the field of health ('EU4Health Programme') for the period 2021–2027.

[34] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/745 z 5 kwietnia 2017 r. w sprawie wyrobów medycznych, DzU L 117 z 5.5.2017. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/746 z 5 kwietnia 2017 r. w sprawie wyrobów medycznych do diagnostyki in vitro, DzU L 117 z 5.5.2017.

[35] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, DzU L 119 z 4.05.2016, s. 1.

[36] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE, DzU L 257 z 28.8.2014.

[37] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, DzU L 194 z 19.07.2016.

Dodatkowo w 2021 r. rozpoczęto wspólne działanie na rzecz europejskiej przestrzeni danych dotyczących zdrowia, zwane TEHDAS (ang. *Towards the European Health Data Space* – Ku europejskiej przestrzeni danych dotyczących zdrowia). W działaniu uczestniczy 26 państw europejskich (22 kraje UE i 4 inne kraje europejskie). Wspólne działania obejmują współpracę z podmiotami korzystającymi z danych dotyczących zdrowia podczas prac badawczych i kształtowania polityki (wtórne wykorzystywanie danych) w UE oraz współpracę w celu tworzenia koncepcji wtórnego wykorzystania danych w zakresie zdrowia. Według planów Komisji istotną rolę odegra tu nie tylko RODO, ale też demokratyczna architektura przestrzeni danych, umożliwiająca dostęp do tego zasobu na bardziej egalitarnych zasadach, niż ma to miejsce w przypadku cyfrowych gigantów, zarazem zaś pozostawiająca prawo decydowania o udostępnianiu swoich danych do wtórnego wykorzystania w rękach obywateli.

Celem europejskiej strategii jest współpraca w zakresie wypracowania krajowych trajektorii opierających się na wytycznych dostarczonych przez Komisję wraz z harmonogramem wdrażania planowanych polityk, przegląd inwestycji potrzebnych do osiągnięcia celów ogólnych i szczegółowych oraz analiz wkładów określonych w krajowych planach działania.

Cyfryzacja a polityka zdrowotna Polski

Najnowsze kierunki polityki zdrowotnej Polski zostały przedstawione w dokumencie strategicznym „Zdrowa przyszłość", opracowanym na lata 2021–2027 jako kontynuacja „Policy Paper dla ochrony zdrowia na lata 2014–2020" (20 lipca 2015).[38,39] Do roku 2020 ustalano dziewięć głównych celów, z których pierwszy polegał na wsparciu systemu informacji w ochronie zdrowia. Wraz z innym celami (mapowaniem potrzeb zdrowotnych, wdrażaniem opieki koordynowanej, wzmocnieniem POZ oraz wsparciem rozwoju zadań publicznych) stanowił główny trzon zmian w systemie cyfryzacji.[40]

W ramach działań podjętych centralnie stworzono Platformę e-Zdrowie, rozwijaną w ramach projektu „Elektroniczna platforma gromadzenia, analizy i udostępniania zasobów cyfrowych o zdarzeniach medycznych" (platforma P1), która została dofinansowana ze środków UE. W ramach fazy II Programu Operacyjnego Polski Cyfrowej oferuje ona cyfrowe usługi publiczne w ochronie zdrowia przez dostarczanie centralnej

[38] Ministerstwo Zdrowia – portal Gov.pl (www.gov.pl).

[39] Krajowe ramy strategiczne. Policy paper dla ochrony zdrowia na lata 2014–2020, Ministerstwo Zdrowia – portal Gov.pl (www.gov.pl).

[40] Fundusze Europejskie dla Zdrowia. Krajowe ramy strategiczne. Policy paper dla ochrony zdrowia na lata 2014–2020, zdrowie.gov.pl.

infrastruktury IT i odpowiednich rozwiązań w zakresie oprogramowania także systemu P2 – platforma udostępniania online przedsiębiorcom usług i zasobów cyfrowych rejestrów medycznych oraz P4 – dziedzinowego systemu teleinformatycznego systemu informacji w ochronie zdrowia oraz rejestrów medycznych. Obecnie, pod auspicjami Ministerstwa Zdrowia oraz jednostki podległej i nadzorowanej przez ministra zdrowia – Centrum e-Zdrowia (właściwej do budowy i utrzymania systemów informatycznych w ochronie zdrowia), zostały udostępnione do użytkowania rozmaite usługi z zakresu e-zdrowia[41] i telemedycyny.

Za pośrednictwem platformy P1 wprowadzono do powszechnego użycia e-receptę[42] (obowiązkową od stycznia 2020 r.), e-skierowanie[43] (od stycznia 2021 r.) oraz aplikację gabinet.gov.pl, przeznaczoną dla lekarzy. Umożliwia ona uzupełnianie e-Karty Szczepień, telekonsultacje,[44] teleopiekę (do której obecnie zalicza się program Domowej Opieki Medycznej – PulsoCare[45] oraz e-stetoskop,[46] opaska telemedyczna,[47] e-spirometr[48]) oraz e-zwolnienie lekarskie.[49] Uruchomiono Internetowe Konto Pacjenta – IKP[50] oraz aplikację mobilną mojeIKP (maj 2021 r)., dzięki którym pacjenci mają dostęp do swoich danych medycznych, mogą zarządzać e-skierowaniami, dokonywać e-rejestracji oraz m.in. pobierać certyfikaty szczepienia przeciw COVID-19. Także w ramach projektu „Wprowadzenie nowoczesnych e-usług w podmiotach leczniczych nadzorowanych przez ministra zdrowia" (projekt e-usługi), realizowanego w latach 2019–2022 w 52 wybranych podmiotach podległych/nadzorowanych przez ministra zdrowia, przewiduje się wdrożenie w nich kluczowych e-usług (wymiany EDM, e-rejestracji, e-zlecenia, e-analizy), jak również wyposażenie tych podmiotów w nowoczesną infrastrukturę IT.

W 2020 r. resort zdrowia podjął decyzję o rozszerzeniu zakresu funkcjonalnego Projektu e-Zdrowie (P1) o usługi pozwalające na załatwienie kluczowych dla pacjenta spraw online, bez kontaktu osobistego z personelem administracyjnym

---

41 Na potrzeby niniejszej pracy przyjęto rozróżnienie terminów e-zdrowie/e-Zdrowie na terminy w rozumieniu:
- potocznym: usługi cyfrowe oferowane interesariuszom systemu ochrony zdrowia (e-zdrowie),
- jako program e-Zdrowie realizowany przez Ministerstwo Zdrowia,
- jako platforma P1 (centralny projekt e-Zdrowia).

42 https://pacjent.gov.pl/internetowe-konto-pacjenta/erecepta (dostęp: 1.05.2022).

43 https://pacjent.gov.pl/internetowe-konto-pacjenta/eskierowanie (dostęp:1.05.2022).

44 https://www.nfz.gov.pl/aktualnosci/aktualnosci-oddzialow/nowe-zasady-korzystania-z-porad-lekarskich,462.html (dostęp: 1.05.2022).

45 https://www.gov.pl/web/pulsocare, https://pacjent.gov.pl/aktualnosc/jak-otrzymac-pulsoksymetr (dostęp: 1.05.2022).

46 https://www.gov.pl/web/estetoskop (dostęp: 1.05.2022).

47 https://www.gov.pl/web/zdrowie/rusza-pilotaz-programu-opaska-telemedyczna (dostęp: 1.05.2022).

48 https://www.gov.pl/web/zdrowie/rusza-pilotaz-programu-e-spirometr (dostęp: 1.05.2022).

49 https://pacjent.gov.pl/e-zwolnienie (dostęp: 1.05.2022).

50 https://pacjent.gov.pl/internetowe-konto-pacjenta (dostęp: 1.05.2022).

i medycznym, co jest szczególnie istotne w stanach zagrożenia epidemicznego. Rozszerzenie Projektu e-Zdrowie zakłada m.in. jego rozbudowę o centralną elektroniczną rejestrację na wybrane świadczenia zdrowotne i usługę e-wizyty z pracownikiem medycznym. Wdrożenie tych usług było przewidziane na koniec 2021 r.

TABELA 1. PROGRAM OPERACYJNY POLSKI CYFROWEJ – KOLEJNE ETAPY

Platforma P1	**Podstawowe funkcje projektu P1:** » Internetowe Konto Pacjenta – IKP[51] oraz aplikacja mobilna mojeIKP » e-recepta,[52] » e-skierowanie,[53] » telekonsultacje,[54] » teleopieka (Domowa Opieka Medyczna – PulsoCare[55] oraz e-stetoskop,[56] opaska telemedyczna[57] oraz e-spirometr[58]), » e-zwolnienia lekarskie,[59] » gabinet.gov.pl – funkcja, która umożliwia lekarzom m.in. wystawianie e-recept i e-skierowań oraz e-Karty Szczepień, » rozliczenia NFZ a świadczeniodawcy oraz aptek.
P2	1. Rejestry podmiotowe:[60] aptek, hurtowni farmaceutycznych, podmiotów wykonujących działalność leczniczą, produktów leczniczych, decyzji głównego inspektora farmaceutycznego, diagnostów laboratoryjnych, ośrodków i banków, systemów kodowania, farmaceutów, surowców farmaceutycznych. 2. Dotychczas utworzono 14 rejestrów przedmiotowych (onkologiczne – KRN,[61] Rejestr Nowotworów Niezłośliwych Dużych Gruczołów Ślinowych,[62] kardiologiczne – Krajowy Rejestr Operacji Kardiochirurgicznych,[63] Ogólnopolski Rejestr Ostrych Zespołów Wieńcowych,[64] Rejestr Operacji Naczyniowych,[65] Krajowy Rejestr Mechanicznego Wspomagania Krążenia,[66] Krajowy Rejestr Infekcyjnego Zapalenia Wsierdzia,[67] Krajowy Rejestr Ablacji Podłoża Arytmii,[68] Krajowy Rejestr Przeznaczyniowych Ekstrakcji Elektrod,[69] Rejestr Hipercholesterolemii Rodzinnej[70] i inne: Polski Rejestr Wrodzonych Wad Rozwojowych,[71] Rejestr endoprotezoplastyk,[71] Rejestr Medycznie Wspomaganej Prokreacji,[73] Krajowy Rejestr Pacjentów z COVID-19[74])

[51] https://pacjent.gov.pl/internetowe-konto-pacjenta (dostęp: 1.05.2022).

[52] https://pacjent.gov.pl/internetowe-konto-pacjenta/erecepta (dostęp: 1.05.2022).

[53] https://pacjent.gov.pl/internetowe-konto-pacjenta/eskierowanie (dostęp: 1.05.2022).

[54] https://www.nfz.gov.pl/aktualnosci/aktualnosci-oddzialow/nowe-zasady-korzystania-z-porad-lekarskich,462.html (dostęp: 1.05.2022).

[55] https://www.gov.pl/web/pulsocare, https://pacjent.gov.pl/aktualnosc/jak-otrzymac-pulsoksymetr (dostęp: 1.05.2022).

[56] https://www.gov.pl/web/estetoskop (dostęp: 1.05.2022).

[57] https://www.gov.pl/web/zdrowie/rusza-pilotaz-programu-opaska-telemedyczna (dostęp: 1.05.2022).

[58] https://www.gov.pl/web/zdrowie/rusza-pilotaz-programu-e-spirometr (dostęp: 1.05.2022).

[59] https://pacjent.gov.pl/e-zwolnienie (dostęp: 1.05.2022).

[60] https://rejestrymedyczne.ezdrowie.gov.pl/

[61] Rozporządzenie ministra zdrowia z 14 czerwca 2018 r. w sprawie Krajowego Rejestru Nowotworów, DzU 2018. 1187.

[62] Rozporządzenie ministra zdrowia z 12 czerwca 2018 r. w sprawie Rejestru Nowotworów Niezłośliwych Dużych Gruczołów Ślinowych, DzU 2018.1182.

[63] Rozporządzenie ministra zdrowia z 30 maja 2018 r. w sprawie Krajowego Rejestru Operacji Kardiochirurgicznych, DzU 2018.1093.

[64] Rozporządzenie ministra zdrowia z 24 maja 2018 r. w sprawie Ogólnopolskiego Rejestru Ostrych Zespołów Wieńcowych, DzU 2018.1063.

[65] Rozporządzenie ministra zdrowia z 8 stycznia 2020 r. w sprawie Rejestru Operacji Naczyniowych, DzU 2020.84.

[66] Rozporządzenie ministra zdrowia z 16 października 2019 r. w sprawie Krajowego Rejestru Mechanicznego Wspomagania Krążenia, DzU 2019.2190.

[67] Rozporządzenie ministra zdrowia z 21 października 2019 r. w sprawie Krajowego Rejestru Infekcyjnego Zapalenia Wsierdzia, DzU 2019.2131.

[68] Rozporządzenie ministra zdrowia z 16 października 2019 r. w sprawie Krajowego Rejestru Ablacji Podłoża Arytmii, DzU 2019.2098.

[69] Rozporządzenie ministra zdrowia z 21 października 2019 r. w sprawie Krajowego Rejestru Przeznaczyniowych Ekstrakcji Elektrod, DzU 2019.2191.

[70] Obwieszczenie ministra zdrowia z 23 grudnia 2021 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia ministra zdrowia w sprawie Rejestru Hipercholesterolemii Rodzinnej, DzU 2022.87 j.t.

[71] Rozporządzenie ministra zdrowia z 12 czerwca 2018 r. w sprawie Polskiego Rejestru Wrodzonych Wad Rozwojowych, DzU 2018.1196.

[72] Rozporządzenie ministra zdrowia z 3 grudnia 2019 r. w sprawie rejestru endoprotezoplastyk, DzU 2019.2409.

[73] Rozporządzenie ministra zdrowia z 16 sierpnia 2018 r. w sprawie Rejestru Medycznie Wspomaganej Prokreacji, DzU 2018.1598.

[74] Obwieszczenie ministra zdrowia z 20 września 2021 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia ministra zdrowia w sprawie Krajowego Rejestru Pacjentów z COVID-19, DzU 2021.1837 j.t.

P4	1. System Statystyki w Ochronie Zdrowia – jako dane statystyczne z zakresu ochrony zdrowia,[75] 2. System Ewidencji Zasobów Ochrony Zdrowia – informacje na temat wyrobów medycznych i środków ochrony osobistej posiadanych przez usługodawców,[76] 3. System Monitorowania Zagrożeń – to system teleinformatyczny, którego zadaniem jest: » poprawa efektywności działań w zakresie zapobiegania skutkom niepożądanych zdarzeń mających wpływ na zdrowie i życie ludzi, » umożliwienie usługodawcom i innym podmiotom obowiązanym do składania informacji i zgłoszeń o zagrożeniach do rejestrów, o których mowa w ust. 2, w postaci dokumentu elektronicznego,[77] 4. Zintegrowany System Monitorowania Obrotu Produktami Leczniczymi – dane związane z obrotem produktami leczniczymi, środkami spożywczymi specjalnego przeznaczenia żywieniowego oraz wyrobami medycznymi,[78] 5. System Monitorowania Kształcenia Pracowników Medycznych (SMK): » gromadzenie informacji pozwalających na określenie zapotrzebowania na miejsca szkoleniowe w określonych dziedzinach medycyny i farmacji oraz w dziedzinach mających zastosowanie w ochronie zdrowia, » monitorowanie kształcenia podyplomowego pracowników medycznych, » monitorowanie przebiegu kształcenia specjalizacyjnego pracowników medycznych, » wspomaganie procesu zarządzania systemem kształcenia pracowników medycznych, » wsparcie finansowania w ramach modułu System Informatyczny Rezydentur.[79]
Ponadto, w ramach dziedzinowych systemów tele-informa-tycznych (systemów uruchomionych po zakończeniu realizacji projektu P4), funkcjonują:	1. System Rejestru Usług Medycznych NFZ (System RUM–NFZ) – system danych o udzielonych i planowanych świadczeniach opieki zdrowotnej finansowanych ze środków publicznych oraz rozliczanie tych świadczeń,[80] 2. System Obsługi List Refundacyjnych dla leków, środków spożywczych specjalnego przeznaczenia żywieniowego i wyrobów medycznych,[81] 3. Instrument Oceny Wniosków Inwestycyjnych w Sektorze Zdrowia (*opinia o celowości inwestycji*),[82] 4. Rejestr Asystentów Medycznych jest systemem teleinformatycznym, w którym przetwarza się dane o pracownikach medycznych i osobach wykonujących zawód medyczny,[83] 5. System Obsługi Importu Docelowego w sprawie sprowadzenia z zagranicy produktu leczniczego lub środka spożywczego specjalnego przeznaczenia żywieniowego oraz dopuszczenia do obrotu produktu leczniczego nieposiadającego pozwolenia.[84]

[75] Art. 23.1 Ustawy z 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia.

[76] Art. 24.1. ibidem.

[77] Art. 26.1. ibidem.

[78] Art. 29.1. ibidem.

[79] Art. 30.1. ibidem.

[80] Art. 22.1. ibidem.

[81] Art. 30a.1. ibidem.

[82] Art. 31a.1. ibidem.

[83] Art. 31b.1. ibidem

[84] Art. 31c. 1. ibidem

W grudniu 2021 r. został przyjęty uchwałą Rady Ministrów nowy dokument wskazujący cele strategiczne polityki zdrowotnej państwa: „Zdrowa przyszłość. Ramy strategiczne rozwoju ochrony zdrowia na lata 2021–2027 z perspektywą do 2030 r."[85] Zaznaczono, że dokument określa ramy strategiczne koniecznych działań, a jego uzupełnieniem na poziomie operacyjnym będą m.in. plany transformacji – krajowy i wojewódzkie, które zastąpią regionalne priorytety polityki zdrowotnej (brak obecnie szczegółowych planów). W dokumencie zdefiniowano cztery podstawowe obszary rozwoju, w obrębie których zdefiniowano wizję i uwarunkowania strategiczne realizacji polityki: pacjent, procesy, rozwój, finanse.

Zgodnie z tą strategią od 1 lipca 2021 r. zaczęło obowiązywać również raportowanie tzw. zdarzeń medycznych, czyli informacji o udzielonych świadczeniach zdrowotnych,[86] na podstawie art. 13a ustawy z 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia.[87] Dzięki temu platforma P1 e-Zdrowie będzie zawierała historię leczenia pacjentów (finansowanego zarówno ze środków publicznych, jak i prywatnych, w tym także informacje od stomatologów czy fizjoterapeutów), do której dostęp będą mieli lekarze i inni pracownicy medyczni na zasadach określonych w przepisach. W praktyce są to informacje m.in. o udzielanych świadczeniach zdrowotnych, kartoteka medyczna pacjenta, rozpoznanie jego problemu zdrowotnego, wyniki badań laboratoryjnych, opis badań diagnostycznych oraz karta leczenia szpitalnego. Istotnym aspektem działań związanych z rozwojem EDM w skali systemowej jest oparcie wprowadzanych rozwiązań na uznanych i przyjętych standardach międzynarodowych, które będą warunkowały interoperacyjność, także transgraniczną, krajowej usługi wymiany EDM między usługodawcami.[88]

Finansowanie wprowadzanych w polskim publicznym systemie opieki zdrowotnej rozwiązań cyfrowych odbywało się do tej pory ze źródeł krajowych i wspólnotowych. Środki krajowe stanowią ok. 15 proc. wkładu własnego projektów, reszta to środki wspólnotowe z Funduszy Strukturalnych i Inwestycyjnych UE. W obecnym, nowym okresie programowania perspektywy finansowej UE na lata 2021–2027[89] kładzie się nacisk na rozwój obszaru cyfryzacji branży medycznej. Dodatkowo pojawiły się dotychczas nieznane instrumenty finansowe, takie jak fundusze specjalne Next Generation, z których są finansowa-

[85] Zdrowa_Przyszłość_tekst_uchwalony_27122021.pdf uchwałą nr 196/2021 Rady Ministrów z 27 grudnia 2021 r.

[86] https://ezdrowie.gov.pl/portal/artykul/dokumentacja-integracyjna-dla-obszaru-zdarzen-medycznych-i-indeksow-edm-czesc-pierwsza (dostęp: 1.05.2022).

[87] DzU z 2021 r., poz. 666 i 1292.

[88] https://ezdrowie.gov.pl/portal/artykul/zalety-prowadzenia-edm-w-tym-mozliwosci-jej-wymiany-miedzy-uslugodawcami (dostęp: 1.05.2022).

[89] Fundusze Europejskie na lata 2021–2027, Ministerstwo Funduszy i Polityki Regionalnej.

ne: REACT-UE[90] oraz Krajowy Plan Odbudowy i Zwiększania Odporności,[91] kładące nacisk na finansowanie e-rozwiązań w medycynie. Przedsięwzięcia cyfrowe w ochronie zdrowia mogą być finansowane także z krajowego programu Polski Ład, który jest rządowym planem odbudowy polskiej gospodarki po pandemii COVID-19. Jedynie w ramach KPO, REACT-EU oraz środków na politykę spójności w nowej perspektywie na lata 2021–2027 przeznaczono łącznie ponad 2 mld euro na cyfryzację i rozwój e-zdrowia.

Strategia „Zdrowa przyszłość" jest adresowana do wszystkich kluczowych grup interesariuszy – pacjentów, kadry medycznej, świadczeniodawców oraz dostawców rozwiązań IT. Ma doprowadzić do ewolucyjnej cyfrowej transformacji systemu ochrony zdrowia. Kierunkowe działania mają zapewnić lepszą opiekę pacjentom przez szersze wykorzystanie m.in. rozwiązań telemedycznych, rozwój usług cyfrowych zwiększających dostępność świadczeń opieki zdrowotnej, rozwój narzędzi teleinformatycznych (e-usług, infolinii, centrów telemonitoringu) jako wsparcia nawigacji pacjenta oraz wymiany informacji w systemie, utworzenie systemu monitorowania satysfakcji pacjenta z udzielonych świadczeń (m.in. przez rozwój funkcji IKP oraz z wykorzystaniem infolinii). Istotnym elementem ma być również stworzenie rozwiązań ułatwiających komunikację między profesjonalistami medycznymi: pracownikami medycznymi, farmaceutami, świadczeniodawcami i płatnikiem. Odrębne narzędzia powinny również umożliwiać komunikację z pacjentami, w tym prowadzenie zdalnych konsultacji. Jednym z działań jest weryfikacja koszyka i identyfikacja świadczeń w celu ich transformacji oraz jednoczesne wypracowanie standardów opieki, zasobów oraz komunikacji (działania edukacyjno-promocyjne – przeprowadzanie szkoleń dla pracowników medycznych i pacjentów, akcji informacyjno-promocyjnych). Dalsze działania mają zapewnić rozwój innowacji także w zakresie telemonitoringu, tworzenia metod i platform analitycznych do predykcji, diagnostyki i leczenia przez zapewnienie niezbędnego sprzętu i wydajnych łączy.

Główne wyzwania transformacji cyfrowej

Zastosowanie mechanicznego i cyfrowego zapisu stanu fizycznego oraz doświadczeń każdego z nas stworzyło grunt pod rewolu-

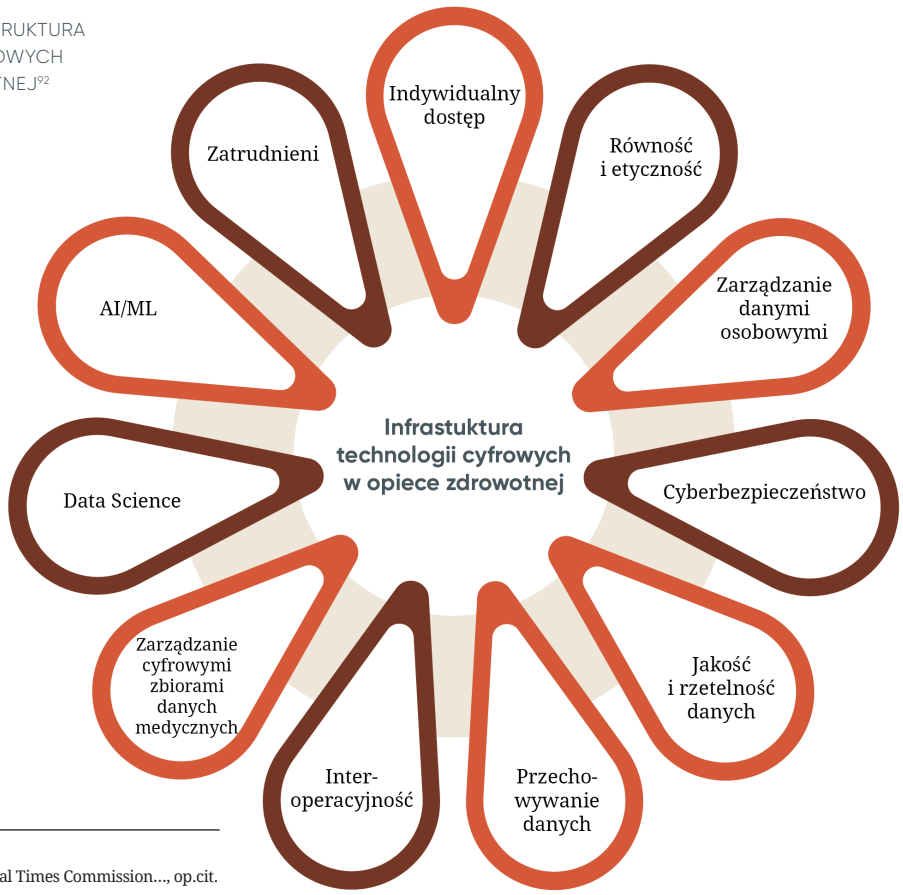
[90] REACT-EU | Komisja Europejska (europa.eu) REACT-EU to wsparcie finansowe na rzecz odbudowy służącej spójności oraz terytoriom Europy. Program stanowi rozwiązanie pomostowe poprzedzające realizację długoterminowego planu odbudowy. REACT-EU wspiera projekty inwestycyjne, które służą rozwijaniu zdolności do wdrażania kryzysowych środków naprawczych i przyczyniają się do ekologicznej i cyfrowej odbudowy gospodarki, zwiększając jej odporność (m.in. wsparcie na rzecz utrzymania miejsc pracy i stosowania mechanizmów zmniejszonego wymiaru czasu pracy oraz wsparcie dla samozatrudnionych). Program może również wspierać tworzenie miejsc pracy i zatrudnienie młodych, systemy ochrony zdrowia, zapewniać kapitał obrotowy oraz wsparcie inwestycyjne dla małych i średnich przedsiębiorstw.

[91] Przewidywany budżet dla Polski to 58 mld euro, w tym 4,5 mld euro na ochronę zdrowia. Źródło: O Krajowym Planie Odbudowy, Ministerstwo Funduszy i Polityki Regionalnej (funduszeeuropejskie.gov.pl).

cyjny postęp w indywidualnym zarządzaniu zdrowiem, strategiach zdrowotnych dla całej populacji oraz zintegrowanym generowaniu nowej wiedzy i informacji. Zarządzanie technologiami cyfrowymi w opiece zdrowotnej musi odbywać się z uwzględnieniem celów publicznych, gdyż ciągle gromadzone dane to wspólne dobro publiczne w ochronie zdrowia i ich bezpieczeństwo stanowi podstawę suwerenności cyfrowej państwa. Ogromne możliwości, jakie stwarza cyfrowa transformacja opieki zdrowotnej, rodzą poważne wyzwania w zarządzaniu na wielu poziomach systemu opieki zdrowotnej, które zostały stworzone na fundamentach zasad powszechności, równości, solidarności, integracji oraz prawach człowieka.

Ze względu na fakt, że wprowadzenie rozwiązań cyfrowych będzie prowadzić do wzrostu asymetrii władzy po stronie publicznej w stosunku do sektora prywatnego, konieczne jest zwiększenie zaufania publicznego do cyfrowego ekosystemu zdrowia oraz zapewnienie wykorzystania możliwości oferowanych przez technologie cyfrowe i dane w celu wsparcia upowszechniania dostępu do systemu opieki zdrowotnej. Dynamika zmian jest zależna od stopniowego rozwoju skomplikowanej infrastruktury cyfrowej oraz oceny jej funkcjonalności i uzyskiwanych efektów zdrowotnych jako fundamentu długofalowej transformacji w kierunku społeczeństwa informacyjnego.

RYSUNEK 10. INFRASTRUKTURA TECHNOLOGII CYFROWYCH W OPIECE ZDROWOTNEJ[92]



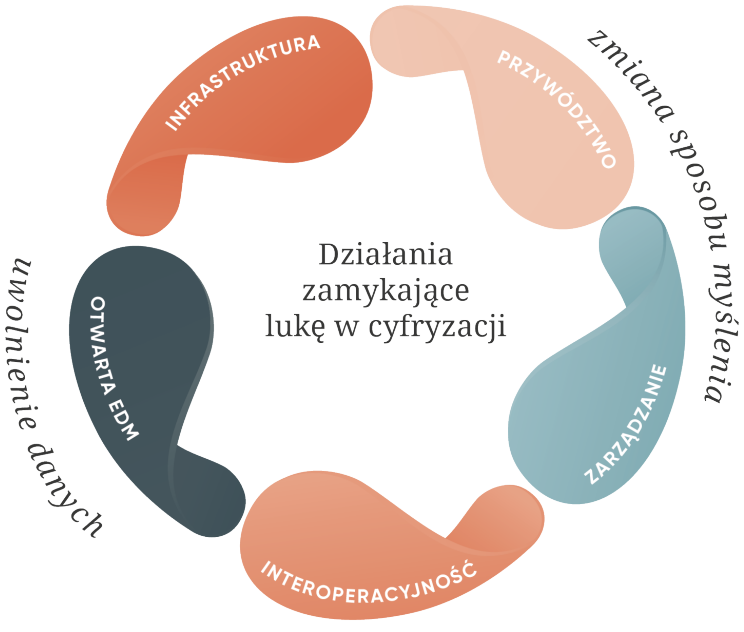
[92] The Lancet and Financial Times Commission..., op.cit.

Główne wyzwania rozwoju opieki zdrowotnej w czasie transformacji cyfrowej są związane ze wszystkimi elementami infrastruktury cyfrowej, a szerzej – ekosystemu cyfrowego. Różne kraje znajdują się na różnych etapach drogi do cyfrowej dojrzałości w zakresie ochrony zdrowia. Podstawą rozwoju inwestycji w drodze do sukcesu, zgodnie z zaleceniami WHO-ITU w zakresie strategii e-zdrowia, oraz przewodnikiem po inwestycjach w implementację cyfrową są kwestie związane z przywództwem, planowaniem strategicznym i zarządzaniem. Polska stopniowo przechodzi na wyższy poziom dojrzałości cyfrowej w zakresie ochrony zdrowia i powinna dążyć do spójnej architektury przedsiębiorstw zdrowotnych i planu inwestycji w cyfrowe zdrowie, które mogą pomóc rządowi, organizacjom pozarządowym i sektorowi prywatnemu w dostosowaniu decyzji inwestycyjnych do potrzeb systemu opieki zdrowotnej.

POLITYKA ZDROWOTNA PAŃSTWA, W TYM POLITYKA INNOWACJI

- *Wypracowanie modeli transparentnej współpracy i konsultacji społecznych w tworzeniu polityki zdrowotnej i planów operacyjnych w zakresie transformacji cyfrowej w ochronie zdrowia.*
- *Wypracowanie długofalowej strategii tworzenia funkcji, związanych z rozwojem precyzyjnej medycyny i zdrowia publicznego, innowacyjnych technologii cyfrowych dla wszystkich poziomów opieki zdrowotnej i dla wszystkich elementów koszyka świadczeń gwarantowanych i sektorów opieki zdrowotnej.*

RYSUNEK 11. KLUCZOWE DZIAŁANIA PROWADZĄCE DO ZNIWELOWANIA LUKI W CYFRYZACJI[93]



[93] Digital transformation. Shaping the future of European healthcare, Deloitte 2020, https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/life-sciences-health-care/deloitte-uk-shaping-the-future-of-european-healthcare.pdf.

- *Wdrażanie podejścia systemowego do zarządzania m.in. danymi dotyczącymi zdrowia w oparciu o solidarność danych, w tym stworzenie modeli współpracy prywatno-publicznej w zakresie przechowywania, gromadzenia i tworzenia funkcji oraz narzędzi cyfrowych w systemie opieki zdrowotnej.*

Zrozumienie i redefiniowanie zadań zdrowia publicznego oraz zasad funkcjonowania systemu opieki zdrowotnej jest konieczne dla wykorzystania nowych możliwości technologii cyfrowych, jednocześnie łagodzi potencjalne szkody związane z nieprawidłowym zarządzaniem zdrowiem. Stworzenie spójnej krajowej strategii i kompleksowych planów operacyjnych transformacji, z zaangażowaniem wszystkich interesariuszy, jest jednym z większych wyzwań transformacji cyfrowej. Kolejnym jest zdobycie zaufania obywateli, rozumiane także jako zmniejszenie ryzyka związanego z wdrażaniem technologii cyfrowych i osiąganiem zakładanych efektów zdrowotnych z jednoczesnym zadbaniem o bezpieczeństwo kliniczne pacjentów, oraz niwelowanie nierówności w zdrowiu.

Wymaga to przyjęcia polityki zdrowotnej nie tylko skupionej na rozwoju infrastruktury do zbierania i przechowywania danych czy wprowadzania nowych pojedynczych technologii, jako innowacji w celu poprawy wydajności systemu lub cięcia kosztów. Najistotniejszy jest sposób wykorzystania danych i rozwój ich funkcjonalności. Rozwiązania *big data* umożliwiają wprowadzenie medycyny spersonalizowanej (precyzyjnej), pozwalają także na rozwój precyzyjnej prewencji. Dlatego kluczowe jest pytanie, czy oprócz zwiększania dostępności, akceptacji i jakości usług zdrowotnych wraz z wdrażaniem wybranych elementów cyfrowego ekosystemu w planowaniu konkretnych rozwiązań uwzględniane są takie czynniki jak zmieniający się charakter opieki w całym systemie organizacji świadczeń, choćby zmierzanie w kierunku profilaktyki. W efekcie obniżenia progu wejścia w rozwiązania cyfrowe w systemie pojawią się nowe zjawiska oraz ryzyka i dopiero wielokierunkowe, wielopoziomowe działania (m.in. edukacja), angażujące wszystkich interesariuszy, pozwolą na ich eliminację lub przeciwdziałanie im. Wprowadzenie rozwiązań cyfrowych w sektorze publicznym, jakim jest opieka zdrowotna, wymaga ciągłego monitorowania zmian i ich koordynacji na poziomie krajowym, z uwzględnieniem zmian zachodzących na poziomie lokalnym, wprowadzanych przez samorządy oraz wszystkie grupy świadczeniodawców.

Podkreślamy potrzebę zbudowania architektury zarządzania i przywództwa, która zrodzi zaufanie do cyfrowego zdrowia dzięki upodmiotowieniu pacjentów (również grup wrażliwych społecznie i ekonomicznie oraz dzieci i młodzie-

ży), zapewnieniu kompleksowych praw cyfrowych oraz rzeczywistym regulacjom potężnych graczy w cyfrowym ekosystemie zdrowia.

ZAUFANIE DO SYSTEMU PUBLICZNEGO

Kluczowym aspektem rozwoju społeczeństwa cyfrowego jest zaufanie obywateli do systemu publicznego, za który odpowiada państwo. Zależy ono od tworzonych ram prawnych, dotyczących mechanizmów ochrony prywatności danych zdrowotnych, które uważane są za szczególnie wrażliwe, lecz także od przestrzegania przepisów i ich rzeczywistego stosowania.

Istotną rolę odegra tu nie tylko GPRD /RODO, ale i demokratyczna architektura przestrzeni danych, umożliwiająca dostęp do tego zasobu na bardziej egalitarnych zasadach, niż ma to miejsce w przypadku cyfrowych gigantów, z pozostawieniem najważniejszego prawa – decydowania o udostępnianiu swoich danych do wtórnego wykorzystania – w rękach każdego obywatela. Utrzymanie demokratycznych zasad jest zależne od wykorzystania danych w ramach systemu zarówno przez publiczne, jak i prywatne podmioty. Te prawa są bezpośrednio związane również z ich rzeczywistym przestrzeganiem i ewolucją relacji z kadrą medyczną i świadczeniodawcami, pomagając kształtować system opieki zdrowotnej. W świetle monitorowania praw istotna staje się poprawa kompetencji cyfrowych (przez ciągłą edukację) wszystkich interesariuszy systemu, co może też być najistotniejszą przyczyną opóźnień lub zagrożeń we wdrażaniu cyfrowej transformacji ochrony zdrowia.

Jednym z wyzwań w budowaniu zaufania publicznego jest łagodzenie szkód związanych ze środowiskiem cyfrowym, takich jak dezinformacja i bezpieczeństwo zdrowotne obywateli. Obecnie nieznane są możliwości wykorzystania informacji i porad dotyczących zdrowia w przyszłości. Wymaga to zbudowania zaufania do wiedzy na temat zdrowia, budowanej w oparciu o rosnące umiejętności cyfrowe. Narzędzia cyfrowe mają uzupełniać (a nie zastępować) bezpośrednie interakcje z pracownikami opieki zdrowotnej, także przez działania dotyczące podniesienia jakości dostępu do Internetu i usług zdrowotnych, z jednoczesnym szukaniem równowagi w zakresie obciążenia związanego z czasem aktywności online obywateli.

PRZYWÓDZTWO (LEADERSHIP) I ZARZĄDZANIE

W praktyce wdrażanie cyfrowej polityki zdrowotnej wymaga synergicznych działań ze strony decydentów. Po pierwsze, wymaga zrozumienia przez nich, że technologie cyfrowe są przyszłością systemu i będą podstawą jego funkcjonowania, obok konwencjonalnych technologii medycznych. Cyfrowa transformacja opieki zdrowotnej może zapewnić

medycynie szansę bycia bardziej ludzką i bliżej ludzi. Po drugie, konieczne jest znalezienie odpowiedniego tempa rozwoju rozwiązań cyfrowych w oparciu o konwencjonalne rozumienie zdrowia publicznego i zmian systemu opieki zdrowotnej. Wynika to z faktu, że przy obecnym kształcie systemu poszerzane będą dotychczasowe usługi zdrowotne i dodawane kolejne, jako nowe determinanty zdrowia. Po trzecie, niezbędne jest nowe podejście do gromadzenia i wykorzystywania danych dotyczących zdrowia, zgodne z koncepcją solidarności w zakresie zbierania danych, w celu ochrony praw jednostki, promowania potencjału danych dla dobra publicznego oraz budowania kultury sprawiedliwości i zrównoważonego kapitału.

Konieczne jest wreszcie stałe i stabilne zaangażowanie decydentów (polityków oraz organów państwowych) w inwestowanie w czynniki umożliwiające cyfrową transformację systemu opieki zdrowotnej. Zadanie to wymaga pełnej odpowiedzialności kraju za cyfrowe strategie zdrowotne i jasnych planów inwestycyjnych, które pomogą nadać priorytet technologiom najbardziej potrzebnym na różnych poziomach opieki wraz z rozwojem dojrzałości cyfrowej interesariuszy systemu, w tym obywateli/pacjentów. Przełożenie tych misji na portfolio inicjatyw, które ułatwią sprawiedliwe rozdzielenie korzyści płynących z cyfrowych technologii medycznych, sprawi, że wdrożenie nowych rozwiązań będzie wykonalne ekonomicznie. Zarządzanie będzie nieuchronnie zależne od kontekstu i oparte na unikalnych cechach różnych systemów opieki zdrowotnej oraz dojrzałości cyfrowej opieki zdrowotnej.

Zarządzanie i nadzór nad cyfrowymi narzędziami stanowią nowe wyzwania etyczne, związane z prawami człowieka. Nadzór jest konieczny do eliminacji białych plam w zakresie praw człowieka. Technologie cyfrowe mogą się przyczynić do zwiększenia solidarności i sprawiedliwości społecznej, a tym samym do rzeczywistego zmniejszenia nierówności zdrowotnych. Możliwe jest to jednak tylko wtedy, gdy zostaną zaprojektowane i wdrożone z uwzględnieniem nowych zasad etyki cyfrowej, opartej na integracji prawa z nowymi regulacjami, skupionymi wokół wspólnych wartości, takich jak prywatność, równość, sprawiedliwość, bezpieczeństwo pacjentów i autonomia człowieka w zakresie decyzji dotyczących zdrowia.

OTOCZENIE PRAWNE

- *Stworzenie ram prawnych dotyczących udostępniania danych zdrowotnych (np. zgody pacjenta na zabieg), z uwzględnieniem kwestii udostępniania danych w systemie publicznym i poza nim jako niezbędnego elementu integracji danych i funkcji.*

- *Opracowanie ram prawnych tworzenia i funkcjonowania składnic oraz wspólnic danych zdrowotnych, a także stworzenie modeli udostępniania danych pod kontrolą społeczną.*
- *Wdrażanie narzędzi cyfrowych z systemami oceny i planów zarządzania bezpieczeństwem zdrowotnym, a także ochroną danych pacjentów oraz obywateli.*

Nowe pokolenie dorasta wśród różnych doświadczeń związanych nierozerwalnie z cyfrowym światem, ale już obecnie przetwarzanie danych całego społeczeństwa stanowi cechę definiującą przyszłość ochrony zdrowia. Korzystanie z technologii cyfrowych prowadzi do pozostawiania danych lub śladów danych nie tylko osobowych, lecz coraz częściej zdrowotnych, np. w social mediach. To zjawisko datyfikacji ciała i oceny funkcji organizmu rozpoczyna się dzisiaj już przed urodzeniem człowieka. Datyfikacja to proces ciągłego cyfrowego monitorowania populacji przez cyfryzację w systemie, m.in. za pomocą urządzeń mobilnych, służących do monitorowania stanu zdrowia człowieka i funkcji jego organizmu nie tylko w systemie opieki zdrowotnej, lecz także w codziennym życiu (w szkole, w miejscu pracy, w domu).

Fundamentalnym warunkiem rozwoju narzędzi cyfrowych i poszerzania zakresu danych jest oczywiście stabilność i silne umocowanie prawne (przede wszystkim pod względem prywatności i bezpieczeństwa danych). Szczególnie istotne stają się kwestie dotyczące prawodawstwa obowiązującego w Polsce, zwłaszcza w świetle nowych danych genetycznych i genomicznych, np. danych gromadzonych w biobankach. Sposób wykorzystania danych przez system publiczny lub prywatny jest coraz częściej oparty na innowacyjnych rozwiązaniach, które powinny zaspokajać potrzeby zdrowotne społeczeństwa oraz konkretnego pacjenta. Także dostęp do zagregowanych danych medycznych, które mogłyby pomóc w podejmowaniu decyzji dotyczących organizacji systemu opieki zdrowotnej czy procesu terapeutycznego, jest obecnie utrudniony z powodu braku odpowiednich regulacji prawnych w zakresie wymiany informacji między świadczeniodawcami a sektorem prywatnym.

W praktyce i z perspektywy pacjentów na plan pierwszy wysuwa się konieczność zapewnienia właściwego poziomu bezpieczeństwa generowania, przetwarzania i udostępniania danych u każdego świadczeniodawcy. Pacjenci obawiają się przede wszystkim przyszłego wykorzystania danych wrażliwych (w rozumieniu RODO). W obowiązujących przepisach istnieje dość duża niespójność definicyjna. Pojęcia takie jak dokumentacja medyczna, dane o stanie zdrowia czy dane zaszyfrowane nastręczają problemów interpretacyjnych, bo ustawo-

dawca nie zadbał o precyzyjną redakcję uregulowań prawnych. Dodatkowo RODO, wprowadzając rozróżnienie na całkowicie i nie w pełni zanonimizowane dane o stanie zdrowia, utrudniło ich wymianę. Bariery prawne (obok braku odpowiedniej publicznej infrastruktury) już stają się widoczne w ramach podejmowanych reform systemowych (przykład: problemy z wdrażaniem rozwiązań telemedycznych w Polsce). Obecny brak rozwiązań prawnych nie pozwala na bezpieczne pobieranie w jednolity sposób danych zanonimizowanych, co ogranicza możliwości rozwoju analityki oraz współpracy lokalnej świadczeniodawców. Istotnym wieloletnim problemem jest brak spójnej komunikacji i centralnej koordynacji w zakresie licznych aktów prawnych tworzonych na poziomie centralnym, co nie pozwala na kompleksowe wprowadzanie konkretnych zagadnień.

Istotnym czynnikiem rozwoju jest wypracowanie ram strategicznych i jasnych zasad prawnych współpracy między instytucjami hostującymi i zarządzającymi elektroniczną dokumentacją medyczną (EHR) a podmiotami prywatnymi, szczególnie firmami z branży IT (w tym dużymi graczami komercyjnymi). Takie zagregowane dane z dużych prób, baz szpitali lub rejestrów medycznych są trudno dostępne nawet dla podmiotów publicznych i prawie niedostępne dla prywatnych podmiotów ochrony zdrowia, a tym bardziej dla pojedynczych naukowców. Obecnie najszerzej w Polsce wykorzystywane są dane KRN oraz zasoby NFZ, z ograniczeniami dostępu choćby z rejestrów medycznych ministra zdrowia (np. wad wrodzonych itd.).

Warunkiem koniecznym do rozbudowy funkcji jest poprawa otoczenia prawnego, szczególnie prawa dostępu do danych medycznych i ich wykorzystania w aspekcie naukowym, klinicznym, zarządczym, komunikacji, a także w ramach współpracy z sektorem prywatnym. Właścicielem danych publicznych jest przede wszystkim sam pacjent i on ma prawo udostępnienia swojej dokumentacji medycznej dowolnej osobie czy instytucji. Ważnym aspektem prawnym jest możliwość wykorzystania gromadzonych danych. Dylematy dotyczą nadmiernej ingerencji państwa w kwestie prywatne obywateli. Niejasne są też przepisy dotyczące współpracy publiczno-prywatnej oraz standardy kontroli danych (tj. klauzule *opt-out*) oraz rozwoju „tokenów cyfrowych" jako nowych narzędzi rynku kapitałowego, który wymaga pilnych regulacji.

WYKORZYSTANIE DANYCH I FUNKCJI TECHNOLOGII CYFROWYCH

- *Zbudowanie szerokiego i spójnego procesu refundacyjnego wraz z wdrażaniem i monitorowaniem rozwiązań lub technologii cyfrowych w opiece zdrowotnej pod kątem skuteczności i bezpieczeństwa pacjenta oraz opłacalności.*

- *Określenie funkcji kluczowych dla rozwoju świadczeń na wszystkich poziomach opieki zdrowotnej przez integrację danych (demograficznych, genetycznych, klinicznych, dotyczących uwarunkowań społeczno-ekonomicznych) i potrzeb wszystkich interesariuszy systemu, także w celu eliminowania nierówności w ochronie zdrowia.*
- *Wypracowanie kompleksowego modelu poprawy jakości danych na poziomie świadczeniodawców z oceną zasadności i ryzyka dla użytkowników oraz rozwojem narzędzi wizualizacji danych dla interesariuszy systemu.*
- *Edukacja i podnoszenie umiejętności cyfrowych społeczeństwa i kadry medycznej (społecznej) w zakresie nowych rozwiązań cyfrowych oraz stworzenie spójnej strategii informacji na ich temat w systemie.*

W podejmowaniu decyzji kształtujących współcześnie ochronę zdrowia dominują dwa trendy: **analiza dużych danych populacyjnych** i związane z nią szukanie narzędzi umożliwiających ich sprawne gromadzenie i przetwarzanie, a także **zwrócenie się w stronę medycyny spersonalizowanej,** w dalszej perspektywie mogące przynieść ogromne korzyści, i to zarówno pacjentowi, jak i całemu systemowi.

Już obecnie w gromadzonych danych drzemie olbrzymi potencjał, który nie jest wykorzystywany. Jeszcze przez długi czas nie będzie możliwości wykorzystania danych stale gromadzonych przez różne instytucje. Konsolidacja danych pochodzących z różnych zbiorów w celu ich integracji, a następnie analizy, jest podstawą poprawy jakości zarządzania oraz opieki nad pacjentami. Dane przechowywane przez różne instytucje publiczne, np. NFZ, KRN, rejestry narządowe czy ZUS, są w Polsce dostępne jedynie dla wybranych instytucji centralnych, także zakres analityki ma przede wszystkim wymiar centralny. Bardzo duża ilość danych surowych, gromadzona przez świadczeniodawców, biurokracja, brak ich uporządkowania nie pozwala na rozwijanie systemów oraz ich prospektywną ocenę przez pacjenta i lekarza. Tymczasem dane mogą być albo po prostu wprowadzone do systemu elektronicznego, zgodnie z określonymi wymaganiami, albo wzbogacone o narzędzie informatyczne, które pozwala na ich analizę i dostarczenie potrzebnych opracowań, raportów na poziomie centralnym, lokalnym oraz świadczeniodawców (m.in. w czasie rzeczywistym).

Dodatkowo olbrzymią barierą w zwiększeniu funkcjonalności jest niekompletność lub niska wartość danych. Wynika to m.in. z konieczności dotrzymania krótkich terminów wprowadzania danych, braku systemu gratyfikacji za dotrzymanie terminów i prawidłowe wprowadzenie danych oraz sankcji za nieterminowość, wpisanie danych niepełnych lub

nieprawidłowych. Proces przekazywania/wprowadzania danych jest jednym z najsłabszych elementów całego systemu i wynika przede wszystkim z mnogości wdrażanych rozwiązań, biurokracji, niedostatków kadrowych oraz braku możliwości rzeczywistej oceny przydatności proponowanych rozwiązań.

W Polsce szczególnie brakuje jednak rozwiązań pozwalających na premiowanie działań podnoszących jakość leczenia, m.in. w oparciu o dane. Nawet w działaniach podejmowanych centralnie wydatki na stworzenie rozwiązań bazodanowych nie są uwzględniane w odpowiedni sposób, a analiza danych (najczęściej retrospektywna) spoczywa na kadrze medycznej. Rozwijanie i tworzenie wskaźników jakościowych nie tylko zależy od potrzeb pacjentów, lecz jest uwarunkowane zakresem zbieranych danych i ich kompletnością.

Za wprowadzanie danych do systemów informacyjnych odpowiedzialna jest kadra medyczna, lecz najbardziej obciążeni wydają się lekarze i coraz częściej pielęgniarki. Obowiązek wprowadzania danych jest czasochłonny, wymaga zapoznania się z licznymi procedurami oraz formularzami, a równocześnie ogranicza czas kontaktu z pacjentami. Podobnie jak korzystanie z tych danych we współpracy z pacjentami czy w celach naukowych. Ze względu na liczne instytucje i ich odmienne kompetencje systemowe istotnym problemem jest odpowiedzialność każdego z interesariuszy za jakość gromadzonych danych, co dodatkowo utrudnia integrację. Niepełność zbiorów danych oraz brak odpowiednich narzędzi do ich analizy nie pozwala na właściwą modyfikację podejmowanych działań. Kadra medyczna od wielu lat postuluje nie tylko wprowadzanie systemów EDM, lecz także stworzenie funkcjonalnych i intuicyjnych narzędzi do korzystania z danych (np. w postaci dashoboardów) w celu monitorowania opieki nad chorym i automatyzacji procesów zbierania danych. Dane dotyczące pojedynczego pacjenta są gromadzone w rejestrach, ale nie docierają zwrotnie do lekarzy, a często nie są podstawą zmian w wytycznych/standardach opieki, co stanowi jeden z przykładów niewykorzystania ich potencjału. To nie tylko polski problem, mierzą się z nim także inne państwa, poszukując różnych rozwiązań (np. National Health Service w Wielkiej Brytanii). Nie ma kraju, który miałby dobrze opracowany model pozwalający na rozwiązanie tego problemu.

Istnieje wiele podmiotów odpowiedzialnych za gromadzenie danych o obywatelu, także w ochronie zdrowia, a zakres ich kompetencji nie pozwala na spójną analizę danych (mapy potrzeb zdrowotnych, raporty NFZ na temat konkretnych obszarów zdrowotnych, dane ZUS). Poza tym w zakresie tworzenia lub zmiany koszyka świadczeń gwarantowanych,

w tym włączania nowych technologii cyfrowych (np. wyrobów medycznych II lub III klasy w leczeniu szpitalnym), nieuwzględniane są aspekty cyfrowe świadczeń czy możliwości wykorzystania gromadzonych danych. Duża liczba rozwiązań przypisanych poszczególnym obszarom prowadzi do chaosu organizacyjnego i obciążenia kadr medycznych, spadku zaufania do wdrażanych narzędzi, a w konsekwencji do niespójności oraz niskiej jakości danych. Dodatkowe utrudnienia wynikają z faktu, że po różne dane trzeba zwracać się do różnych podmiotów – proces uzyskania dostępu do danych wymaga więc wiedzy o tym, kto je przechowuje i w jakim zakresie je udostępnia. Nie jest to system przyjazny dla użytkowników, nawet publicznych instytucji czy naukowców.

Głównym ograniczeniem tworzonych rozwiązań jest brak analizy ich kompleksowości, mapowania na poziomie centralnym czy lokalnym oraz celów długoterminowych dotyczących analityki. Obecnie zgromadzone dane służą głównie do tworzenia dokumentów dotyczących sytuacji epidemiologicznej (choć nie dla wszystkich chorób) lub analizie tylko określonych rozwiązań oraz technologii stosowanych w Polsce. Podejmowane są także działania w kierunku monitorowania skuteczności diagnostyki i leczenia w poszczególnych placówkach – dokonywania porównania jakościowego. To złożony proces, który powinien uwzględniać wskaźniki dotyczące zjawisk negatywnych, czyli zagrożeń bezpieczeństwa pacjentów (wskaźnik powikłań pooperacyjnych, błędów medycznych), ale także zjawisk pozytywnych, które są znacznie trudniejsze do zaplanowania (efektywność ścieżek postępowania, kompleksowego leczenia np. pacjentów z niewydolnością serca).

W procesie tworzenia systemowych rozwiązań w ochronie zdrowia ważną rolę odgrywa Agencja Oceny Technologii Medycznych i Taryfikacji, która analizuje proces leczenia na podstawie zebranych danych medycznych także z ekonomicznego punktu widzenia. Taka analiza pozwala na bardziej efektywne kosztowo zarządzanie procesem opieki oraz tworzenie koszyków świadczeń gwarantowanych. Głównym ograniczeniem w prowadzeniu analiz przez AOTMiT jest sposób gromadzenia danych (liczne bazy), przetwarzania (odmienne zakresy danych) oraz rozproszenie procesów analitycznych (MZ, NFZ, CEZ). Agencja potrzebuje danych pozwalających na rzeczywistą ocenę skutków zdrowotnych oraz faktycznych kosztów poszczególnych świadczeń, tymczasem napotyka trudności nie tylko techniczne, lecz także związane z transparentnością procesów. Rozwiązaniem mogącym poprawić proces analizy, a ostatecznie także wykorzystania zgromadzonych danych, byłoby według niektórych ekspertów stworzenie interdyscyplinarnego

RYSUNEK 12. NAJWAŻNIEJSZE WYZWANIA DLA ORGANIZACJI IMPLEMENTUJĄCYCH ROZWIĄZANIA CYFROWE

zespołu, który potrafi dostrzec potencjał tkwiący w zgromadzonych danych, wypracować modele pozwalające przygotowywać prognozy, procedury dotyczące najbardziej palących potrzeb ochrony zdrowia w Polsce.

BEZPIECZEŃSTWO ZDROWOTNE PACJENTÓW

Niezwykle ważne jest również edukowanie personelu i pacjentów w zakresie środków bezpieczeństwa i najlepszych praktyk, które zmniejszają ryzyko naruszenia z jednej strony bezpieczeństwa danych, a z drugiej – bezpieczeństwa pacjenta. Ograniczenie dostępu niektórych pracowników do dokumentacji pacjentów za pomocą różnych metod uwierzytelniania stanowi dodatkową strefę ochronną. Oczywiście, jak wcześniej wspomniano, kwestie prawne są w Polsce stopniowo rozwiązywane, lecz nie wyprzedzają tworzonych rozwiązań ani zastosowań narzędzi cyfrowych

w ochronie zdrowia. Przygotowanie planów zarządzania kryzysowego dla rzadkich, lecz poważnych sytuacji naruszenia praw pacjenta wymaga także przedefiniowania roli rzecznika praw pacjenta i wdrożenia systemów monitorowania bezpieczeństwa zdrowotnego pacjenta na poziomie konkretnego świadczeniodawcy oraz na poziomie integracji opieki u różnych świadczeniodawców. Wraz z wdrażaniem narzędzi czy rozwiązań cyfrowych muszą być opracowywane plany oceny bezpieczeństwa zdrowotnego pacjenta, systemy reagowania nawet na małe incydenty. Powstaje również konieczność ciągłego ich aktualizowania. Tworzenie rozwiązań skierowanych do pacjentów wymaga pogłębionych analiz w zakresie sposobu komunikacji, budowania kompetencji cyfrowych rozumienia przekazywanych treści i intuicyjności zastosowanych rozwiązań.

NIERÓWNOŚCI W OCHRONIE ZDROWIA

Polska, tak jak inne kraje europejskie, dąży do osiągnięcia celów systemów opieki zdrowotnej, które obejmują wysoką jakość, efektywność, równość, przystępność cenową i dostępność opieki zdrowotnej. Równość w opiece zdrowotnej jest wypadkową działań podejmowanych zarówno w ochronie zdrowia, jak i w innych dziedzinach życia, czyli w szeroko rozumianych uwarunkowaniach środowiskowych. Rozwój systemu opieki zdrowotnej obejmuje różnego rodzaju kompromisy (choćby w zakresie czystości powietrza w Polsce w zestawieniu z polityką energetyczną państwa), a ich równoważenie jest ciągłym procesem, opartym na decyzjach podejmowanych przez decydentów i samych obywateli. Wiele krajów boryka się z jednej strony ze stymulowaniem cyfryzacji i implementowaniem usług cyfrowych w celu poprawy wydajności, a z drugiej strony z oceną skutków podejmowanych działań, w tym rzeczywistej równości w dostępie do opieki zdrowotnej czy poprawy zdrowia obywateli.

Technologie cyfrowe już teraz napędzają przemiany zdrowotne bezpośrednio (przez ich zastosowanie w opiece zdrowotnej oraz w samokontroli stanu zdrowia i zachowań jednostki) i pośrednio (przez wpływ na społeczne, ekonomiczne i środowiskowe uwarunkowania zdrowia). Transformacje cyfrowe prowadzą do zmiany wymiarów w relacjach międzyludzkich i tworzą nowe terytoria cyfrowe, umożliwiając rozwój gospodarczy i społeczny. Obecnie zaczynamy widzieć fundamentalne zmiany w sposobie organizacji naszego społeczeństwa, najbliższego środowiska oraz całego kraju. Transformacja cyfrowa staje się determinantą zdrowia, obok tradycyjnych, z którymi jest związana, np. edukacji.

Stworzenie nowych modeli wdrażania innowacji, m.in. biznesowych, nie ma

jasnych podstaw w wartościach społecznych i zasadach etycznych w odniesieniu do zdrowia i jego cyfrowych uwarunkowań. Po pierwsze, dostęp do cyfrowego sprzętu i oprogramowania stanowi fundament integracji technologii cyfrowych z życiem obywateli i określa zdolność do przezwyciężania istniejących podziałów cyfrowych i budowania gotowości cyfrowej. Ponieważ systemy opieki zdrowotnej stają się coraz bardziej cyfrowe i wzajemnie połączone, elementy takie jak dostęp do łączności, interoperacyjność danych i ich bezpieczeństwo również stały się kluczowe dla zmiennej zdolności kraju do wykorzystania takiej technologii w celu sprawiedliwego osiągnięcia celów zdrowotnych. Innowacyjne rozwiązania, które reprezentują pewne cyfrowe usługi zdrowotne, mogą (ale nie muszą), jeśli zostaną zaprojektowane celowo i wdrażane w sposób efektywny kosztowo, zapewnić lepsze wyniki zdrowotne i przyczynić się do zwiększenia stabilności systemów opieki zdrowotnej.

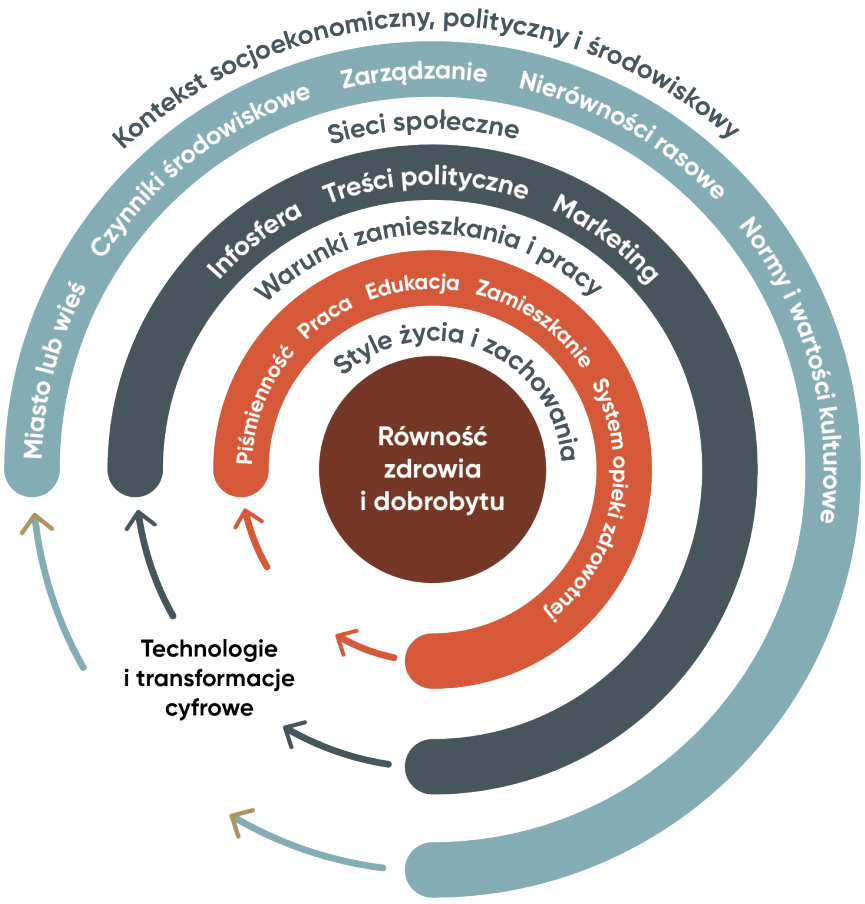
Ewaluacja i monitorowanie dostępu oraz efektów zdrowotnych powinny być stałymi elementami zarządzania, także w przypadku określonych cyfrowych usług zdrowotnych czy innowacyjnych. Zakres takiej oceny, również przy zarządzaniu systemem, musi być stale monitorowany i dostosowywany do potrzeb konkretnych grup społeczno-ekonomicznych, szczególnie dzieci i ludzi starszych. Podkreślenia wymaga fakt, że osiąganie celów zdrowotnych dla jednych grup może przynosić negatywny efekt w innych grupach. Samo wdrożenie rozwiązań bez odpowiedniego przeszkolenia personelu lub pacjentów może ograniczać dostęp do opieki zdrowotnej lub prowadzić do różnych efektów w określonych grupach chorych, łącznie z pogorszeniem stanu zdrowia. Co więcej, ze względu na wpływ, jaki dynamika dostępu cyfrowego może mieć na wyniki w zakresie zdrowia i dobrego samopoczucia, możemy uznać ekosystem cyfrowy za coraz ważniejszy wyznacznik zdrowia.

UMIEJĘTNOŚCI CYFROWE SPOŁECZEŃSTWA

Kluczowe znaczenie będzie miało budowanie i wykorzystywanie umiejętności cyfrowych całego społeczeństwa, szczególnie młodych ludzi oraz personelu medycznego i opieki społecznej wraz z kadrą zarządzającą. Istotnym aspektem jest brak odpowiednich kompetencji cyfrowych u wszystkich interesariuszy systemu, co stanowi najistotniejszą przyczynę opóźnień we wdrażaniu cyfrowej transformacji i prowadzi do nierówności w dostępie do opieki zdrowotnej.

Na szczeblu europejskim kompetencje cyfrowe są uznawane i definiowane jako jedne z kluczowych w procesie uczenia się przez całe życie. Po raz pierwszy na arenie europejskiej wspomniano

RYSUNEK 13. RELACJE MIĘDZY TECHNOLOGIAMI CYFROWYMI A DETERMINANTAMI ZDROWIA[94]



o nich w 2006 r. w Zaleceniach Parlamentu Europejskiego i Rady w sprawie kompetencji kluczowych przez całe życie.[95] Kompetencje informatyczne zostały ostatecznie zdefiniowane w 2018 r. jako „pewne, krytyczne i świadome korzystanie z technologii cyfrowych w celu nauki, pracy i uczestnictwa w życiu społecznym".[96]

Edukacja cyfrowa obejmuje dwa główne nurty: rozwój kompetencji cyfrowych obywateli, w tym pacjentów, oraz kadry medycznej i zarządzającej. Programy szkoleniowe są podstawowymi narzędziami budowania umiejętności cyfrowych i umiejętności korzystania z danych kadry medycznej, pracowników socjalnych, ale także decydentów i organów regulacyjnych w dziedzinie zdrowia. Z perspektywy rynku pracy istnieje luka w umiejętnościach. Coraz większa liczba stanowisk w opiece zdrowotnej wymaga podstawowych umiejętności w dziedzinie technologii informacji i komunikacji (TIK). Programy szkoleń powinny obej-

[94] The Lancet and Financial Times Commission..., op.cit.

[95] Recommendation of the European Parliament and of the Council of 18 December 2006 on key competences for lifelong learning, OJ L 394, 30.12.2006.

[96] https://rada.wib.org.pl/wp-content/uploads/2021/01/Edukacja-cyfrowa-w-UE.pdf.

mować okresową aktualizację zmian technologicznych i budowanie umiejętności cyfrowych pracowników służby zdrowia przez wyposażenie ich w możliwości i narzędzia potrzebne do zapewnienia wyższej jakości opieki, bardziej skoncentrowanej na pacjencie, zwłaszcza na obszarach wiejskich. Jednak silna potrzeba zbudowania nowych zasobów jako siły roboczej z zakresu zarządzaniami informacjami czy informatyką zdrowotną istnieje nawet w innych środowiskach niż kadra medyczna.

W zakresie edukacji społeczeństwa stworzono „Europejskie ramy kompetencji cyfrowych dla obywateli", znane również jako DigComp, które szczegółowo opisują modelowe kompetencje informatyczne i zostały już wykorzystane przez wiele krajów europejskich (w tym Polskę). DigComp dzieli kompetencje informatyczne na pięć obszarów: (1) kompetencje informacyjne i kompetencje w zakresie przetwarzania danych, (2) komunikację oraz współpracę, (3) tworzenie treści cyfrowych, (4) bezpieczeństwo i (5) rozwiązywanie problemów. W ramach rozwoju społeczeństwa informacyjnego powstają luki w podstawowych umiejętnościach, które mogą pogłębiać nierówności w ochronie zdrowia, także z powodu niekorzystania z rozwiązań cyfrowych w codziennym życiu.

Istnieje pilna potrzeba ukierunkowania cyfrowych priorytetów zdrowotnych na ustanowienie silnych podstaw dla cyfrowej ochrony zdrowia już od dziecka. Cel ten będzie wymagał w szczególności dostosowania usług zdrowotnych do populacji najmłodszych, gdyż budowanie zdrowia na wczesnych etapach życia ma kluczowe znaczenie dla kapitału ludzkiego w zmieniających się na przestrzeni życia uwarunkowaniach społeczno-ekonomicznych. Dzieci i młodzież już dzisiaj mają największy i najbardziej zróżnicowany kontakt ze światem cyfrowym (najczęściej też cierpią z powodu negatywnych skutków tych interakcji). Zbudowanie odpowiednich kompetencji cyfrowych to także promocja zdrowia w tym obszarze i możliwości rzeczywistego kształtowania społeczeństwa informacyjnego, także jako świadomych przyszłych pacjentów czy wyszkolonej kadry w systemie opieki zdrowotnej.

Innym istotnym aspektem wpływającym na gromadzenie i wykorzystanie danych jest brak informacji dla pacjentów na temat prowadzonych działań zdrowotnych (profilaktycznych czy w zakresie opieki), badań klinicznych, komercyjnych i niekomercyjnych, na poziomie poszczególnych ośrodków oraz w skali kraju. Co więcej, niedostatek informacji obejmuje nie tylko badania technologii lekowych, lecz także innowacji organizacyjnych, polegających na wykorzystaniu np. rozwiązań telemedycznych czy innych z obszaru e-zdrowia, nie tylko w komunikacji pomiędzy pacjentami a świadczeniodawcami, ale również między podmiotami leczniczymi.

RYSUNEK 14. ZARZĄDZANIE OCHRONĄ ZDROWIA W PRZYSZŁOŚCI[97]

Otoczenie ekonomiczno-finansowe

- *Wypracowanie długofalowych planów inwestycji w e-zdrowie i konieczność finansowania utrzymania oraz rozwoju systemów i nowych inwestycji w ochronie zdrowia.*
- *Konieczne wypracowanie propozycji modeli finansowania współpracy prywatno-publicznej przy wdrażaniu rozwiązań cyfrowych i ich utrzymaniu lub nowych inwestycji.*
- *Rozbudowa systemu inwestycji w polskie firmy cyfrowe albo inicjatywy start-up (naukowe, informatyczne, szkoleniowe, konsultingowe) jako model wsparcia świata nauki i polskiej gospodarki.*

[97] The Lancet and Financial Times Commission..., op.cit.

Wprowadzenie nowych rozwiązań do systemu ochrony zdrowia pociąga za sobą długofalowe wydatki, które są i będą finansowane z różnych źródeł (MZ, NFZ, granty naukowe, finansowanie przez podmioty komercyjne). W tym kontekście transformacje cyfrowe zmieniają również nasze konwencjonalne rozumienie ekonomii zdrowia. W każdym kraju konfiguracja podmiotów zaangażowanych w gospodarkę zdrowotną zawsze była zróżnicowana, w zależności od tego, czy świadczeniem usług zdrowotnych zajmowały się podmioty z sektora publicznego czy prywatnego. Firmy z sektora prywatnego zapewniają znaczną część usług zdrowotnych.[98]

Wprowadzanie rozwiązań cyfrowych jest kosztochłonne, a ich zmiana, utrzymanie i integracja wymagają dodatkowych nakładów finansowych ze strony przede wszystkim świadczeniodawców. Rozwiązania zastosowane na poziomie centralnym (w ramach platformy P) nie pozwalają na transformację w poszczególnych obszarach zdrowotnych lub u określonych grup świadczeniodawców. Zarówno rozwój własnych systemów informatycznych świadczeniodawców, jak i coraz częściej implementacja cyfrowych technologii medycznych, wymagają inwestycji. Tymczasem ich finansowanie nie jest możliwe z środków publicznych, przeznaczonych na realizację świadczeń zdrowotnych. Jeśli chodzi o konkretne technologie, np. sztuczną inteligencję, nie znamy jeszcze ich wpływu na zdrowie, nie mamy też ram oceny efektywności ich zastosowania do osiągnięcia konkretnych efektów w zakresie zdrowia publicznego.

Coraz częściej niezbędne jest tworzenie struktur i rozbudowanie kadry biegłej w kwestiach cyfrowych/informatycznych u świadczeniodawcy czy płatnika, ze względu na konieczność indywidualnego dostosowania rozwiązań do potrzeb kadry medycznej i zakresu wykonywanych świadczeń oraz poniesienia wysokich kosztów dostosowania oprogramowania zewnętrznych dostawców. Inwestycja w podniesienie kompetencji analitycznych i rozwój narzędzi analitycznych na wszystkich poziomach zarządzania opieką zdrowotną, ze względu na jej zróżnicowanie oraz potrzeby interesariuszy, jest kolejnym krokiem o znaczeniu strategicznym. Analizy mogą cechować się wielką różnorodnością, dlatego zakup narzędzi analitycznych jest bardziej uzasadniony niż przechowywanie ogromnej liczby danych analizowanych odrębnie dla różnych podmiotów. Odpowiednie finansowanie całego procesu ma kluczowe znaczenie dla jego przebiegu. Doświadczenie wskazuje, że dobrze działające rozwiązania funkcjonują na stabilnych i długofalowych podstawach finansowych. Jednakże oprócz

[98] The Lancet and Financial Times Commission..., op.cit.

tworzenia i rozwoju rejestrów medycznych niezbędne jest także finansowanie dalszego procesu informatyzacji i digitalizacji szpitali, a na poziomie centralnym – rozwój integralności i kompleksowości danych z tworzeniem narzędzi ich wykorzystania. Planowanie rozwoju systemów informatycznych świadczeniodawców w oparciu o wkład własny, ze względu na obecne problemy gospodarcze i falę uchodźców z objętej konfliktem zbrojnym Ukrainy, jest mało prawdopodobne.

Wyzwaniem zarówno w skali krajowej, jak i dla UE pozostają kwestie związane z bezpieczeństwem i ochroną danych. Ostatecznym celem prac jest opracowanie analizy prawnej w kontekście przyszłego ustanowienia europejskiej przestrzeni danych dotyczących zdrowia (*European Health Data Space*). Rozwiązanie to ma zapewnić krajom UE zarówno bezpieczeństwo danych, jak i interoperacyjność obejmującą rozszerzoną sferę rynkową oraz społeczną (obywatelską i indywidualną). Wyzwaniem jest silne zróżnicowanie cyfrowych/informatycznych ekosystemów zdrowia w poszczególnych państwach oraz ograniczenia w analityce na poziomie centralnym. Obecnie większość krajów nie dysponuje jeszcze systemami czy narzędziami umożliwiającymi maksymalizację korzyści płynących z cyfryzacji w ochronie zdrowia w sposób, który pozwoliłby wpłynąć na poprawę wyników zdrowotnych w wybranych obszarach.

Brak transparentności oraz przemyślanego skoordynowanego planu działania na rzecz kompleksowej cyfrowej opieki zdrowotnej prowadzi do utrwalenia fragmentacji i niewydolności systemu krajowego oraz lokalnych, a także działających u poszczególnych świadczeniodawców. Utrudnia to uzyskiwanie zakładanych korzyści z inwestycji zarówno w zakresie wydajności, jak i finansowym, w wymiarze krótko- i długoterminowym. Już obecnie zebrane dane nie są wykorzystywane, a nawet analizowane w sposób skoordynowany czy całościowy, a czas poświęcony na analitykę jest silnie związany z ograniczeniami zasobów ludzkich.

MARTA MUSIDŁOWSKA

Analityczka polskich, unijnych i amerykańskich regulacji związanych z nowymi technologiami, przede wszystkim w zakresie ochrony i zarządzania danymi osobowymi. Marcin Król Fellow w Visegrad Insight

JAN ZYGMUNTOWSKI

Współprzewodniczący Polskiej Sieci Ekonomii, dyrektor zarządzający CoopTech Hub, wykładowca Akademii Leona Koźmińskiego

ANNA PADIASEK

Młodsza analityczka programu badawczego gospodarki cyfrowej w Fundacji Instrat, studentka filozofii, politologii i ekonomii na uniwersytecie King's College London

04

Suwerenność cyfrowa w ochronie zdrowia

W niniejszym rozdziale szukamy odpowiedzi na pytanie, jakie horyzontalne zasady należy stosować przy tworzeniu cyfrowej infrastruktury w opiece zdrowotnej, aby 1) zapewnić operatorowi pełną kontrolę nad systemem i 2) zminimalizować ryzyko wystąpienia negatywnych zjawisk, typu uzależnienie od jednego dostawcy rozwiązań czy niekontrolowane użycie danych przez podmioty komercyjne?

Wskazujemy, że korzystanie z popularnych rozwiązań chmurowych, przede wszystkim oferowanych przez przedstawicieli Big Tech, może wydawać się najbardziej optymalne, ale pociąga za sobą ryzyko uzależnienia się od usługodawcy i nieprzestrzegania poziomu ochrony danych osobowych wyznaczonego przez RODO. Suwerenność cyfrową można osiągnąć przez inwestowanie w promocję lokalnych rozwiązań chmurowych przez sektor publiczny oraz ułatwianie dostępu do informacji o modelach zarządzania danymi. Aby uniknąć polegania na rozwiązaniach dostarczanych przez jednego dostawcę, powinno się stworzyć nową politykę zamówień publicznych, która będzie ułatwiała rozwój innowacji chmurowych na polskim rynku technologicznym, wspierając otwarte procesy zamówień na rozwiązania IT, w tym rozwiązania zarządzania danymi, oparte na licencjach typu Open Source.

Konieczne jest wprowadzenie ocen oprogramowania używanego w sektorze medycznym jeszcze przed ich wdrożeniem, aby wpływać na taryfikację rozwiązań stosowanych w ochronie zdrowia. Wynika to z tego, że wyceny świadczeń medycznych przeprowadzanych przy użyciu technologii z różnym oprogramowaniem mogłyby pokazywać rentowność danego rozwiązania nie tylko pod względem klinicznym, ale też z perspektywy cyfrowej. Z uwagi na budzące kontrowersje transfery specjalistów z sektora publicznego do firm prywatnych należy przyjąć kodeks etyczny dla pracowników sektora publicznego zatrudnionych przy cyfryzacji ochrony zdrowia i ustalić karencję, w trakcie której nie będzie można podjąć pracy w firmach prywatnych.

Opis zjawiska

Współczesna gospodarka i przedsiębiorstwa funkcjonujące w sieci podzieliły się na te, których niewielka grupa najskuteczniej korzysta z uwarunkowań wyznaczanych przez rewolucję cyfrową, i na te, które próbują za nimi nadążyć.[99] Rezultatem tego stanu rzeczy jest wyznaczanie zasad korzystania z przestrzeni cyfrowej przez kilka firm technologicznych i odbieranie jej użytkownikom możliwości egzekwowania własnych praw i ewentualnej zmiany warunków.

[99] J.J. Zygmuntowski, *Kapitalizm sieci,* Stowarzyszenie Rozruch, ISBN: 978-83-957-6720-3.

Ostatnio często mówi się o tzw. suwerenności cyfrowej. Biorąc pod uwagę, jak ważna jest nasza obecność w sieci, jej brak to brak kontroli nad rzeczywistością. Ma to szczególne znaczenie dla ochrony zdrowia, której cyfryzacja polega na umieszczaniu dużej ilości wrażliwych danych pacjentów w bazach opartych na rozwiązaniach chmury obliczeniowej. Wybieranie popularnych, lecz niedochowujących odpowiednich środków bezpieczeństwa rozwiązań, może stanowić zagrożenie dla prywatności pacjentów i narazić ich na wykorzystywanie ich danych w złej wierze. Niekontrolowane wdrażanie technologii, nawet mającej na celu pomaganie pacjentom, może spowodować „wysyp" ofert niebezpiecznych usług leczniczych. Znane są przypadki stron internetowych, na których wystarczy wypełnić formularz, podając swoje dane zdrowotne, by pod pretekstem konsultacji kupić receptę.[100] Możliwości techniczne, w połączeniu z brakiem odpowiednich regulacji w tym zakresie, zezwalających na udzielanie konsultacji i wystawianie recept, naraża wielu pacjentów na pogorszenie zdrowia w wyniku nieprofesjonalnie przeprowadzonych wywiadów i niedokładnie dobranych zaleceń. Tak udostępniane dane nie trafiają do rejestrów publicznych, jedynie do użytku komercyjnego, którego głównym celem jest osiągnięcie zysku, a nie ulepszanie „silnej" interoperacyjności danych dotyczących zdrowia.

Sprawozdania finansowe z „Wykonania planu wydatków Centrum e-Zdrowia w latach 2018–2021" wskazują, że w stosunku do kwot wydanych w 2018 r. budżet przeznaczony w 2021 r. na cyfryzację sektora medycznego wzrósł ponad dwukrotnie.[101] Zbierane dane dotyczą jednak jedynie perspektywy centralnej, podczas gdy wiele wydatków mogło być finansowanych z innych źródeł (regionalnych lub lokalnych). W ramach zbieranych statystyk brak również informacji, jaka część budżetu np. na teleporadę przeznaczana jest na infrastrukturę techniczną umożliwiającą jej dokonanie, a jaka dla lekarza, który ją przeprowadza. Nie istnieje też jeden spójny system wybierania dostawców oprogramowania wykorzystywanego w publicznych placówkach medycznych, ponieważ „podmioty lecznicze podejmują indywidualnie decyzje w zakresie wyboru rozwiązań informatycznych, spełniających warunek interoperacyjności z centralną architekturą zdrowia cyfrowego".[102] Jak

---

[100] A. Porażka, *Jak kupić receptę? Przeklikuję się przez myśli samobójcze, choroby nerek, wątroby, serca*, https://weekend.gazeta.pl/weekend/7,177334,27918647,jak-kupic-recepte-przeklikuje-sie-przez-mysli-samobojcze-choroby.html (dostęp: 6.03.2022). Zobacz także: M. Fraser, *Jak cyfrowy marketing poluje na przyszłe matki?* #CyberMagazyn 2021, https://cyberdefence24.pl/bezpieczenstwo-informacyjne/cybermagazyn-jak-cyfrowy-marketing-poluje-na-przyszle-matki (dostęp: 7.03.2022).

[101] Odpowiedź na interpelację nr 3092 posła Roberta Kwiatkowskiego w sprawie dostępu do informacji dotyczących cyfryzacji służby zdrowia, Ministerstwo Zdrowia 2022, https://interpelacje.sejm.gov.pl/interpelacje9.nsf/0/E8019F514173502EC12587EC0040E718/%24File/ODP_K9INT30932.pdf (dostęp: 6.03.2022).

[102] Ibidem.

wiadomo jednak z danych udostępnianych przez Asseco, ponad 450 szpitali miało system oferowany przez tę firmę,[103] a także 14 tys. przychodni i gabinetów lekarskich. Również system KSI ZUS jest dostarczany przez Asseco.[104]

Brak przepisów wskazujących procedury wyboru dostawcy dla placówek publicznych może prowadzić do sytuacji, która miała miejsce w 2021 r. i dotyczyła podejrzenia zmowy przetargowej między trzema podmiotami: Asseco Poland, Comarch Healthcare oraz Bestprojects. Wymienione firmy miały umawiać się w kwestii postępowań przetargowych na dostawę i wdrożenie systemów informatycznych wykorzystywanych przez służbę zdrowia.[105] Rozwiązaniem problemów z brakiem jednolitych standardów usług informatycznych w ochronie zdrowia miała być Chmura dla Zdrowia, powołana przez Asseco Poland i Chmurę Krajową dla dokonywania wdrożeń elektronicznej dokumentacji medycznej w chmurze, a także dostosowywania sektora do regulacji prawnych w zakresie cyfryzacji.[106] Chociaż firma przetwarza dane lokalnie i zgodnie z RODO,[107] oferuje m.in. rozwiązania w oparciu o chmury publiczne globalnych dostawców.

Zarysowanie możliwych kierunków zmian

W związku z newralgiczną naturą danych dotyczących zdrowia infrastruktura przeznaczona do ich gromadzenia powinna wykazywać się wyższym standardem bezpieczeństwa niż opracowana dla innych sektorów. Podobnie jak w przypadku RODO, ważne jest ustalenie zasad przetwarzania danych oraz współpracy między podmiotami biorącymi udział w całym procesie: od wyboru odpowiednich rozwiązań informatycznych po ich wdrożenie i utrzymanie. Dobrym rozwiązaniem byłoby przyjęcie Kodeksu Dobrych Praktyk lub rekomendacji sektorowych co do przetwarzania danych określonego rodzaju w chmurze, na wzór standardu PolishCloud dla sektora bankowego.[108]

---

[103] *Asseco wdraża e-Usługi w 9 szpitalach województwa lubelskiego*, Asseco Poland 2019, https://pl.asseco.com/aktualnosci/asseco-wdraza-e-uslugi-w-9-szpitalach-wojewodztwa-lubelskiego-3232/ (dostęp: 15.03.2022).

[104] Asseco Poland, 2022. Zakład Ubezpieczeń Społecznych, Case study, Asseco 2022, https://pl.asseco.com/case-study/kompleksowy-system-informatyczny-zus-96/ (dostęp: 6.03.2022).

[105] *Przeszukanie w Asseco Poland i Comarch Healthcare z powodu podejrzenia zmowy przetargowej, PAP Biznes 2021*, Bankier.pl, https://www.bankier.pl/wiadomosc/UOKiK-przeprowadzil-przeszukanie-w-Asseco-Poland-i-Comarch-Healthcare-z-powodu-podejrzenia-zmowy-przetargowej-8251029.html (dostęp: 6.03.2022).

[106] *Asseco i Chmura Krajowa razem dla e-Zdrowia,* Healthcare Market Experts 2021, https://healthcaremarketexperts.com/aktualnosci/rynek-trendy/asseco-i-chmura-krajowa-razem-dla-e-zdrowia/ (dostęp: 7.03.2022).

[107] *Lokalizacje – gwarancja bezpieczeństwa, Centrum Danych by Asseco 2022*, https://centrumdanych.asseco.cloud/lokalizacje/ (dostęp: 15.03.2022).

[108] *Standard Polishcloud 2.0. Standard wdrożenia usługi chmury obliczeniowej publicznej lub hybrydowej,* red. A. Gutenbaum, Związek Banków Polskich, Warszawa 2022.

Ze względu na ryzyko związane z niejasnością przepisów dotyczących przetwarzania danych w Stanach Zjednoczonych i możliwość wycieku danych do tamtejszych służb należy przede wszystkim każdorazowo sprawdzać, czy operacje na konkretnym zbiorze danych dotyczących zdrowia są zgodne z procedurą wyznaczoną przez Trybunał Sprawiedliwości Unii Europejskiej po wyroku Schrems II.[109] Ponadto rekomendowane jest poszukiwanie rozwiązań lokalnego przetwarzania danych w regionalnych wspólnicach danych, funkcjonujących jako ośrodki integrowania eksperckiej wiedzy o gospodarce informacyjnej.[110] Odzyskanie kontroli nad danymi użytkowników mogłoby zapobiec wyciekowi nie tylko danych dotyczących pacjentów, ale też wartości związanej z danymi dotyczącymi zdrowia, i przyczynić się do ulepszania własnych narzędzi AI.

Odzyskanie suwerenności cyfrowej nie mogłoby się odbyć bez określenia transparentnych zasad i ustrukturyzowanych wymogów, jakie powinny spełniać zamawiane, a następnie wdrażane technologie. Konieczne jest zatem wprowadzenie nowej polityki zamówień publicznych na usługi IT, nakierowanej na stworzenie inkluzyjnej infrastruktury publicznej.[111] Biorąc za wzór dobrze już funkcjonującą Politykę Lekową Państwa, dotyczącą wspólnych zakupów medykamentów, należy zastąpić rozproszony model wyboru dostawców struktury informatycznej modelem scentralizowanym, by wspierać jednocześnie interoperacyjność systemów ochrony zdrowia.

Analiza SLEPT

ASPEKTY SPOŁECZNE

Znajomość praw cyfrowych w kontekście ochrony zdrowia powinna obowiązywać przede wszystkim tych, którzy zajmują się zabezpieczeniem danych w placówkach sektora medycznego. Zgodnie z art. 37 ust. 1 RODO, podmioty publiczne, przetwarzające na dużą skalę dane wrażliwe, oraz podmioty, których główna działalność polega na monitorowaniu osób na dużą skalę, są odpowiedzialne za utworzenie stanowiska inspektora ochrony danych. Według informacji podawanych na stronach internetowych szpitali, inspektor jest odpowiedzialny za bezpośredni kontakt w imieniu szpitala z pacjentami w sprawach ochrony i przetwarzania ich danych. To on ma obowiązek udzielać odpowiedzi na pyta-

[109] C.D. Linebaugh, E.C. Liu, EU Data Transfer Requirements and the US Intelligence Laws: Understanding Schrems II and Its Impact on the EU-US Privacy Shield, Congressional Research Service, Version 3, 2021. Zobacz także: M. Fraser, Austriacki organ: korzystanie z Google Analytics narusza przepisy RODO, CyberDefence24, 2022, https://cyberdefence24.pl/prywatnosc/austriacki-organ-korzystanie-z-google-analytics-narusza-przepisy-rodo (dostęp: 7.03.2022).

[110] J.J. Zygmuntowski, op.cit.

[111] N.J. Bąk, J. Erbel, J. Galiński, P. Małańczuk, M. Pasierbski, J.J. Zygmuntowski, Spółdzielczy Plan Odbudowy: Raport, CoopTech Hub 2021.

nia związane ze zgodą na udostępnienie swoich danych i rozwiewać wątpliwości w kwestii bezpieczeństwa ich przetwarzania. W Wytycznych Grupy Roboczej do art. 29 wskazuje się, że powinna to być zatem osoba przygotowana fachowo do pełnienia niniejszej funkcji, dzięki wiedzy na poziomie „współmiernym do charakteru, skomplikowania i ilości danych przetwarzanych w danej jednostce".[112] Nie jest jednak wymagany żaden konkretny certyfikat poświadczający zdobycie określonych umiejętności czy odbycie przeszkolenia w zakresie ochrony danych i systemów informatycznych wykorzystywanych w ochronie zdrowia. Trudno więc określić, czy osoby wybierane na te stanowiska rzeczywiście spełniają określony wymóg profesjonalizmu.

W ostatnim czasie widoczny jest jednak trend polegający na otwieraniu kierunków studiów podyplomowych w zakresie „ochrony danych osobowych w sektorze medycznym", które przede wszystkim mają przygotowywać kandydatów do pełnienia funkcji inspektora ochrony danych osobowych w placówce medycznej.[113] Mimo jednak możliwego wzrostu profesjonalizmu osób kandydujących na stanowisko inspektora, dziś trudno ustalić, kto pełni funkcję inspektorów danych w publicznym sektorze zdrowia. Ze względu na warunek posiadania określonego poziomu doświadczenia i wiedzy merytorycznej z pewnością funkcji tych nie obejmują osoby krótko po ukończeniu studiów. Z drugiej strony osoby bardziej doświadczone i starszej daty mimo posiadanej wiedzy mogą nie znać problemów płynących z braku suwerenności cyfrowej placówek sektora medycznego i kierować się innymi parametrami, nieświadomie działając przeciw uwolnieniu się spod dyktanda cyfrowych gigantów. Szpitale rzadko udostępniają jednak informacje na temat tożsamości inspektorów danych, dlatego jakiekolwiek wnioski płynące z powyższych rozważań należy odsunąć na dalszy plan.

ASPEKTY PRAWNE

Nie ulega wątpliwości, że europejskie RODO stanowi pionierski projekt ochrony danych osobowych. Regulacja ta kompleksowo obejmuje swoją jurysdykcją sytuacje, w których siedziba podmiotu przetwarzającego dane osobowe znajduje się na terenie Unii Europejskiej, bez względu na to, gdzie faktycznie dochodzi do tego przetwarzania. Uwzględnia rozmaite aspekty związane z poszanowaniem prywatności osób fizycznych, pozostawiając jednocześnie pewien margines wyjątków niezbędnych w interesie

[112] Article 29 Working Party, Newsroom, Komisja Europejska 2022, https://ec.europa.eu/newsroom/article29/items/itemType/1358 (dostęp: 8.03.2022).

[113] *Ochrona danych w sektorze medycznym (inspektor ochrony danych) – studia podyplomowe*, otouczelnie.pl, https://www.otouczelnie.pl/artykul/18878/OCHRONA-DANYCH-OSOBOWYCH-W-SEKTORZE-MEDYCZNYM-INSPEKTOR-OCHRONY-DANYCH-STUDIA-PODYPLOMOWE (dostęp: 6.03.2022).

publicznym.[114] Każdorazowe przekazanie danych osobowych organom publicznym wymaga odpowiedniego dla danego celu uzasadnienia, z poszanowaniem zasady praworządności.

Ze względu na znaczące różnice w poziomie danych osobowych między regulacjami unijnymi a amerykańskimi w 2016 r. Komisja Europejska przyjęła decyzję nr 2016/1250 („Tarcza Prywatności"), zgodnie z którą transfer danych do podmiotów, które dobrowolnie zobowiązywały się do przestrzegania zasad ochrony danych osobowych zapisanych w „Tarczy Prywatności", był adekwatny do ochrony zapewnianej zgodnie z art. 45 ust. 1 RODO.[115] W wyniku skargi złożonej przez Maximiliana Schremsa do irlandzkiego organu ochrony danych osobowych, dotyczącej zasad umożliwiających przekazywanie danych osobowych z UE do Stanów Zjednoczonych, TSUE unieważnił „Tarczę Prywatności", orzekając, że dalszy transfer danych na podstawie niniejszej decyzji jest zabroniony. Powodem takiego rozstrzygnięcia były przede wszystkim budzące wątpliwości przepisy amerykańskie, będące podstawą funkcjonowania tzw. programów nadzoru wywiadowczego. Regulacje te nie spełniają bowiem wymogu nakładanego przez RODO, dotyczącego uzasadnionej niezbędności ingerencji w prawo do prywatności osób, których dane dotyczą. Co więcej, tamtejsze prawo nie w każdym przypadku zapewnia możliwość zaskarżania decyzji sądów przyznających poszczególnym organom uprawnienia „elektronicznej inwigilacji". Aby jednak całkowicie nie niweczyć transferu danych osobowych z EOG do państw trzecich, pozostawiono furtkę w postaci standardowych klauzul umownych, które mają ujednolicić postanowienia gwarantujące odpowiednią ochronę takiej operacji. Eksporter powinien jednak najpierw ocenić, czy importer danych będzie w stanie dopełnić warunków ochrony określonych w tych klauzulach, zwłaszcza przez pryzmat wewnętrznego prawa obowiązującego w tym państwie.[116]

Ostatnio austriacki Urząd Ochrony Danych Osobowych orzekł, że korzystanie z narzędzia Google Analytics (najpowszechniejszego programu statystycznego) nie jest zgodne z RODO. Max Schrems podkreślił, odwołując się do tej decyzji, że firmy nie mogą już korzystać z amerykańskich usług chmurowych w Europie.[117] Konieczna jest w związku

---

[114] X. Konarski, *Wyrok w sprawie Schrems II i jego znaczenie dla transferu danych do Stanów Zjednoczonych i innych państw trzecich*, Traple Konarski Podrecki i Wspólnicy Sp. J., 2020, https://www.traple.pl/2020/07/27/wyrok-w-sprawie-schrems-ii-i-jego-znaczenie-dla-transferu-danych-do-stanow-zjednoczonych-i-innych-panstw-trzecich/ (dostęp: 7.03.2022).

[115] Ibidem.

[116] R. Cumbley, T. Van Overstraeten, G. Kon, *The Schrems judgement – Transfer Impact Assessments for international data transfers?*, Linklaters 2020, https://www.linklaters.com/pl-pl/insights/blogs/digilinks/2020/july/the-schrems-judgment (dostęp: 7.03.2022).

[117] *Austriacki DSB: przekazywanie danych między UE a USA do Google Analytics niezgodne z prawem*, Noyb 2022, https://noyb.eu/pl/austriacki-dsb-przekazywanie-danych-miedzy-ue-usa-do-google-analytics-niezgodne-z-prawem (dostęp: 7.03.2022).

z tym zmiana po stronie amerykańskiego ustawodawcy lub całkowite uniezależnienie się od dostawców ze Stanów Zjednoczonych przez wybór lokalnej infrastruktury informatycznej.

Gromadzenie danych przez największe spółki jest możliwe dzięki nieuczciwym kontraktom zawieranym z innymi podmiotami. Ich celem jest wykorzystywanie nadzwyczajnych sytuacji i wyjątków w ochronie danych osobowych do wyciągnięcia jak największej ilości cennych danych możliwie najniższymi nakładami. Przykładem takiej sytuacji może być kontrowersyjny kontrakt założonej przez milionera popierającego Trumpa spółki Palantir z National Health Service.[118] Umowa opiewała na 23 mln funtów i zezwalała na przetwarzanie wrażliwych danych medycznych pacjentów przez dwa lata. Kontrakt przedstawiono jako reakcję na pandemię, a projekt miał być swego rodzaju „składnicą danych" (*data store*), której zawartość po pandemii miała zostać zniszczona. Zapewniano też, że każde rozszerzenie zostanie poddane publicznemu przetargowi, w ramach którego podatnicy będą mogli przedyskutować sporne kwestie. W rzeczywistości jednak spółka uzyskiwała na podstawie umowy dostęp do najbardziej poufnych informacji zdrowotnych obywateli Wielkiej Brytanii, narażając ich dane na wyciek do służb amerykańskich, z którymi Palantir już wcześniej współpracował (m.in. CIA, Departament Obrony USA i policja Los Angeles).[119]

Europejski Związek na rzecz Danych Przemysłowych, Infrastruktury i Chmury (European Alliance for Industrial Data, Edge and Cloud) podaje, że jednym z celów Unii Europejskiej powinno być powszechniejsze wykorzystanie technologii chmury obliczeniowej, umożliwiającej wdrażanie nowych technologii.[120] Od kilku lat istnieje jednak w tym zakresie wielowymiarowy konflikt interesów, toczący się z jednej strony na poziomie regulacyjnym, a z drugiej – na poziomie kontraktowym, powodując przewagę rynkową gigantów technologicznych nad mniejszymi graczami. Współpraca polegająca na stawianiu jednej strony kontraktu w korzystniejszej pozycji w stosunku do drugiej, a także na wyzyskiwaniu nieświadomej strony trzeciej, powinna być zabroniona nie tylko ze względu na bezpieczeństwo danych osobowych, ale również konieczność budowania zaufania obywateli do organów publicznych, by byli skłonni do dzielenia się danymi na potrzeby rozwoju nowych technologii.

---

[118] M. Williams, *'Spy tech' firm Palantir made £22m profit after NHS data deal*, Open Democracy 2021, https://www.opendemocracy.net/en/dark-money-investigations/spy-tech-firm-palantir-made-22m-profit-after-nhs-data-deal/ (dostęp: 7.03.2022).

[118] M. Fitzgerald, C. Crider, *Controversial tech firm Palantir lands £23m NHS data deal*, Open Democracy 2020, https://www.opendemocracy.net/en/ournhs/controversial-tech-firm-palantir-23m-nhs-data-deal/ (dostęp: 7.03.2022).

[118] European Alliance for Industrial Data, Edge and Cloud, Komisja Europejska, 2022, https://digital-strategy.ec.europa.eu/en/policies/cloud-alliance (dostęp: 7.03.2022).

ASPEKTY EKONOMICZNE

Tworzenie infrastruktury chmurowej dla sektora ochrony zdrowia wiąże się z wyborem między ogólnodostępnymi rozwiązaniami, oferowanymi przez komercyjne podmioty, a wypracowaniem własnych rozwiązań na potrzeby państwa. Stworzenie bezpiecznego, krajowego systemu informatycznego wymaga wysokich początkowych kosztów, ale pozwala na uniknięcie negatywnych skutków uzależnienia się od komercyjnego dostawcy.

Zakup rozwiązań chmurowych u komercyjnego dostawcy, takiego jak Microsoft Azure bądź Amazon EC2, jest tylko pozornie bardziej opłacalny niż inwestowanie w krajową infrastrukturę cyfrową. Próba optymalizacji kosztów przez wybór jednego prywatnego podmiotu działa bowiem na niekorzyść sektora publicznego, ponieważ może prowadzić do uzależnienia systemu zarządzania danymi od usługodawcy. *Vendor lock-in*, czyli sytuacja, w której zmiana usługodawcy jest nieopłacalna, ze względu na wysokie koszty migracji systemów, pojawia się najczęściej w kryzysowym momencie.[121] Usługobiorca bywa zmuszony do ograniczenia możliwości zarządzania danymi w przypadku próby wprowadzenia danych niekompatybilnych z usługami oferowanymi przez dostawcę. Korzystanie z jednego dostawcy chmurowego może okazać się niekorzystne także w przypadku cyberataku, który – skierowany na daną platformę – dotknie całej bazy danych. Ponadto bezpośrednie konflikty z usługodawcą, np. w zakresie przestrzegania zasad kontraktu lub nieprawidłowości w zarządzaniu danymi, mogą doprowadzić do czasowego zawieszenia dostępu do chmury lub do utrudnień w korzystaniu z platformy powodowanych przez usługodawcę.

Jednocześnie korzystanie z publicznej chmury obliczeniowej, udostępnianej przez duże koncerny, może przynosić wiele korzyści. Usługobiorca nie ponosi kosztów stworzenia infrastruktury IT, nie ponosi także odpowiedzialności za zapewnienie dostępności usługi. Instalacja, obsługa i utrzymanie systemów IT są uproszczone, a usługodawca zobowiązany jest do rozwiązywania problemów, które pojawią się podczas korzystania z oferowanych przez niego rozwiązań chmurowych.[122]

Na polskim rynku istnieją jednak modele, których wprowadzenie lub rozwijanie w ramach sektora ochrony zdrowia pozwoliłoby na zarządzanie danymi

---

[121] J. Opara-Martins, R. Sahandi, F. Tian, *Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective*, Journal of Cloud Computing: Advances, Systems and Applications 2016, 5:4

[122] A. Rot, *Wybrane zagadnienia bezpieczeństwa danych i usług w modelu cloud computing* w: *Gospodarka cyfrowa 2016: Zarządzanie, innowacje, społeczeństwo i technologie*, red. A. Gąsiorkiewicz. K. Sitarski, Wydział Zarządzania Politechniki Warszawskiej, https://repo.pw.edu.pl/docstore/download/WUTf04c3fea96374292b58a2ac1ca523620/DEMIST16-Monografia.pdf#page=99.

medycznymi w chmurze, a jednocześnie uniezależniłoby od usług dużych korporacji cyfrowych. Do alternatywnych rozwiązań należy Polska Chmura – inicjatywa dostawców rozwiązań chmurowych zachęcająca firmy oraz administrację publiczną do korzystania z usług polskich dostawców.[123] Firmy tworzące inicjatywę posiadają międzynarodowe certyfikaty jakości usług, ich centra znajdują się w Polsce i gwarantują bezpieczeństwo danych dzięki zgodności z prawem polskim i prawem Unii Europejskiej. Istnieją także projekty publiczne, takie jak System Zapewniania Usług Chmurowych, które mają za zadanie wspierać wymianę informacji o rozwiązaniach chmurowych przez budowanie katalogu ofert.[124] ZUCH przekazuje informacje zarówno o dużych korporacjach, jak i o lokalnych dostawcach. Nie rozwiązuje więc problemu, jakim jest priorytetowa pozycja Big Techów na rynku *cloud computingu*.

Aby jednak tworzyć bezpieczne systemy informatyczne dla sektora publicznego, należy zapewnić pełną transparentność kryteriów wyboru dostawcy i standaryzacji zamówień publicznych.[125] Tak jak organizuje się centralne zakupy leków, by ujednolicić sposób przeprowadzanej terapii w obrębie danej jednostki chorobowej, tak powinno się ujednolicić standardy bezpieczeństwa infrastruktury informatycznej przeznaczonej do gromadzenia danych medycznych pacjentów. W tym momencie nie wiadomo jednak, jakie jest główne kryterium decydujące o tym, który dostawca wygra przetarg. Ze względu na znaczenie bezpieczeństwa danych zamawiający powinien zwrócić szczególną uwagę na to, by dostawca miał swoją główną siedzibę w obszarze EOG, a więc w tych państwach, do których przekazywanie danych zostało uznane za bezpieczne. Dla zapewnienia transparentności na odpowiednim poziomie podmioty świadczące usługi za pośrednictwem infrastruktury informatycznej powinny wyszczególniać, która część danej kwoty faktycznie została przeznaczona na infrastrukturę, a która na wynagrodzenie personelu. Pozwoli to ustalić wpływ finansowania na rozwój infrastruktury i ewentualnie zaplanować inne rozłożenie wydatków.

ASPEKTY POLITYCZNE

Wspieranie rozwiązań wzmacniających suwerenność sektora publicznego w Polsce jest zgodne zarówno z krajowymi planami zarządzania danymi, jak i z wymogami Komisji Europejskiej. Od czasu wyroku TSUE w sprawie Schrems II – określającej czynności, które

[123] Polska chmura, https://polska-chmura.pl/ (dostęp: 23.02.2022).

[124] *Czym jest ZUCH?*, Gov.pl, https://chmura.gov.pl/informacje/czym-jest-zuch (dostęp: 23.02.2022).

[125] Ł. Węgrzyn, *Chmurowy vendor lock-in. Jak go uniknąć?*, „Computerworld" 2020, https://www.computerworld.pl/news/Chmurowy-vendor-lock-in-Jak-go-uniknac,421547.html (dostęp: 7.03.2022),

należy wykonać w przypadku transferu danych do państwa poza Unią Europejską – KE dąży do rozwijania technologii chmurowych na terenie Unii, ujednolicania zasad oferowania usług chmurowych oraz stworzenia jednolitego rynku danych.[126]

Jednym z głównych celów ogłoszonej w 2020 r. „Europejskiej strategii w zakresie danych" opublikowanej przez KE i Parlament Europejski jest stworzenie do roku 2027 sfederowanej infrastruktury chmurowej, opartej na ekosystemach wypracowanych w Europie. Komisja wspiera także inicjatywy, których celem jest zwiększenie transparentności dostawców rozwiązań chmurowych. Opracowany wspólnie ze środowiskiem usługodawców chmur EU Cloud Code of Conduct udziela gwarancji systemom operującym na terenie UE, jeżeli sposób, w jaki zarządzają danymi, jest zgodny z zasadami UE, ułatwiając klientom znalezienie bezpiecznego środowiska cyfrowego.[127]

W ramach planów krajowych długoterminowym celem dla sektora publicznego w Polsce jest tworzenie zdecentralizowanych repozytoriów danych oraz zbudowanie zaufanej publicznej chmury informatycznej do przechowywania danych obywateli polskich (Uchwała nr 196 Rady Ministrów z 28 grudnia 2020).[128] Prace nad krajowym, niezależnym środowiskiem chmurowym są także zgodne ze „Strategią rozwoju ochrony zdrowia na lata 2021–2027".[129] By podnieść jakość opieki zdrowotnej w Polsce, proponuje się wsparcie inicjatyw w zakresie zbierania i analizy danych. Korzystanie z lokalnych usług chmurowych może więc stanowić narzędzie do osiągnięcia tego celu.

Jednocześnie obserwujemy w Polsce rozwój zagranicznych operatorów rozwiązań chmurowych, we współpracy z krajowymi operatorami. Szczególnym przykładem wprowadzania rozwiązań spoza UE na polski rynek jest Chmura Krajowa, spółka założona z inicjatywy PKO Banku Polskiego i PFR. Oferuje usługi chmurowe oraz doradcze w zakresie transformacji cyfrowej. Jej celem jest oferowanie i promowanie rozwiązań chmurowych, których serwery znajdują się na terenie Polski.[130] Zastanawiające więc jest, że spółka ta działa również jako dostawca rozwiązań chmurowych Google Cloud i Microsoft

---

[126] Europejska strategia w zakresie dostępu do danych, Komisja Europejska 2020, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_pl (dostęp: 23.02.2022).

[127] EU Cloud CoC, 2020. EU Data Protection Code of Conduct for Cloud Service Providers, Version 2.11, December 2020.

[128] Uchwała nr 196 Rady Ministrów z 28 grudnia 2020 r. w sprawie ustanowienia „Polityki dla rozwoju sztucznej inteligencji w Polsce od roku 2020", https://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20210000023/O/M20210023.pdf (dostęp: 16.02.2022).

[129] Ministerstwo Zdrowia 2021, Zdrowa przyszłość. Ramy strategiczne rozwoju systemu ochrony zdrowia na lata 2021–2027, z perspektywą do 2030, Załącznik do uchwały nr 196/2021 Rady Ministrów z 27 grudnia 2021 r., https://www.gov.pl/web/zdrowie/zdrowa-przyszlosc-ramy-strategiczne-rozwoju-systemu-ochrony-zdrowia-na-lata-2021-2027-z-perspektywa-do-2030 (dostęp: 16.02.2022),

[130] A. Tarkowski, *Polska Chmura Krajowa – o co chodzi w tym projekcie*, „Polityka" 2018, https://www.polityka.pl/tygodnikpolityka/ludzieisty-le/1770726,1,polska-chmura-krajowa–o-co-chodzi-w-tym-projekcie.read (dostęp: 14.03.2022).

Azure, na mocy zobowiązań zawartych w 2020 r. [131] Partnerstwa te, choć opierają się na lokalnych infrastrukturach zarówno Google'a, jak i Microsoftu, związane są z korporacjami, których główne siedziby znajdują się poza Unią Europejską.

W obliczu regulacji wprowadzanych przez Stany Zjednoczone, takich jak CLOUD Act, możliwe, że usługi oferowane za pośrednictwem Chmury Krajowej nie pozostaną suwerenne. Trzeba jednak zaznaczyć, że pojawienie się w regionie lokalnych oddziałów amerykańskich dostawców jest zjawiskiem pozytywnym, pozwalającym na lepsze monitorowanie systemów zarządzania danymi. Dodatkowo w momencie zawierania umowy przez krajową firmę z usługodawcą przez Chmurę Krajową odpowiedzialność usługodawcy jest ustalana według polskiego prawa co ułatwia prowadzenie dokumentacji oraz dochodzenia w przypadku naruszeń kontraktów. Największym problemem, wynikającym z opierania rozwiązań i dla sektora prywatnego, i dla publicznego na produktach zagranicznych usługodawców, jest jednak ograniczanie innowacyjności krajowych rynków. Zawieranie umów o usługi chmurowe z korporacjami Big Tech prowadzi do monopolizacji rynku rozwiązań zarządzania danymi, utrudniając rozwój krajowych dostawców.

Monopolizację rynku rozwiązań cyfrowych podtrzymują także instytucje publiczne przez podpisywanie zleceń z korporacjami Big Tech. Centrum GovTech, działające przy Kancelarii Prezesa Rady Ministrów, na początku 2021 r. zawarło porozumienie z firmą Microsoft, w ramach którego wspólnie realizowane mają być projekty z wykorzystaniem rozwiązań cyfrowych, w tym AI.[132] Ominięcie etapu zgłoszeń podwykonawców lub organizacji przetargów, choć z perspektywy KPRM korzystne, gdyż minimalizuje koszty transakcyjne i ułatwia zawieranie umów, zawęża pole dialogu między sektorem publicznym a prywatnym. Ponadto obecny stan regulacji zatrudnienia w jednostkach sektora publicznego nie ogranicza powstawania sytuacji „obrotowych drzwi".[133] Owe „obrotowe drzwi" pozwalają na szybkie przejście między administracją publiczną a sektorem prywatnym, ale powodują konflikt interesów oraz wyciek wewnętrznej wiedzy do aktora rynkowego, tak jak miało to miejsce w przypadku dyrektora Departamentu Cyberbezpieczeństwa w KPRM, który po zakończeniu pracy w kancelarii przeszedł do Microsoftu, gdzie obecnie zajmuje się budową infrastruktury chmurowej dla sektora publicznego.

---

[131] K. Mokrzycka, *Megaprojekty chmur obliczeniowych Google i Microsoft w Polsce – wiceprezes PKO BP wyjaśnia, jak będą działać*, 300Gospodarka 2020, https://300gospodarka.pl/wywiady/megaprojekty-chmur-obliczeniowych-google-i-microsoft-w-polsce-wiceprezes-pko-bp-wyjasnia-jak-beda-dzialac (dostęp: 14.03.2022).

[132] A. Klimczuk, *Centrum GovTech i Microsoft łączą siły*, Microsoft 2021, https://news.microsoft.com/pl-pl/2021/01/21/centrum-govtech-i-microsoft-lacza-sily/ (dostęp: 23.02.2022).

[133] Wirsching, E, *The Revolving Door for Political Elites: An Empirical Analysis of the Linkages between Government Officials' Professional Background and Financial Regulation*. OECD Global Anti-Corruption & Integrity Forum: 1–2, 2018..

ASPEKTY TECHNOLOGICZNE

Przed wejściem na polski rynek zdrowotny nowa technologia medyczna musi uzyskać pozytywną ocenę Agencji Oceny Technologii Medycznych i Taryfikacji pod względem przydatności społecznej, ceny oraz wpływu na system ochrony zdrowia.[134] Standaryzacja zgodności technologii z prawem oraz z dobrem społecznym ułatwia funkcjonowanie systemu ochrony zdrowia, ponieważ zmniejsza liczbę decyzji, które podejmować muszą poszczególne jednostki. Pozwala też na spójną wycenę świadczeń (taryfikację świadczeń), umożliwiając prowadzenie wspólnej polityki zakupowej przez podmioty z publicznego sektora zdrowia.

Obecnie jednak opiniowanie wyrobów medycznych ogranicza się do oceny urządzeń wykorzystywanych w praktyce lekarskiej, pomijając kwestię zgodności oprogramowania tych urządzeń z kryteriami wyznaczonymi w „Ocenie technologii medycznych" (*Health Technology Assessment*). Urządzenia, z których korzystają jednostki medyczne, zbierają i zapisują dane o stanie zdrowia pacjentów, lecz sposób, w jaki dane są przechowywane i udostępniane, nie jest poddawany analizie HTA. Prowadzi to do sytuacji, w której każdy administrator danych w jednostce ochrony zdrowia musi indywidualnie podjąć decyzję, czy jego zdaniem skorzystanie z danej technologii jest zgodne z prawem i z interesem społecznym oraz nie narusza prywatności pacjenta. Problem istotny jest także w przypadku zakupu rozwiązań chmurowych dla podmiotów ochrony zdrowia, które również nie podlegają ocenie przydatności.

Cloud computing pozwala na szybką integrację informacji z różnych źródeł, dlatego może sprawdzić się w zarządzaniu danymi medycznymi.[135] Brak standaryzacji tego typu rozwiązań prowadzi jednak do problemów z podejmowaniem decyzji o wyborze dostawcy rozwiązań cyfrowych, ponieważ każda jednostka musi wypracować własne kryteria oceny rozwiązania przez organizowanie przetargów. Usługodawcy zazwyczaj nie są jednak zobowiązani do ukazania sposobu, w jaki działa ich technologia, muszą jedynie wyjaśnić, co oferuje. Rozwiązania chmurowe nie są więc transparentne. Alternatywą umieszczania danych w chmurze jest skorzystanie z lokalnego oprogramowania, dzięki któremu dane przetwarzane są w jednostce je wytwarzającej. *On premise software* wiąże się jednak z wysokimi nakładami na wypracowanie rozwiązania, w tym zakup infrastruktury do przetwarzania danych, potrzebą zapewnienia fizycznej prze-

[134] Agencja Oceny Technologii Medycznych i Taryfikacji, 2022. O nas, AOTMiT, https://www.aotm.gov.pl/o-nas/ (dostęp: 19.03.2022).

[135] A. Fesak, *Benefits and Drawbacks of Cloud-Based versus Traditional ERP Systems. Proceedings of the 2012-13 Course on Advanced Resource Planning*, 2012.

strzeni dla serwerów instytucji i zatrudnienia osób z kompetencjami cyfrowymi oraz problemem ze skalowaniem wprowadzanych rozwiązań.[136] Dzielenie się danymi jest więc utrudnione, dlatego rozwiązanie to nie zaspokaja potrzeby rozwoju ochrony zdrowia w Polsce. Konieczne jest więc zreformowanie rozwiązań chmurowych dla sektora ochrony zdrowia.

By zapewnić swobodny przepływ informacji między zleceniodawcą a zleceniobiorcą o sposobach zarządzania danymi przez *cloud computing*, w zamówieniach publicznych na rozwiązania IT uwzględnić można otwarte procesy zamówień, na licencji typu Open Source Software.[137,138] Open Source to kategoria licencji, na mocy których oprogramowanie udostępniane jest zleceniodawcy razem z kodem źródłowym.[139] Umożliwia więc sprawdzenie przydatności rozwiązania dla usługobiorcy oraz zmniejsza prawdopodobieństwo nadużyć przez firmy pośredniczące w zarządzaniu danymi. Celowe wprowadzanie błędów do kodu jest w tym przypadku niemożliwe do ukrycia, ponieważ dane o rozwiązaniu są jawne i powszechnie dostępne.[140]

Co więcej, przydatność oprogramowania powinna być sprawdzana już podczas oceny technologii medycznej i jej taryfikacji. Wprowadzenie weryfikacji oraz oceny oprogramowania wykorzystywanego w sektorze zdrowia pozwoliłoby zwiększyć transparentność rozwiązań cyfrowych oraz systemów zarządzania danymi. Umożliwiłoby także poprawne wykorzystywanie danych, przy wsparciu suwerenności technologicznej, ponieważ jednostki sektora medycznego miałyby pewność, że proponowane rozwiązania bądź urządzenia zbierające dane uzyskały pozytywną opinię AOTMiT. Ponadto wprowadzenie ocen oprogramowania wpłynęłoby na taryfikację rozwiązań medycznych, gdyż wyceny świadczeń medycznych przeprowadzanych przy użyciu technologii z różnym oprogramowaniem obrazowałyby przydatność danego rozwiązania nie tylko pod względem klinicznym, ale także z perspektywy cyfrowej.

Wytyczne dla oprogramowania zbierającego dane medyczne mogą opierać się na zasadach oceny, podobnych do stosowanych w przypadku aplikacji medycznych, które istnieją już w innych państwach, np. w Australii.[141] W ich skład wchodzą

---

[136] C. Fisher, *Cloud versus On-Premise Computing*, „American Journal of Industrial and Business Management", 2018.

[137] M. Maruta, Z. Okoń, *Open source: trochę dłuższa analiza*, cz. I, „CRN" 2021, https://crn.pl/artykuly/open-source-troche-dluzsza-analiza-cz-i/ (dostęp: 26.02.2022).

[138] B. Jussak, P. Wasilewski, *Open Source w zamówieniach publicznych*, „CRN" 2015, https://crn.pl/artykuly/open-source-w-zamowieniach-publicznych (dostęp: 26.02.2022).

[139] *What is 'open source' software*, Open Source Initiative 2022, https://opensource.org/faq#osd (dostęp: 26.02.2022).

[140] *Open source to tańsza i przyjaźniejsza administracja? W Jaworznie o tym wiedzą*, Interaktywnie.com 2017, https://interaktywnie.com/biznes/newsy/biznes/open-source-to-tansza-i-przyjazniejsza-administracja-w-jaworznie-o-tym-wiedza-255327 (dostęp: 26.02.2022).

[141] V. Vukovic, C. Favaretti, W. Ricciardi, C. de Waure, *Health technology assessment evidence on e-Health / m-Health technologies: evaluating the transparency and thoroughness*, „International Journal of Technology Assessment in Health Care" 2018, doi:10.1017/S0266462317004512.

aspekty techniczne (w tym możliwość skalowania rozwiązań), ekonomiczne, przydatność kliniczna, zgodność z prawem, łatwość w obsłudze i organizacji pracy z danym systemem oraz aspekty etyczne. Do najważniejszych należy prawo do prywatności pacjenta, ale także kwestie udostępniania danych.[142] Zarówno oprogramowania urządzeń, jak i całe rozwiązania chmurowe podlegałyby więc weryfikacji uwzględniającej transparentność zarządzania danymi, przydatność społeczną oraz suwerenność technologiczną jednostek korzystających z danych technologii.

Przegląd międzynarodowych najlepszych praktyk

Problem uzależnienia się od największych dostawców technologicznych jest jednakowo dotkliwy w niemal wszystkich krajach UE. Mimo chęci uniezależnienia się od cyfrowych gigantów, w dalszym ciągu w Europie przeważa strach przed pozostaniem w tyle za Stanami Zjednoczonymi i Chinami w wyścigu innowacji. Dodatkowo niezależności nie sprzyja brak kapitału na przedsięwzięcia związane z podwyższonym ryzykiem, a także brak umiejętności na odpowiednim poziomie.[143] Poszczególne państwa próbują sobie jednak radzić z problemem braku suwerenności cyfrowej na własne sposoby, przede wszystkim przez monitorowanie rynku i reagowanie na nieuczciwe praktyki dostawców, a także kontrolowanie sposobów wykonywania obowiązków ochrony danych osobowych wynikających z regulacji europejskich.

Jednym z kluczowych elementów zmian w zakresie uzyskania suwerenności cyfrowej jest uświadamianie swoim obywatelom zagrożeń związanych z wykorzystywaniem technologii amerykańskich dostawców. Przykładowo, Francuska Krajowa Komisja Informatyki i Wolności (CNIL) wydała zalecenia dla podmiotów, które w związku ze swoją działalnością gromadzą dane dotyczące zdrowia, by wybierały raczej rozwiązania oferowane przez europejskich dostawców chmurowych, a unikały korzystania z narzędzi firm takich jak Google Cloud, Amazon Web Services czy Microsoft Azure.[144] Rekomendacje te są efektem kontrowersji wokół transferu danych osobowych do USA, jakie powstały po wyroku Schrems II, i planowanej uprzednio współpracy z Microsoftem w celu budowy platformy danych zdrowotnych.

---

[142] M. Moshi, R. Tooher, T. Merlin, *Development of a health technology assessment module for evaluating mobile medical applications*, „International Journal of Technology Assessment in Health Care", 36(3) 2020, 252-261. doi: 10.1017/S0266462320000288.

[143] A. Renda, *Europe's Big Tech Contradiction*, Centre for European Policy Studies 2019, https://www.ceps.eu/europes-big-tech-contradiction/ (dostęp: 10.03.2022).

[144] PAP 2020, *Dane medyczne Francuzów nie trafią do USA. Paryż stawia na chmurę w UE*, CyberDefence24, https://cyberdefence24.pl/polityka-i-prawo/dane-medyczne-francuzow-nie-trafia-do-usa-paryz-stawia-na-chmure-w-ue (dostęp: 10.03.2022).

Ciekawym przykładem radzenia sobie z dominacją niektórych podmiotów technologicznych jest też polityka zamówień publicznych na usługi informatyczne przyjęta przez Barcelonę.[145] Miasto postawiło przede wszystkim na inkluzyjność infrastruktury, wybieranie rozwiązań open source, w zarządzaniu projektami, a także zgodne z zasadami etycznymi przetwarzanie danych osobowych. W przeciwieństwie do częstych praktyk innych państw, kryterium ceny nie było tutaj najważniejsze.

Na uwagę zasługują również działania społeczne w zakresie wspierania suwerenności cyfrowej. Poddanie debacie publicznej wspomnianych wcześniej umów między spółką Palantir a NHS prawdopodobnie nie byłoby możliwe bez aktywnego nagłaśniania sprawy przez Open Democracy – niezależną globalną organizację medialną, która nie tylko publikowała artykuły krytycznie nastawione do tego przedsięwzięcia, ale też podjęła odpowiednie środki prawne, by uniemożliwić dalszą współpracę angielskiego płatnika i wspominanej spółki.[146] Głównym celem wejścia na drogę sądową przez Open Democracy było przywrócenie równowagi między rządem a obywatelami Wielkiej Brytanii przez przeprowadzenie konsultacji społecznych przed zawarciem kolejnych umów, takich jak ta z Palantirem. Organizacja walczyła również o to, by dla każdej nowej umowy przeprowadzano szczegółową ocenę wpływu na ochronę danych wyjaśniającą, komu i jakie dane dotyczące zdrowia są udostępniane, a także, jakie poczyniono zabezpieczenia. Chociaż rząd brytyjski przyznał, że oba te kroki są wymagane, pozostaje jeszcze wiele do zrobienia, aby konsultacje były szerokie, dogłębne i reprezentatywne dla wszystkich użytkowników NHS.

W dyskusji na temat przywrócenia równowagi rynkowej nie powinno również zabraknąć głosu przedstawicieli nauki. Projekt „Modern Bigness" powstał na uniwersytecie w Utrechcie i uzyskał wsparcie Europejskiej Rady ds. Badań Naukowych w ramach programu Unii Europejskiej „Horyzont 2020" w zakresie badań naukowych i innowacji. Głównym celem projektu jest badanie, czy europejskie prawo konkurencji może stawić czoła nowoczesnym uwarunkowaniom wynikającym z gospodarki cyfrowej. „Modern Bigness" łączy różne projekty badawcze w ramach zespołu pracowników akademickich, by wspólnie zastanawiać się nad charakterem i granicami europejskiego prawa konkurencji w odniesieniu do rozwoju technologii cyfrowych.[147]

---

[145] N.J. Bąk, et al, op.cit., s. 4.

[146] M. Fitzgerald, C. Crider, *We've won our lawsuit over Matt Hancock's £23m NHS data deal with Palantir*, Open Democracy 2021, https://www.opendemocracy.net/en/ournhs/weve-won-our-lawsuit-over-matt-hancocks-23m-nhs-data-deal-with-palantir/ (dostęp: 14.03.2022).

[147] Modern Bigness, Utrecht University 2022, https://www.uu.nl/en/research/modern-bigness (dostęp: 14.03.2022).

Rekomendacje

Aby odzyskać suwerenność cyfrową w sektorze medycznym, powinno się ujednolicić standardy bezpieczeństwa infrastruktury informatycznej przeznaczonej do gromadzenia danych medycznych pacjentów, wybierając przede wszystkim rozwiązania europejskie.

I. Zasady wykorzystania zasobów danych i wybierania dostawców chmurowych

a. Ramy czasowe: 1–2 lata

Im szybciej przejdzie się do działania i ujednolicania praktyk w zakresie wyboru dostawców, tym lepiej dla całego sektora medycznego. Konieczne jest wydanie dokumentu opisującego dobre praktyki dla podmiotów medycznych przetwarzających dane pacjentów w chmurze. Z uwagi na niewiążący charakter takiego standardu, jego wydanie nie powinno napotkać większych trudności.

Wykonanie zaleceń dotyczących rezygnacji z rozwiązań dużych dostawców, zmiany wykorzystywanego narzędzia, migracji danych i po prostu zbudowanie zaufania placówek medycznych do nowych rozwiązań może potrwać jakiś czas.

b. Konieczność zmian instytucjonalnych

Nieuczciwe praktyki rynkowe, w tym zmowy przetargowe, nadzoruje Urząd Ochrony Konkurencji i Konsumentów. Natomiast Urząd Ochrony Danych Osobowych jest odpowiedzialny za monitorowanie poziomu ochrony danych w Polsce. To zatem te organy powinny wspólnie stworzyć, we współpracy z przedstawicielami sektora medycznego, dostawców europejskich i firm doradczych (prawników, ekonomistów itd.), zbiór wytycznych, jakie musi spełniać dostawca usług chmurowych, jeżeli ma dostarczać chmurę obliczeniową dla danych dotyczących zdrowia.

Bezpieczna infrastruktura informatyczna i rozwój technologii w dziedzinie ochrony zdrowia są równie ważne, jak pozostałe wyposażenie szpitali i innych placówek medycznych. W związku z tym należy przyjąć politykę wspólnych zakupów u dostawców infrastruktury z UE dla placówek medycznych i szpitali oraz kodeks dla dostawców opracowywany w dialogu z Urzędem Ochrony Danych Osobowych. Polityka ta obowiązuje od 2021 r. dla wspólnych postępowań na zakup leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych.

Obecnie dokonywanie wyboru dostawcy chmurowego jest chaotyczne i pozostawia podmiotom medycznym dowolność w tym zakresie, a wydatki na cyfryzację ponoszone są na trzech różnych płaszczyznach: centralnej, regionalnej i lokalnej.[148] Należy więc skoordynować wydatki na ten cel w taki sposób, by ujednolicić praktykę i doprowadzić do całkowitego uniezależnienia się od Big Techów.

c. Konieczność zmian prawnych

Stworzenie takiego standardu mogłoby stać się początkiem wzmożonych prac nad aktem prawnie wiążącym na poziomie krajowym lub (najlepiej) unijnym.

Obecnie istniejąca „Polityka zakupowa państwa" stanowi dokument o charakterze średniookresowej strategii, przygotowywany raz na cztery lata. Mimo zbioru dobrych praktyk, nie jest aktem prawnie wiążącym. Konieczne jest zatem przyjęcie wskazanych rekomendacji w formie regulacji, by zobowiązać poszczególne podmioty do odpowiedniego wdrożenia strategii. W tym celu ważne będzie również wyznaczenie i przeszkolenie pracownika odpowiedzialnego za zorganizowanie przetargu na infrastrukturę informatyczną w placówkach medycznych, uwzględniając w Specyfikacji Warunków Zamówienia nie tylko ogólnie ujmowany wymóg „określenia wymagań dotyczących bezpieczeństwa systemów informatycznych i informacji oraz ochrony prywatności w całym cyklu życia produktu, w tym jurysdykcji",[149] ale też konkretne wskazanie, że powinien to być dostawca mający siedzibę w Europejskim Obszarze Gospodarczym. Z uwagi na wspomniane wcześniej wątpliwości, dotyczące poziomu ochrony danych osobowych w państwach trzecich, przesłanka ta będzie mogła zostać uznana za „merytorycznie uzasadnioną".

II. Wprowadzenie oceny i taryfikacji oprogramowania wykorzystywanego w celach medycznych

a. Ramy czasowe: 1–2 lata

Rozwój technologii medycznych, zbierających i przechowywujących wielkie ilości danych o pacjentach, a także aplikacji medycznych wymaga wprowadzenia mechanizmu opiniującego oprogramowanie wykorzystywane w sektorze ochrony zdrowia, w celu sprawdzania jego zgodności z interesem społecznym i prawem. Działanie to wymaga jednak nowelizacji ustawy o świadczeniach opieki zdrowotnej lub osobnej regulacji, co sprawia, że niemożliwe jest wprowadzenie proponowanego rozwiązania w krótkim czasie.

---

[148] Ministerstwo Zdrowia, 2022, op.cit.

[149] Prezes Urzędu Zamówień Publicznych, *Postępowanie o udzielenie zamówienia publicznego na system informatyczny,* Tom II, 2021, https://www.uzp.gov.pl/__data/assets/pdf_file/0024/53826/II-TOM-REKOMENDACJI-PREZESA-UZP-ZAMoWIENIA-PUBLICZNE-NA-SYSTEMY-INFORMATYCZNE.pdf.

b. Konieczność zmian instytucjonalnych

W zakresie wprowadzenia oceny oraz taryfikacji oprogramowania wykorzystywanego w celach medycznych konieczne jest rozszerzenie zadań i uprawnień Agencji Oceny Technologii Medycznych i Taryfikacji. Organ ten powinien zostać rozszerzony o wydział zajmujący się wyłącznie oceną oprogramowania, w tym rozwiązań chmurowych, z których mogą korzystać podmioty ochrony zdrowia. Konieczne jest zatrudnienie specjalistów z sektora IT, którzy będą współpracowali ze specjalistami medycznymi. W dalszej perspektywie powinno się wprowadzić także jednostkę notyfikowaną, dopuszczającą oprogramowanie do obrotu i używania, na wzór lub w ramach Polskiego Centrum Badań i Certyfikacji.[150]

c. Konieczność zmian prawnych

Do rozszerzenia kompetencji AOTiMT niezbędna jest nowelizacja ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych. Przyjęcie wskazanych rekomendacji w postaci regulacji, umożliwiających opiniowanie rozwiązań cyfrowych z uwzględnieniem m.in. ich transparentności i zgodności prawnej, zapewni jednostkom ochrony zdrowia stosowanie przygotowanych kryteriów do oceny oprogramowania wykorzystywanego do celów medycznych. Stworzenie zaś jednostki weryfikującej nowe oprogramowanie przed jego wejściem na rynek medyczny przyczyni się do podniesienia bezpieczeństwa pacjentów i ich danych.

III. Karencja na zatrudnienie w prywatnych sektorach osób pracujących uprzednio w sektorze publicznym

a. Ramy czasowe: do 1 roku

Z uwagi na popularność tematów cyfrowych w ostatnim czasie i brak zaufania do aktywności firm Big Tech możliwe jest nasilenie się podobnych praktyk w najbliższym czasie. W związku z tym regulacje powinny pojawić się jak najszybciej, by uniknąć negatywnych skutków takiej praktyki.

b. Konieczność zmian instytucjonalnych

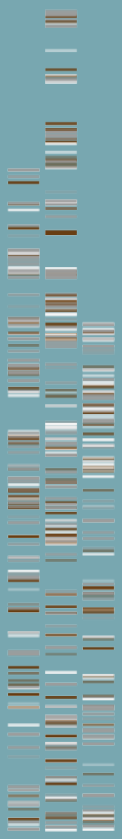
Karencja w zatrudnieniu ma zapobiegać natychmiastowym transferom z sektora publicznego do firm prywatnych. Dotyczyłaby tych obszarów działalności, którymi dana osoba zajmowała się w ramach pracy w instytucji publicznej. Jej okres zależałby natomiast od wcześniej pełnionego publicznego stanowiska.

c. Konieczność zmian prawnych

Należy przyjąć kodeks etyczny dla pracowników sektora publicznego działa-

[150] Polskie Centrum Badań i Certyfikacji, O firmie, 2022, https://www.pcbc.gov.pl/pl/o-firmie (dostęp: 20.03.2022).

jących przy cyfryzacji zdrowia. Kodeks mógłby znaleźć się w zarządzeniu w sprawie ustalenia regulaminu organizacyjnego właściwego w tej sprawie ministerstwa czy Kancelarii Premiera Rady Ministrów. Podobną praktykę przyjął Europejski Bank Centralny: po odejściu z EBC osoby pełniące wysokie funkcje i pracownicy muszą niekiedy odczekać pewien czas przed podjęciem nowej pracy. Koniecznym zabiegiem może być również zobowiązanie funkcjonariuszy do informowania wyznaczonej osoby (np. ministra zdrowia, ministra ds. cyfryzacji itd.) o zamiarze podjęcia zarobkowej działalności zawodowej w okresie dwóch lat od dnia zakończenia pełnienia przez nich funkcji w sektorze publicznym.



MARTA MUSIDŁOWSKA

Analityczka polskich, unijnych i amerykańskich regulacji związanych z nowymi technologiami, przede wszystkim w zakresie ochrony i zarządzania danymi osobowymi. Marcin Król Fellow w Visegrad Insight

JAN ZYGMUNTOWSKI

Współprzewodniczący Polskiej Sieci Ekonomii, dyrektor zarządzający CoopTech Hub, wykładowca Akademii Leona Koźmińskiego

ANNA PADIASEK

Młodsza analityczka programu badawczego gospodarki cyfrowej w Fundacji Instrat, studentka filozofii, politologii i ekonomii na uniwersytecie King's College Lond

05

Zarządzanie danymi dotyczącymi zdrowia

W jaki sposób zbierać, przetwarzać i udostępniać dane dotyczące zdrowia przekazywane podmiotom świadczącym prywatnie/publicznie usługi medyczne, aby zapewnić ich dostępność, interoperacyjność i transparentność oraz aby maksymalizować użyteczność danych w podejmowaniu decyzji? Szukając odpowiedzi na to pytanie, wskazujemy, że mimo licznych postulatów i strategii w tym zakresie, do tej pory w Polsce nie udało się ujednolicić standardów związanych z cyfryzacją ochrony zdrowia. Aby efektywnie zarządzać danymi w sektorze medycznym, konieczne jest zapewnienie współistnienia trzech komponentów: interoperacyjności, dostępności i transparentności. Dla osiągnięcia pełnego wykorzystania zasobów danych i ich wartości konieczne jest wspieranie rozwoju interoperacyjności silnej (zdefiniowanej w Kluczowych pojęciach, s. 4). W tym celu dane dotyczące zdrowia z różnych źródeł (publicznych i prywatnych) powinny być zbierane, analizowane i udostępniane w formatach wyznaczanych regulacyjnie. Aby ulepszyć wspólne użytkowanie danych, należy utworzyć wspólnicę danych zdrowotnych (*health data commons*) umożliwiającą bezpieczne przechowywanie i demokratyczne zarządzanie zebranymi danymi. Wykorzystywanie danych ze wspólnic przez zewnętrzne podmioty byłoby możliwe jedynie na ściśle określonych warunkach: darmowo dla celów naukowych i odpłatnie dla komercyjnych. Prawidłowy rozwój wspólnic i powtórne wykorzystanie danych jest możliwe jedynie przy odpowiedniej kompletności baz danych. Z uwagi na braki kadrowe w sektorze zdrowia należy zwiększyć kadrę pracowników medycznych o asystentów, których zadaniem byłoby dbanie o kompletność, stosowanie właściwych standardów oraz odciążanie z tych zadań kadry medycznej. Fundamentem zmian w zarządzaniu danymi dotyczącymi zdrowia powinno być wzmacnianie zaufania publicznego do zastosowania nowych technologii w ochronie zdrowia. Instytucja asystentów byłaby również pierwszym kontaktem dla pacjentów wątpiących w bezpieczeństwo swych danych i sens dzielenia się nimi dla wsparcia rozwoju technicznego.

Opis zjawiska

Mimo powszechnego poglądu, że korzystanie z Internetu jest i zawsze będzie darmowe, a pozostawiany przez użytkowników w sieci ślad cyfrowy nie ma żadnej wartości, w rzeczywistości stanowi on bezcenną bazę wiedzy, której mądre wykorzystanie może przynieść nieocenione korzyści całemu społeczeństwu.[151] Wskutek globalnej epidemii koronawirusa znacznie wzrosło korzy-

[151] J.J. Zygmuntowski, op.cit.

stanie z technologii medycznych, takich jak elektroniczna dokumentacja medyczna, elektroniczne recepty, a także różnego rodzaju aplikacje i inteligentne urządzenia.[152] Zgodnie z informacjami podanymi przez Centrum e-Zdrowia, w 2019 r. zarejestrowanych było ok. 600 tys. kont pacjenta w systemie e-zdrowie, a zaledwie dwa lata później liczba ta przekroczyła 10 mln.[153] Również w prywatnej ochronie zdrowia, z której decyduje się korzystać już prawie połowa Polaków, podkreślane jest znaczenie inwestowania w bezpieczne środowisko informatyczne i gromadzenia danych pacjentów w sposób uporządkowany, dla dalszego wykorzystania tych zasobów.[154]

Odpowiednio zarządzane i zabezpieczone, masowo udostępniane dane mogłyby przyczynić się do monitorowania jakości leczenia, a także zapobiegania zjawiskom wielolekowości i wielochorobowości, wynikającym m.in. z rozproszenia danych w różnych formatach i w różnych systemach informatycznych. Zablokowany w ten sposób potencjał powoduje, że mimo istnienia zaawansowanych, zautomatyzowanych technologii wspomagających lekarzy na różnych etapach ich pracy, dane dotyczące zdrowia wiszą w próżni informatycznych systemów i nie są właściwie wykorzystywane. Konieczne jest zatem podjęcie działań w celu zarządzania danymi zdrowotnymi w taki sposób, by wspierać rozwój technologii, która będzie wspierała nas.

Maksymalizacja użyteczności danych przekazywanych podmiotom świadczącym prywatne i publiczne usługi medyczne opiera się na trzech filarach, których efektywne współdziałanie stanowi gwarancję dobrego zarządzania posiadanymi zasobami: interoperacyjności, transparentności i dostępności danych dotyczących zdrowia. Definicja interoperacyjności zaproponowana w Krajowych Ramach Interoperacyjności odwołuje się jednak jedynie do zapewnienia interoperacyjności w sektorze publicznym. Ponadto wymóg ujednolicania standardów dotyczy Programu Informatyzacji Ochrony Zdrowia, a więc przedsięwzięć związanych z utworzeniem Elektronicznej Platformy Gromadzenia, Analizowania i Udostępniania Zasobów Cyfrowych o Zdarzeniach Medycznych, czy platformy udostępniania rejestrów medycznych prywatnym placówkom ochrony zdrowia.[155] Żaden z tych projektów nie dotyczy wymiany danych doty-

---

[152] R*aport: Inteligenta automatyzacja 2020*, Deloitte 2020, https://www2.deloitte.com/pl/pl/pages/technology/articles/raport-Inteligentna-Automatyzacja-2020.html.

[153] K. Torchała, *Internetowe konto pacjenta posiada już ponad 10 mln osób*, Bankier.pl, 2021, https://www.bankier.pl/wiadomosc/Internetowe-Konto-Pacjenta-posiada-juz-ponad-10-mln-osob-8150520.html (dostęp: 12.02.2022).

[154] M. Pawlak, J*uż prawie połowa Polaków leczy się prywatnie*, „Rzeczpospolita" 2021, https://pieniadze.rp.pl/ubezpieczenia-zycia/art18940831-juz-prawie-polowa-polakow-leczy-sie-prywatnie (dostęp: 12.02.2022).

[155] Ministerstwo Zdrowia 2018, *Krajowe działania na rzecz e-Zdrowia*, Gov.pl, https://www.gov.pl/web/zdrowie/krajowe-dzialania-na-rzecz-e-zdrowia (dostęp: 12.02.2022).

czących pacjentów między jednostkami sektora publicznego i prywatnego.

Niska interoperacyjność w tym zakresie generuje wysokie koszty transakcyjne w postaci konieczności przenoszenia swojej dokumentacji z jednej do drugiej przychodni i zajmuje dużo więcej czasu niż przekazanie danych za pośrednictwem systemu elektronicznego.

W porównaniu z innymi państwami członkowskimi Unii Europejskiej Polska wypada kiepsko nawet w zakresie słabej interoperacyjności. Zgodnie z badaniem prowadzonym przez Empirica w 2020 r., Polska, *ex aequo* z Rumunią, plasuje się na ostatniej pozycji w Unii Europejskiej pod względem interoperacyjności danych medycznych zawartych w Elektronicznej Dokumentacji Medycznej pacjenta. Ponadto wraz z Bułgarią i Czechami wypadamy najgorzej w zakresie szkoleń pracowników ochrony zdrowia dotyczących cyberbezpieczeństwa.[156] Problemy związane z nieodpowiednim poziomem interoperacyjności w Polsce można określić dwupoziomowo. Z jednej strony, po zgłoszeniu się pacjenta do danej placówki brak danych ukazujących pełną ścieżkę leczenia, od momentu zgłoszenia się do innej placówki z określonym problemem. Nie jest też możliwe dokonanie oceny pacjenta korzystającego równocześnie z publicznych i prywatnych usług. Z drugiej strony natomiast, mimo coraz powszechniejszego stosowania aplikacji zbierających dane dotyczące zdrowia (m.in. monitorujących kondycję, saturację, puls, płodność, dietę, sen itd.), placówki medyczne nie są skłonne do korzystania z danych gromadzonych na urządzeniach. Pozostają więc one niewykorzystanym, choć wartościowym zasobem.

Aby jednak zapewnić interoperacyjność na jak najwyższym poziomie, konieczne jest również poprawienie dostępności danych dotyczących zdrowia. Prawodawstwo w Polsce, inaczej niż w Szwajcarii, Belgii czy Wielkiej Brytanii, które ułatwiają dostęp do danych dotyczących zdrowia, nastawione przede wszystkim na ochronę prywatności i blokuje potencjał drzemiący w zasobach tego rodzaju.

Możliwe jest jednak dokonanie zmian polegających na traktowaniu danych jako wielofunkcyjnego dobra wspólnego, zarządzanego w imieniu właścicieli przez instytucje publiczne.[157] Dostępności danych nie należy jednak mylić z ich całkowitą otwartością – udzielanie dostępu do różnego rodzaju zanonimizowanych danych odbywałoby się za opłatą uiszczaną przez podmioty chcące wykorzystać udostępniane zasoby. Otwarte

[156] MonitorEHR, Empirica 2022, https://empirica.com/project/details/?projectid=291 (dostęp: 13.02.2022).

[157] P. Nemitz, L. Zoboli, J.J. Zygmuntowski, *Embedding European values in data governance: a case for public data commons*, Internet Policy Review 2021, Volume 10, Issue 3, https://policyreview.info/articles/analysis/embedding-european-values-data-governance-case-public-data-commons.

dane natomiast to dane instytucji czy urzędów, z których każdy może korzystać nieodpłatnie.[158]

Brak zrozumienia działania niektórych rozwiązań technicznych oraz lęk pacjentów przed wykorzystaniem ich danych w złej wierze może skutkować niechęcią do dzielenia się swoimi danymi, a w konsekwencji – poprawiania precyzyjności diagnostyki i decyzji wynikających z działania sztucznej inteligencji. Wobec braku chęci udostępniania danych interoperacyjność i dostępność nie mają większego znaczenia. Konieczne jest zatem zapewnienie transparentności zarówno procesów decyzyjnych, jak i sposobów zbierania, zarządzania i przetwarzania danych dotyczących zdrowia. Ma to zapobiegać tzw. efektowi czarnej skrzynki, a więc takiemu działaniu sztucznej inteligencji, które analizuje i kojarzy ze sobą różne dane w celu podjęcia właściwej decyzji w nikomu nieznany sposób. Wynika to ze stosowanych technik uczenia maszynowego, które polegają na tym, że właściwie maszyna wytwarza swój własny program na podstawie przykładowych danych i pożądanego wyjścia.[159] Udzielenie informacji na temat tych procesów zwiększy zaufanie pacjentów do nowych rozwiązań, a w konsekwencji stanie się czynnikiem zachęcającym do podzielenia się swoimi danymi z podmiotami działającymi na rzecz polepszenia informatyzacji sektora medycznego.

Aby efektywnie zarządzać danymi w sektorze zdrowia, trzeba zapewnić współistnienie trzech komponentów: interoperacyjności, dostępności i transparentności. Funkcje te wpływają na siebie, tworząc sieć powiązanych problemów o różnorodnym charakterze. W tym zakresie zostały już podjęte pewne środki zaradcze, polegające m.in. na wprowadzeniu na poziomie unijnym międzynarodowego dostępu do recept i danych pacjentów. Obecnie z tych udogodnień można jednak korzystać jedynie w: Czechach, Chorwacji, Francji, Luksemburgu, Portugalii i na Malcie. Polska ma dołączyć do inicjatywy w 2025 r.[160]

Zaistnienie interoperacyjności silnej wymaga zbierania danych pacjentów, analizowania i udostępniania w ujednoliconych za pomocą odgórnej regulacji formatach. Obowiązywałyby one zarówno dla placówek publicznych, jak i prywatnych, by przenoszenie danych z jednego miejsca do drugiego odbywało się bezproblemowo. Istnieje bowiem ekosystem firm i instytucji gotowych zmodernizować ochronę zdrowia w Polsce, jednak potrzebne im są dane do wykorzystania w diagnostyce i rozwoju

[158] Otwarte dane publiczne, Cyfryzacja KPRM 2019, gov.pl, https://www.gov.pl/web/cyfryzacja/otwarte-dane-publiczne (dostęp: 13.02.2022).

[159] *Powiedz kotku, jak myślisz w środku – efekt czarnej skrzynki*, „Młody Technik" 2022; mlodytechnik.pl, https://mlodytechnik.pl/technika/30208-powiedz-kotku-jak-myslisz-w-srodku (dostęp: 13.02.2022).

[160] Electronic cross-border health services, Komisja Europejska 2021, https://ec.europa.eu/health/ehealth-digital-health-and-care/electronic-cross-border-health-services_en (dostęp: 13.02.2022).

systemów opartych na sztucznej inteligencji. W tym celu proponuje się utworzenie wspólnicy danych zdrowotnych (*health data commons*) jako instytucji powołanej do zarządzania dostępem.[161] Przechowywane w ten sposób dane byłyby odpowiednio zabezpieczone i zanonimizowane, a ich wykorzystanie byłoby możliwe jedynie dla określonych podmiotów i za opłatą, a także w celu demokratyzacji wiedzy, wykorzystania potencjału badaczy i analityków zewnętrznych dla instytucji publicznych do prowadzenia badań naukowych, epidemiologicznych, społecznych. Jednak konieczna jest poprawa przejrzystości całego procesu zarządzania danymi, począwszy od poinformowania pacjenta o tym, co z jego danymi będzie się działo.

Żadna z tych zmian nie będzie jednak możliwa bez zwiększenia liczebności kadry sektora medycznego odpowiedzialnego za właściwe wprowadzanie danych i dbanie o ich kompletność oraz kompatybilność. Obecnie w Polsce na pacjenta przypada najmniejsza liczba lekarzy w Europie,[162] wobec czego większa ilość danych w systemie ochrony zdrowia będzie wymagała odciążenia lekarzy przez asystentów, którzy pomogą w realizacji zadań wynikających z poprawy interoperacyjności prywatnych i publicznych przychodni.

Analiza SLEPT

ASPEKTY SPOŁECZNE

Badania przeprowadzane przez Polski Instytut Ekonomiczny w celu sprawdzenia skłonności Polaków do dzielenia się swoimi danymi z sektorem publicznym pokazały, że zaledwie mniej niż połowa respondentów byłaby gotowa to zrobić, a około 30 proc. ankietowanych zajęło negatywne stanowisko wobec przekazania danych do takich obszarów jak transport, zużycie energii elektrycznej czy ochrona zdrowia.[163] Taki stan rzeczy może wynikać przede wszystkim z braku wiedzy o wartości danych, zwłaszcza dotyczących zdrowia, i jest utrwalany przez postrzeganie ich jedynie przez pryzmat RODO, jako sloganu reprezentującego ochronę prywatności w sieci, z pominięciem innych, istotnych kwestii. Z powodu małej znajomości praw cyfrowych i polegania jedynie na populistycznym przekazie co do ich zakresu większość Polaków boi się udostępniać swoje dane dotyczące zdrowia albo w ogóle się nad tym nie zastanawia. Wiele osób nie widzi też korzyści wynikających z digitalizacji takich danych: 46 proc. ankietowanych w Polsce uważa za istotne, by korzyści z digitalizacji danych medycznych

[161] J.J. Zygmuntowski, *Wspólnice danych: Alternatywny model zarządzania danymi*, Raport projektu: SpołTech, Centrum Cyfrowe 2020.

[162] Health at a Glance 2021: OECD Indicators, OECD Publishing, Paris, https://doi.org/10.1787/ae3016b9-en.

[163] J. Grzeszak, P. Śliwowski, I. Święcicki, A. Wincewicz-Price, *Czy chcemy dzielić się prywatnymi danymi?*, współpr. A. Tarkowski, M. Trojanowska, J.J. Zygmuntowski, Polski Instytut Ekonomiczny, Warszawa 2020.

były ogólnodostępne.[164] Średnia w Europie wynosi 48 proc., natomiast najwyższy wynik (76 proc.) można było odnotować na Malcie. Według innego raportu co trzecia Polka odczuwa negatywne emocje w związku z cyfryzacją sektora medycznego: niechęć, rozczarowanie, frustrację, a nawet złość. Taki stan rzeczy wynikać może ze strachu przed błędną diagnozą, co z kolei bierze się z niezrozumienia sposobów działania niektórych rozwiązań technologicznych.[165]

Jak zostało wyjaśnione wcześniej, chęć dzielenia się swoimi danymi jest kluczowa dla możliwości zaistnienia jakichkolwiek innych funkcji związanych z zarządzaniem zasobami danych. Społeczeństwo nie jest jednorodne w tym zakresie, wiele zależy bowiem od wieku, wykształcenia czy stopnia urbanizacji badanych.[166] Niechęć do dzielenia się swoimi danymi może wynikać również z braku zaufania do instytucji publicznych i obaw związanych z nadużyciami ze strony władz w zakresie wykorzystywania danych dotyczących zdrowia obywateli. Z badań wynika, że jedynie 18 proc. ankietowanych ufa polskiej ochronie zdrowia.[167]

Brak zaufania nie dotyczy jedynie sektora medycznego. Wiele osób obawia się trafienia ich danych w niepowołane ręce, przede wszystkim do organów władzy publicznej.[168] Szczególnie widoczne było to w kontekście objęcia ciąż nadzorem w postaci prowadzenia specjalnego rejestru. Zgodnie z projektem nowelizacji rozporządzenia ministra zdrowia z 26 czerwca 2020 r. w sprawie szczegółowego zakresu danych zdarzenia medycznego przetwarzanego w systemie informacji oraz sposobu i terminów przekazywania tych danych do Systemu Informacji Medycznej, wszystkie podmioty świadczące usługi medyczne będą musiały przekazywać do owego systemu dane o pacjentkach będących w ciąży. Niektóre powody wprowadzenia zmian były uzasadnione – skorzystanie z zapisów poza kolejnością przez takie kobiety, ratowanie życia kobiety w ciąży czy przepisywanie jej leków itd.[169] Ze względu jednak na ogólną sytuację kobiet w Polsce i szczególne zainteresowanie władz kwestiami związanymi z rozrodem reakcja na projekt nowelizacji była bardzo nieprzychylna. Domniemywano, że tak naprawdę chodzi o „przymus i kontrolę"

---

[164] Digital Rights and Principles, Special Eurobarometer 518, Komisja Europejska 2021, doi: 10.2759/30275.

[165] *Cyfrowe Zdrowie Polek. Co digitalizacja usług medycznych zmieni w profilaktyce zdrowia Polek?*, Infuture.Institute, Gdańsk 2021.

[166] *Wykorzystanie technologii informacyjno-komunikacyjnych w jednostkach administracji publicznej, przedsiębiorstwach i gospodarstwach domowych w 2021 r.*, GUS 2021, https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/wykorzystanie-technologii-informacyjno-komunikacyjnych-w-jednostkach-administracji-publicznej-przedsiebiorstwach-i-gospodarstwach-domowych-w-2021-roku,3,20.html (dostęp: 14.02.2022).

[167] Ipsos, 2020. Ipsos Global Health Service Monitor 2020, Ipsos Game Changers, https://www.ipsos.com/sites/default/files/ct/news/documents/2020-11/ipsos-global-health-service-monitor-2020.pd (dostęp: 14.02.2022).

[168] M. Fraser, S. Marska-Maj: *Dostęp do danych medycznych powinien być zawężony – wywiad,* CyberDefence24 2021, https://cyberdefence24.pl/polityka-i-prawo/marska-maj-dostep-do-danych-medycznych-powinien-byc-zawezony-wywiad (dostęp: 15.02.2022).

[169] *Ciąże pod specjalnym nadzorem? Zabieramy głos w konsultacjach*, Fundacja Panoptykon 2021, https://panoptykon.org/rejestr-ciaz (dostęp: 15.02.2022).

nad obywatelkami, a nie o zapewnienie im odpowiedniej opieki lekarskiej.[170]

Wobec tak ukształtowanych nastrojów społecznych konieczne jest przede wszystkim zbudowanie odpowiednio wysokiej kultury zaufania. Jej wzmocnienie może przynieść pozytywne rezultaty w zakresie dzielenia się danymi, a w związku z tym wspierania projektów dotyczących interoperacyjności, dostępności. Raport Cooptech Hub wskazuje, że kulturę zaufania można budować przez zapobieganie odgradzaniu się murem od szeroko rozumianej przestrzeni publicznej. Niezagospodarowany potencjał współpracy międzysektorowej może zostać uwolniony dzięki pracy edukacyjnej, przez oddziaływanie na świadomość oraz za pomocą narzędzi technicznych ułatwiających komunikację, organizację i realizację celu.[171] Przykładem wysokiego poziomu zaufania i współpracy różnych organizacji jest przepisywanie aplikacji na receptę w Niemczech. Aplikacje te mają pomagać w rozpoznawaniu, monitorowaniu, leczeniu i zmniejszaniu skutków choroby. Wśród chorób, w leczeniu których stosowane mogą być aplikacje, wyróżnia się choroby psychiczne, cukrzycę, bóle migrenowe, bezsenność i otyłość. Aby jednak aplikacje były skuteczne, pacjenci muszą mieć dostęp do technologii i wiedzę na temat korzystania z niej, muszą także stosować się regularnie do zaleceń lekarza i mieć zaufanie do przepisanego „leku".[172]

ASPEKTY PRAWNE

Z uwagi na bezpośrednie stosowanie RODO we wszystkich państwach członkowskich Unii Europejskiej stanowi ono kompleksową regulację zagadnień związanych z danymi osobowymi o różnym charakterze. W niektórych sferach rozporządzenie pozostawia przestrzeń państwom członkowskim do uregulowania poszczególnych kwestii, co powoduje, że ochrona danych osobowych może się nieco różnić, w zależności od przepisów krajowych.

W obliczu istnienia rozmaitych aplikacji i urządzeń zbierających dane związane z aktywnością ich użytkowników często pojawia się pytanie, czy należy traktować tego rodzaju dane w taki sam sposób, jak dane zbierane przez placówki medyczne w związku z przeprowadzanymi badaniami. Z uwagi na brak jednolitej definicji „danych dotyczących zdrowia" w prawie polskim i dokładnego określenia przykładów takich danych przez RODO warto zwrócić uwagę na propozycję zawartą w wytycznych Euro-

[170] DGP, 2021. *Rejestr ciąż. Ministerstwo Zdrowia: „Chodzi o względy medyczne"*, „Dziennik Gazeta Prawna", https://serwisy.gazetaprawna.pl/zdrowie/artykuly/8299619,rejestr-ciaz-ministerstwo-zdrowia-chodzi-o-wzgledy-medyczne.html (dostęp: 20.02.2022).

[171] N.J. Bąk, et al, op.cit.

[172] A. Olesch, *A Year with Apps on Prescription in Germany*, Sidekick Health 2021, https://sidekickhealth.com/news/a-year-with-apps-on-prescription-in-germany/?utm_source=Artur&utm_medium=aboutDigitalHealth&utm_campaign=DiGA_10_2021 (dostęp: 15.02.2022).

pejskiej Rady Ochrony Danych. W ślad za orzecznictwem TSUE w tym zakresie Rada uznała, że dane dotyczące zdrowia należy rozumieć „dostatecznie szeroko". Zasługują na większą ochronę, ponieważ „wykorzystanie takich danych wrażliwych może mieć istotne negatywne skutki dla osób, których te dane dotyczą" („Wytyczne w sprawie przetwarzania danych dotyczących zdrowia do celów badań naukowych"). W związku z tym EROD proponuje, by za dane dotyczące zdrowia uznawać następujące kategorie danych:

- informacje zebrane przez świadczeniodawcę opieki zdrowotnej w dokumentacji medycznej pacjenta (w postaci wywiadu chorobowego lub wyników badań bądź terapii),
- informacje, które stały się danymi dotyczącymi zdrowia w wyniku odniesienia do innych danych, co ujawniło stan zdrowia lub zagrożenia dla zdrowia (takie jak założenie, że u danej osoby występuje większe ryzyko zawału serca ze względu na wysokie ciśnienie krwi, jakie odnotowano podczas pomiarów prowadzonych przez określony czas),
- informacje przekazane w ankietach „samokontroli" przez osoby, których dane dotyczą, w ramach odpowiedzi na pytania dotyczące ich stanu zdrowia (np. opisy objawów),
- informacje, które stały się danymi dotyczącymi zdrowia ze względu na sposób ich wykorzystania w określonym kontekście (np. informacje dotyczące niedawnej podróży lub obecności w regionie dotkniętym COVID-19, przetwarzane przez pracownika służby zdrowia w celu postawienia diagnozy).[173]

Uznanie określonych danych za dotyczące zdrowia ma znamienne skutki, jeśli chodzi o sposób postępowania z nimi. Ograniczenia związane z dostępem do takich danych i ich przetwarzaniem mają niwelować ryzyko naruszenia podstawowych praw i wolności, z którym trzeba byłoby się zmierzyć w przypadku traktowania ich w taki sam sposób jak zwykłe dane (RODO). Wskazówkę dotyczącą odpowiednich zabezpieczeń danych wrażliwych pozostawia art. 32 RODO. Wskazuje, że powinno się je zabezpieczać co najmniej przez pseudonimizację, czyli takie przetwarzenie, by przypisanie ich do konkretnej osoby było niemożliwe bez użycia dodatkowych informacji, a także ich oddzielne przechowywanie i takie zabezpieczenie, by ewentualne ich użycie w celu zidentyfikowania danej osoby również nie było możliwe. Inne, komplementarne sposoby to m.in. szyfrowanie, zawieranie umowy o nieujawnianiu informacji, a także ścisły podział ról, ograniczenia praw dostępu i rejestry dostępu.

---

[173] *Wytyczne w sprawie przetwarzania danych dotyczących zdrowia do celów badań naukowych w kontekście pandemii COVID-19*, European Data Protection Board 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_pl.pdf (dostęp: 18.02.2022).

W prawie polskim regulacje dotyczące udzielania dostępu do danych medycznych zapisywanych cyfrowo ustanawiane były niezależnie od ogólnych zasad dostępu do dokumentacji medycznej. W konsekwencji doszło do powstania „skomplikowanej, rozproszonej i niespójnej terminologicznie regulacji zasad dostępu do danych zawartych w dokumentacji medycznej".[174] Zgodnie z art. 26 ust. 1 ustawy o prawach pacjenta, podmiot udzielający świadczeń zdrowotnych udostępnia dokumentację medyczną pacjentowi lub jego przedstawicielowi ustawowemu bądź osobie upoważnionej przez pacjenta.[175] Art. 26 ust. 3 ustawy wskazuje natomiast katalog osób uprawnionych do ubiegania się o dostęp do dokumentacji medycznej na podstawie odrębnych aktów prawnych. Są to m.in. podmioty udzielające świadczeń zdrowotnych, organy władzy publicznej, podmioty kontrolujące, ale też np. Agencja Badań Medycznych, której celem jest wspieranie działalności innowacyjnej w ochronie zdrowia, ze szczególnym uwzględnieniem rozwoju niekomercyjnych badań klinicznych.[176]

RODO traktuje dane dotyczące zdrowia w sposób szczególny, w związku z czym ich przetwarzanie odbywa się na innej podstawie niż przetwarzanie zwykłych danych. Art. 9 wymienia kilka możliwych podstaw przetwarzania danych wrażliwych, wśród których na największą uwagę zasługuje udzielenie wyraźnej zgody przez pacjenta, a także kilka innych wariantów, gdy przetwarzanie danych jest niezbędne, np. do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej albo zabezpieczenia społecznego, będących najczęstszą podstawą przetwarzania danych pacjenta.[177]

Regulacje te wynikają z podejścia do danych z perspektywy ochrony prywatności osób, których dane dotyczą. W imię interesu publicznego możliwe jest jednak takie uregulowanie zasad, by umożliwić korzystanie również z prywatnej własności.[178] Zgodnie z art. 26 ust. 4 ustawy o prawach pacjenta, dane zdrowotne pacjentów w celu ich agregacji w ramach wspólnic mogłyby zostać udostępnione m.in. szkole wyższej lub instytutowi badawczemu, a ściślej jednostkom wymienionym w art.

---

[174] P. Najbuk, J. Pachocki, A. Kruczyk-Gonciarz, P. Kaźmierczyk, R. Lorent, *Wykorzystanie danych medycznych w celu rozwoju AI w Polsce i w celu prowadzenia badań naukowych, Raport Regulacyjny*, DZP, Warszawa 2020.

[175] Ustawa z 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, DzU 2009 nr 52, poz. 417.

[176] E. Bielak-Jomaa, M. Ćwikiel, Art. 26, w: *Prawa pacjenta i Rzecznik Praw Pacjenta. Komentarz*, red. D. Karkowska, Warszawa 2021.

[177] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), OJ L 119, 4.5.2016, p. 1–88, art. 9.

[178] J.J. Zygmuntowski, op.cit.

7 ust. 1 i 4–7 ustawy – Prawo o szkolnictwie wyższym i nauce.[179] Dane te miałyby służyć do wykorzystania w celach naukowych, bez ujawniania nazwiska i innych danych umożliwiających identyfikację osoby, której dokumentacja dotyczy (ustawa o prawach pacjenta). Krąg tych podmiotów jest znacznie węższy niż ten, który wynika z RODO – rozporządzenie nie ogranicza podmiotowo możliwości prowadzenia badań naukowych i powoływania się na art. 9 ust. 2 lit. j).

Tak ukształtowana sytuacja podmiotów chcących przetwarzać dane dotyczące zdrowia w Polsce nie oznacza jednak, że jedynie podmioty wymienione we wspomnianych przepisach mogą to zrobić. Firmy prowadzące określone badania mają prawo przetwarzać dane na podstawie art. 9 ust. 2 lit. j) RODO, ale nie mogą „pominąć" np. wymagań określonych w art. 15 RODO (prawo dostępu do danych). Jak piszą autorzy raportu DZP, w przypadku prawa polskiego należy wskazać, że możliwość prowadzenia działalności gospodarczej w zakresie badań naukowych i prac rozwojowych przewiduje wprost Polska Klasyfikacja Działalności, która wyróżnia dział 72 – Badania naukowe i prace rozwojowe.[180]

ASPEKTY EKONOMICZNE

Wprowadzenie wspólnicy danych dla systemu ochrony zdrowia w Polsce musi zostać poprzedzone analizą ekonomiczną, wykazującą opłacalność tego rozwiązania. Choć projekt początkowo może generować wysokie koszty, z czasem popularyzacja informatyzacji sektora medycznego przyczyni się do zmniejszenia niepotrzebnych wydatków związanych ze zdrowiem o ok. 0,36 proc. PKB.[181] Zaoszczędzone środki mogłyby zostać wykorzystane do usprawnienia innych obszarów ochrony zdrowia. Zwiększenie interoperacyjności danych medycznych pozwoli na wypracowywanie nowych cyfrowych rozwiązań dla ochrony zdrowia, ułatwi wymianę informacji między różnymi podmiotami oraz ulepszy możliwości diagnozowania i zapobiegania chorobom. Koszty operacyjne wspólnicy będą zaś automatycznie pokrywane przez przychody z udostępniania danych i innej jej działalności.

Integracja pozornie bezwartościowych informacji z sektora medycznego w jednym punkcie dostępu do danych będzie, w perspektywie długoterminowej, korzystna. Zebranie danych powiązanych ze sobą

[179] Ustawa z 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce, DzU 2018, poz. 1668.

[180] P. Najbuk, et al., op.cit.

[181] P. Arak, J. Wójcik, *Transforming eHealth into a political and economic advantage*, Polityka Insight 2017.

tematycznie ułatwi pracę nad cyfrowymi rozwiązaniami dla ochrony zdrowia przez zmniejszenie kosztów transakcyjnych pozyskiwania informacji z różnych źródeł.[182] Łączenie danych w większe zbiory przynosi bowiem pozytywne efekty zewnętrzne. Interoperacyjność wspólnicy pozwala na wyciąganie wniosków z danych gromadzonych przez różne, często niepowiązane ze sobą instytucje, umożliwiając np. tworzenie i testowanie modeli predykcyjnych i rozwiązań AI dla ochrony zdrowia. Lepsza wymiana informacji między różnymi podmiotami, w tym naukowcami, oraz ułatwiony rozwój technologii medycznych może więc spowodować skok w jakości usług sektora medycznego.

Najbardziej kosztownym elementem wprowadzania i zarządzania wspólnicą będzie stworzenie bezpiecznej architektury informatycznej do zarządzania danymi. Wypracowane rozwiązanie może być jednak w dalszej perspektywie wykorzystywane na różnych poziomach sektora publicznego oraz w różnych obszarach usług publicznych. Stworzony system powinien, w miarę możliwości, opierać się na rozwiązaniach pochodzących z sektora publicznego oraz kręgów akademickich. Pozwoli to na wypracowanie rozwiązań niezależnych od komercyjnych firm technologicznych, zmniejszając koszty prawne i transakcyjne outsourcingu.

Proponowana inwestycja będzie także generować koszty operacyjne. Konieczne będzie zatrudnienie asystentów do obsługi wspólnicy, pośredniczących między lekarzami i innymi pracownikami ochrony zdrowia a wspólnicą. Równocześnie z wprowadzaniem nowych rozwiązań cyfrowych należy także przeznaczyć środki na podnoszenie kompetencji cyfrowych osób, które będą na co dzień korzystać ze wspólnicy danych, w szczególności personelu medycznego i okołomedycznego.[183] Jest to jednakże koszt niezależny od typu wprowadzanych innowacji w sektorze medycznym.

Wspólnica danych może być nie tylko wypłacalna, ale również generować przychody. Dane medyczne mogą być odpłatnie udostępniane firmom lub osobom prywatnym, przyczyniając się do wzrostu innowacyjności prywatnej ochrony zdrowia.[184] Ponadto dzięki udostępnianiu danych wspólnica może uzyskać przychód z kontroli i zysków z wytworzonych praw własności intelektualnej, określony jako np. procent wartości w spółce celowej, komercjalizującej produkt w oparciu o informacje z sektora publicznego. Opłaty za udzielanie dostępu do danych

[182] J.J. Zygmuntowski, op.cit.

[183] J. Hardinges, P. Wells, A. Blandford, J. Tennison, A. Scott, *Data trusts: lessons from three pilots*, Open Data Institute 2019, https://docs.google.com/document/d/118RqyUAWP3WIyyCO4iLUT3oOobnYJGibEhspr2v87jg/edit (dostęp: 16.02.2022).

[184] J.J. Zygmuntowski, op.cit.

powinny być różnicowane, zależnie od ilości lub charakteru pobieranych danych. Ceny jednorazowego wglądu do wspólnicy i dostępu abonamentowego powinny także się różnić, zależnie od tego, czy klientem jest podmiot niekomercyjny, taki jak inicjatywa naukowa, czy nastawiony na zysk z wypracowanego rozwiązania. Wspólnica dofinansowywana może być także ze środków publicznych przez pozyskiwanie grantów na swoją działalność.

Jest szansa poprawy jakości ochrony zdrowia w Polsce przez wspólnicę danych medycznych w wyniku zwiększania efektywności korzystania z tych danych w procesach profilaktyki, diagnozowania i leczenia. Oparcie modelu biznesowego wspólnicy na współpracy z sektorem prywatnym pozwoli pokryć w całości koszty operacyjne rozwiązania, a tym samym generować więcej korzyści niż strat z wprowadzenia przedstawionego modelu. Udostępnianie danych podmiotom komercyjnym i niekomercyjnym będzie zaś miało pozytywny wpływ na całą gospodarkę, umożliwiając zwiększenie innowacyjności w sektorze medycznym.

ASPEKTY POLITYCZNE

Zmiany w zakresie poprawy cyfryzacji sektora medycznego były planowane w Polsce jeszcze przed wybuchem pandemii, a więc w grudniu 2017 r. Ministerstwo Zdrowia oraz Ministerstwo Cyfryzacji przyjęły wówczas „Strategię rozwoju e-zdrowia w Polsce na lata 2018–2022", która miała poprawić interoperacyjność systemów informatycznych w ochronie zdrowia, ich kompatybilność i kompletność. W 2018 r. Centrum Systemów Informacyjnych Ochrony Zdrowia przystąpiło do międzynarodowej organizacji IHE International (Integrating the Healthcare Enterprise).[185] Mimo braku publikacji pełnej wersji raportu i sprawozdania z jego wykonania, zgodnie z postulatami zaprezentowanymi przez przedstawicieli obu resortów podczas konferencji prasowej i obecnie realizowanymi projektami z zakresu informatyzacji sektora medycznego, można uznać, że cele postawione przez organy władzy publicznej zostały w pewnym stopniu osiągnięte. Konieczność dalszej poprawy stopnia cyfryzacji ochrony zdrowia w Polsce wyraża przyjęcie kolejnych ram strategicznych na lata 2021–2027.[186] Autorzy wskazują, że głównym wyzwaniem pozostaje obecnie zróżnicowany i co do zasady niewystarczający poziom informatyzacji ochrony zdrowia, a także interoperacyjności poszczególnych systemów i rozwiązań informatycznych. W związku z tym należy dążyć do stworzenia systemu, który zapewni szybki dostęp

[185] B. Mejssner, *Cyfrowa opieka zdrowotna oczami polskich i amerykańskich pacjentów*, „Rzeczpospolita" 2018, https://cyfrowa.rp.pl/it/art-16907961-cyfrowa-opieka-zdrowotna-oczami-polskich-i-amerykanskich-pacjentow (dostęp: 16.02.2022).

[186] *Zdrowa przyszłość. Ramy strategiczne rozwoju systemu ochrony zdrowia na lata 2021–2027, z perspektywą do 2030*. Załącznik do uchwały nr 196/2021 Rady Ministrów z 27 grudnia 2021 r., Ministerstwo Zdrowia 2021, https://www.gov.pl/web/zdrowie/zdrowa-przyszlosc-ramy-strategiczne-rozwoju-systemu-ochrony-zdrowia-na-lata-2021-2027-z-perspektywa-do-2030 (dostęp: 16.02.2022).

do informacji medycznej w różnych placówkach, do których uda się pacjent.

Strategia ta jest również kompatybilna z innymi projektami pilotażowymi zorientowanymi na rozwój AI w medycynie, m.in. „Polityką dla rozwoju sztucznej inteligencji w Polsce od roku 2020", przyjętą uchwałą nr 196 Rady Ministrów z 28 grudnia 2020 r.[187] W rozdziale szóstym, przedstawiającym cele krótkoterminowe, na szczególną uwagę zasługuje cel siódmy, który dotyczy wprost „wykorzystania potencjału badawczego danych medycznych w celu poprawy zdrowia obywateli (…) przez pilotażowe programy składowania zanonimizowanych danych medycznych", jak również wskazanie, że istotnym dalszym działaniem w kontekście rozwoju sztucznej inteligencji w Polsce będzie „wspieranie projektów w dziedzinie e-zdrowia, w tym mających na celu interoperacyjność istniejących systemów. W uchwale nie wskazano, czy będzie to dotyczyło i sektora publicznego, i prywatnego. Można natomiast przypuszczać, że deklaracja stworzenia kultury współpracy między oboma sektorami otwiera drogę do stworzenia regulacji w zakresie interoperacyjności silnej. Chociaż postulaty przedstawione w niniejszej publikacji są jak najbardziej spójne z planowaną polityką rządu, pozostaje pytanie o sposób ich realizacji. Wiele bowiem zależy od tego, czy plany dotyczące interoperacyjności i dostępności obejmą również sektor prywatny, oraz czy tworzenie wspomnianych „pilotażowych programów składowania zanonimizowanych danych medycznych" będzie odbywało się w inkluzyjny sposób, z włączeniem różnych organizacji do wspólnego podejmowania decyzji w tym zakresie.

Wiele o współużytkowaniu danych zdrowotnych mówi się również w regulacjach i strategiach unijnych. W lipcu 2021 r. powstał projekt Komisji Europejskiej dotyczący stworzenia europejskiej przestrzeni danych dotyczących zdrowia.[188] Ma on m.in. zachęcać do korzystania z tych danych do celów badawczych, kształtowania polityki i stanowienia prawa, określić kwestie bezpieczeństwa i odpowiedzialności w kontekście korzystania z AI w dziedzinie zdrowia, a także promować bezpieczną wymianę danych pacjentów oraz kontrolę obywateli nad ich własnymi danymi dotyczącymi zdrowia.

Na początku marca 2022 r. wypłynął natomiast projekt Komisji Europejskiej dotyczący nowych ram zarządzania danymi dotyczącymi zdrowia, które mają obejmować wymogi interoperacyjności transgranicznej oraz wprowadze-

[187] Uchwała nr 196 Rady Ministrów 2020, op.cit.

[188] *Cyfrowe dane i usługi dotyczące zdrowia – europejska przestrzeń danych dotyczących zdrowia*, Komisja Europejska 2022, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12663-Cyfrowe-dane-i-us%C5%82ugi-dotyczace-zdrowia-europejska-przestrzen-danych-dotyczacych-zdrowia_pl (dostęp: 17.02.2022).

nie paneuropejskiej infrastruktury.[189] To pierwszy akt prawny, który będzie opierać się na „Rozporządzeniu ws. zarządzania danymi" (Data Governance Act) i „Akcie ws. Danych" (Data Act). Jednym z głównych założeń projektu jest zapewnienie osobom fizycznym dostępu do zestawu „podstawowych" danych dotyczących zdrowia: szczepień, elektronicznych recept, zdjęć, wyników badań laboratoryjnych, raportów z wypisów i innych, w ramach bezpłatnej usługi dostępu. Co ważne dla interoperacyjności silnej, nowe regulacje będą miały wpływ na rynek istniejących produktów oraz zasady prowadzenia projektów publicznych, takich jak elektroniczne karty zdrowia czy oprogramowanie medyczne, ale też aplikacje wellness różnego rodzaju. Pacjenci będą mogli sami ograniczyć dostęp do swoich danych lub je bezpłatnie udostępnić. Projekt zakłada również możliwość wtórnego wykorzystania danych, do których należą dane z dokumentacji zdrowotnej, dane społeczne, administracyjne, genetyczne i genomiczne, rejestry publiczne, badania kliniczne, kwestionariusze badawcze oraz dane biomedyczne, np. z biobanków. Wśród dozwolonych zastosowań znalazły się m.in.: wspieranie organów publicznych w wykonywaniu zadań, cele edukacyjne i badawczo-rozwojowe, opracowywanie innowacyjnych rozwiązań w interesie publicznym, a także trenowanie algorytmów mających zastosowanie w medycynie. W projekcie wniosku przedstawiono również szczegółowe wymagania dotyczące systemów elektronicznych kart zdrowia (EHR), czyli oprogramowania wykorzystywanego do przechowywania i udostępniania dokumentacji zdrowotnej. Dotyczą one interoperacyjności i bezpieczeństwa, a także warunków technicznych, jakie systemy te będą musiały spełniać. Tworzenie przestrzeni będzie finansowane i rozwijane przez EU4Health oraz inne programy związane ze zdrowiem cyfrowym, np. Horyzont Europa i Digital Europe.

ASPEKTY TECHNOLOGICZNE

Różnorodność elementów składających się na strukturę informatyczną sektora medycznego sprawia, że trudno może być zarządzać placówkami, które nie są w tym zakresie zaawansowane. Systemy składające się na infrastrukturę IT to przede wszystkim systemy dla jednostek służby zdrowia i systemy wspomagania diagnostyki, przetwarzania i analizy sygnałów medycznych (np. EKG), przetwarzania i analizy obrazów medycznych, oprogramowanie aparatury medycznej, standardy wymiany informacji HL7 (Health Level Seven), DICOM (Digital Imaging and Communications in Medicine), medyczne bazy danych.[190] Para-

[189] L. Bertuzzi, G. Fortuna, *LEAK: The EU Commission's data space for unleashing health data*, Euractiv 2022, https://www.euractiv.com/section/digital/news/leak-the-eu-commissions-data-space-for-unleashing-health-data/ (dostęp: 15.03.2022).

[190] K. Batko, *Możliwości wykorzystania systemów analitycznych w usprawnianiu opieki zdrowotnej,* „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" nr 316/2017, s. 18–28.

doksalnie 94,19 proc. pomieszczeń posiada dostęp do sieci komputerowej i w 90 proc. ankietowanych podmiotów wszyscy pracownicy medyczni lub ich zdecydowana większość mają dostęp do komputera, ale ponad 69 proc. podmiotów nie digitalizuje dokumentacji papierowej.[191] Mimo dostępu do sieci i możliwości skorzystania z wypracowywanych międzynarodowo standardów informatycznych, aż 93 proc. ankietowanych podmiotów wskazywało wydruk jako najpowszechniejszą metodę przekazania innemu podmiotowi lub placówce medycznej dokumentacji w postaci elektronicznej. Jedynie 37 proc. ankietowanych eksportuje dokumentację na elektroniczny nośnik, a nieco ponad 15 proc. przez usługi elektroniczne udostępnione z systemu teleinformatycznego.

Mimo istnienia regulacji dla sektora publicznego zawartych w Krajowych Ramach Interoperacyjności czy rekomendacji Rady ds. Interoperacyjności działającej przy Centrum e-Zdrowia, jedynie 68 proc. placówek posiada rozwiązania IT pozwalające na prowadzenie dokumentacji w postaci elektronicznej oraz przetwarzanie jednostkowych danych medycznych, a 89 proc. badanych świadczeniodawców nie wdrożyło usług elektronicznych przeznaczonych dla innych podmiotów leczniczych. Taki stan rzeczy uniemożliwia zapewnienie odpowiedniego poziomu interoperacyjności w placówkach publicznych, nie mówiąc już o całkowitym braku włączania danych pozyskanych z inteligentnych urządzeń, tj. Apple Watch, aplikacji zdrowotnych i medycznych.[192]

Statystyki z ostatnich lat wskazują jednak, że danych zbieranych cyfrowo będzie przybywać. Do grudnia 2019 r. Internetowe Konto Pacjenta miało zaledwie 900 tys. osób, ale wybuch pandemii koronawirusa spowodował niemal dziesięciokrotny wzrost ich liczby: w lipcu 2021 r. sięgnęła 10 mln.[193,194] Z kolei od lipca 2021 r. ok. 20 tys. podmiotów medycznych zgłosiło blisko 100 mln zdarzeń medycznych, co jak na początek działania systemu stanowi dość obiecującą liczbę.[195]

Tak znacząca ilość danych, przy zapewnieniu odpowiedniej interoperacyjności, mogłaby nie tylko przyczynić się do rozwoju rozwiązań technologicznych wspierających lekarzy w podejmowaniu decyzji, ale również przyspieszyć pewne

---

[191] Centrum e-Zdrowia, *Badanie stopnia informatyzacji podmiotów wykonujących działalność medyczną*, Warszawa 2021, wydanie V, https://cez.gov.pl/fileadmin/user_upload/Ankieta/raport_z_v_edycji_badania_stopnia_informatyzacji_podmiotow_wykonujacych_dzialalnosc_lecznicza_61127c7891061.pdf (dostęp: 4.03.2022).

[192] J.J. Zygmuntowski, op.cit., s. 22.

[193] *Internetowe Konto Pacjenta: liczba użytkowników przekroczyła 10 mln*, „Puls Medycyny" 2021 [online].

[194] „Puls Medycyny", https://pulsmedycyny.pl/ponad-10-mln-polakow-posiada-internetowe-konto-pacjenta-1121716 (dostęp: 4.03.2022).

[195] *Ekosystem innowacji dla szpitali – podsumowanie panelu dyskusyjnego z jesiennej konferencji programowej Polskiej Federacji Szpitali*, Medonet 2022, https://www.medonet.pl/magazyn-digital-health/ochrona-zdrowia-w-polsce,ekosystem-innowacji-dla-szpitali-podsumowanie-panelu-dyskusyjnego-z-jesiennej-konferencji-programowej-polskiej-federacji-szpitali,artykul,49728409.html#-najwazniejsze-osiagniecia-technologiczne-w-opiece-nad-pacjentem (dostęp: 4.03.2022).

procesy dla pacjentów. Problemem jest jednak wielość stosowanych systemów, nabywanych od różnych prywatnych dostawców – nawet w ramach sektora publicznego nie jest to jeden operator. Jeśli chodzi natomiast o rekomendowane systemy, mające wspierać wymianę danych między placówkami, większość podmiotów nie stosuje udostępnionej przez CeZ Polskiej Implementacji Krajowej HL7 CDA.[196] Wyróżnia się sześć głównych systemów zapisywania danych: HIS, LIS, PACS, RIS, Apteka oraz Hurtownia danych medycznych. W związku z tym dane mogące występować w różnych formatach i zapisach nie będą łatwe do przenoszenia między placówkami. Konieczne jest zatem przyjęcie jednego, wspólnego standardu, zarówno dla podmiotów publicznych, jak i prywatnych, by móc wykorzystać inne możliwości techniczne, które w Polsce już teraz prężnie się rozwijają (np. projekt dotyczący Internetowego Konta Pacjenta).

ASPEKTY DEMOGRAFICZNE

Pewne bariery w adaptacji proponowanych rozwiązań mogą wynikać ze starzenia się ludności, a także poziomu umiejętności cyfrowych zarówno pacjentów, jak i pracowników służby zdrowia wymaganego do korzystania z różnych rozwiązań. Raport Polskiego Instytutu Ekonomicznego wskazuje, że osoby w wieku od 18 do 24 lat chętniej dzielą się danymi niż starsze, z wyłączeniem danych dotyczących oszczędności energii.[197] Pozostaje również kwestia nierówności w umiejętnościach cyfrowych. Autorzy raportu twierdzą, że respondenci posiadający wysokie umiejętności cyfrowe, ze względu na poczucie posiadania kontroli nad dalszym losem ich danych, częściej deklarowali chęć podzielenia się nimi na potrzeby publicznych programów. Powstaje tu sytuacja paradoksalna: osoby, które statystycznie najczęściej korzystają z opieki medycznej, mają największe problemy z zaadaptowaniem się do nowych warunków. W rezultacie wprowadzenie nawet najbardziej innowacyjnych rozwiązań może nie przynieść oczekiwanego rezultatu, a zaawansowane zarządzanie danymi może napotkać identyczne bariery w adaptacji jak rozwój Internetowego Konta Pacjenta pod kątem demografii – wśród osób posiadających konto najliczniejszą grupę użytkowników stanowią osoby między 35. a 50. rokiem życia (30 proc.), natomiast najmniej liczną – osoby mające ponad 75 lat, które aktywowały ponad 108 tys. kont. Od 2020 r. odnotowano jednak przyrost aktywowanych kont osób powyżej 75. roku życia.[198] Dla wyrównania

[196] Centrum e-Zdrowia, op.cit.

[197] J. Grzeszak, et al., op.cit.

[198] Centrum e-Zdrowia, *Już 10 milionów Polaków korzysta z Internetowego Konta Pacjenta w serwisie pacjent.gov.pl*, Warszawa 2021, https://cez.gov.pl/aktualnosci/szczegoly/juz-10-milionow-polakow-korzysta-z-internetowego-konta-pacjenta-w-serwisie-pacjentgovpl/ (dostęp: 17.02.2022).

szans i możliwości osób nieposiadających wystarczających kompetencji cyfrowych w zakresie dzielenia się danymi dobrym rozwiązaniem jest przeszkolenie pracowników działów technicznych ochrony zdrowia.

Praktyki międzynarodowe

Państwa różnią się ze względu na sposób organizacji sektora medycznego, stosują systemy ogólnokrajowe (np. Wielka Brytania, Francja, Belgia) i regionalne (np. Hiszpania, Włochy), a także ze względu na sposób finansowania (model oparty na ubezpieczeniach stosowany jest w Niemczech, Francji, Belgii i Holandii, natomiast finansowanie bezpośrednio z budżetu państwa można spotkać w krajach skandynawskich, Wielkiej Brytanii i Hiszpanii).[199] Metody te, jak również posiadane przez państwo doświadczenie w tworzeniu zbiorów danych, dzielą kraje europejskie na bardziej i mniej zaawansowane w zakresie przetwarzania danych dotyczących zdrowia (np. w krajach skandynawskich narodowe zbiory danych istnieją od lat 70. XX w., a krajowe strategie EDM ułatwiają powiązanie informacji na temat różnych rodzajów opieki).

Inicjatywy wykorzystywania zbiorów danych dotyczących zdrowia i zarządzania nimi w celu dalszego wykorzystania można podzielić na rozwijane oddolnie przez rozmaite organizacje i odgórnie – przez organy państwowe. Flagowym przykładem zapewnienia interoperacyjności danych dotyczących zdrowia na wysokim poziomie jest estoński X-Road. To program wymiany danych stawiający jakość usług i dobro obywatela na pierwszym miejscu, zgodnie z przekonaniem, że zarówno publiczni, jak i prywatni usługodawcy muszą być przygotowani do współpracy ze sobą, a udostępnienia danych powinno się wymagać od obywatela tylko raz.[200] Pracownicy ochrony zdrowia mają obowiązek przesyłania danych do systemu informacji zdrowotnej (HIS), do którego dostęp mają wyłącznie licencjonowani pracownicy medyczni, za pomocą kart identyfikacyjnych do uwierzytelniania i podpisów cyfrowych.[201] Pacjenci natomiast mają możliwość dostępu do danych zdrowotnych i ich kontroli za pośrednictwem Portalu Pacjenta, delegowania dostępu do swoich danych, monitorowania wizyt i rezygnacji z udostępniania swoich danych w bazie („opt-out"). Cała architektura przekazu działa jak „nakładka" na bazy danych, która odpowiednio standaryzu-

---

[199] *Onkologia. W stronę polityki zdrowotnej opartej na danych. Rekomendacje dla Polski. Raport*, red. M. Libura, M. Władysiuk, Alivia Fundacja Onkologiczna, Warszawa 2020.

[200] *Interoperability services,* e-Estonia 2022, https://e-estonia.com/solutions/interoperability-services/x-road/ (dostęp: 5.03.2022).

[201] World Health Organization, 2018, *Towards a roadmap for the digitalization of national health systems in Europe*, Regional Office for Europe, https://www.euro.who.int/__data/assets/pdf_file/0008/380897/DoHS-meeting-report-eng.pdf (dostęp: 5.03.2022).

je informacje o pacjentach i udostępnia je usługodawcom. Podstawą bezpieczeństwa tego systemu są zaawansowane metody szyfrowania, dzięki którym autentyczność danych elektronicznych można udowodnić matematycznie i ani hakerzy, ani administratorzy systemów, ani nawet rząd nie mogą manipulować danymi czy przepisać historii.[202]

Innym przykładem dobrych praktyk zagranicznych, zapewnianych przez władzę publiczną, jest francuski Health Data Hub. To chmura obliczeniowa działająca od 2019 r. i zbierająca dane medyczne z różnych instytucji w ramach jednej przestrzeni cyfrowej. W systemie znajdują się dane z Krajowego Systemu Danych Zdrowotnych (SNDS), a więc wszystkie dane zdrowotne związane z refundacją ubezpieczenia zdrowotnego, niezależnie od tego, czy zostały zebrane podczas leczenia szpitalnego, wizyty lekarskiej, uczestnictwa w kohorcie badawczej, epidemiologicznej, rejestru praktyk.[203] Dane są pseudonimizowane i dostęp do nich będą mieli jedynie koordynatorzy wybrani przez państwową instytucję nadzorującą przestrzeganie zasad korzystania z danych (CNIL) oraz panel ekspertów. Prawo francuskie zabrania używania i wykorzystywania danych, chyba że są przeznaczone do celów związanych z interesem publicznym pod warunkiem wyrażenia zgody przez Krajową Komisję Ochrony Danych i Wolności (CNIL).[204] Rozwiązanie to nie jest jednak idealne – dane dotyczące zdrowia francuskich obywateli znajdują się w chmurze dostarczanej przez Microsoft Azure, co w związku z ryzykiem uzyskania dostępu amerykańskich służb bezpieczeństwa do tych danych budzi znaczne wątpliwości dotyczące ich bezpieczeństwa. Mimo licznych kontrowersji i zapowiedzi migracji na inną platformę, do tej pory nie podano bardziej szczegółowych informacji na ten temat.[205]

Ciekawym rozwiązaniem dysponuje również Finlandia. W systemie Findata przechowywane są dane dostarczone m.in. od prywatnych i publicznych dostawców usług z sektora medycznego, Fińskiego Instytutu Zdrowia i Opieki Społecznej, Fińskiego Instytutu Zdrowia Pracy, dane pobrane z usługi podobnej do polskiego Internetowego Konta Pacjenta.[206] Udzielaniem pozwoleń na wykorzystywanie danych zajmuje się Fiński Urząd ds. Zezwoleń na Udostępnianie Danych Społecznych i Zdrowotnych, a zainteresowane podmioty mogą wysyłać wnioski o udzielenie pozwolenia przez aplika-

---

[202] *Enterprise Estonia, 2022 b, Cybersecurity*, e-Estonia, https://e-estonia.com/solutions/cyber-security/ksi-blockchain/ (dostęp: 5.03.2022).

[203] *About the Health Data Hub*, Health Data Hub 2022, https://www.health-data-hub.fr/page/faq-english (dostęp: 5.03.2022).

[204] Ibidem.

[205] M. Pollet, *French decision too have Microsoft host Health Data Hub still attracts criticism*, Euractive France 2021, https://www.euractiv.com/section/health-consumers/news/french-decision-to-have-microsoft-host-health-data-hub-still-attracts-criticism/ (dostęp: 5.03.2022).

[206] *About Findata*, Findata – Finnish Social and Health Data Permit Authority 2022, https://findata.fi/en/about-findata/ (dostęp: 5.03.2022).

cję. Jeżeli istnieje taka potrzeba, dane są wcześniej anonimizowane i udostępniane przez kontrolerów Findata w ustandaryzowanej formie. Za uzyskanie dostępu należy uiścić odpowiednią opłatę. Ceny usług Findata zależą od tego, ilu materiałów oraz na jak długo potrzebuje klient, a także, do jakich celów zostaną wykorzystane dane. Przykładowo, udostępnienie danych do pracy naukowej (magisterskiej, doktoranckiej) kosztuje 250 euro, a do celów biznesowych – 1000 euro. Jeżeli dane będą używane poza Unią Europejską, koszt pozwolenia wzrasta do 3000 euro.[207]

Warto zwrócić uwagę również na projekty z inicjatywy obywatelskiej czy akademickiej. Salus.coop to spółdzielnia danych obywatelskich, której celem jest wspieranie badań i innowacji w sektorze opieki zdrowotnej.[208] Dzielenie się danymi zgromadzonymi w ramach spółdzielni oparte jest na licencji SALUS CG umożliwiającej przekazywanie danych dotyczących zdrowia pod pięcioma warunkami: (1) dane będą wykorzystywane w badaniach nad ochroną zdrowia, (2) przez instytucje niekomercyjne, (3) które otwarcie i nieodpłatnie dzielą się wynikami swoich badań (4) przy jednoczesnej ich pseudonimizacji na najwyższym poziomie (5) i do czasu wycofania zgody przez dawcę danych.[209]

[207] *Pricing*, Findata – Finnish Social and Health Data Permit Authority 2022, https://findata.fi/en/pricing/ (dostęp: 5.03.2022).

[208] *About us*, Salus Coop 2021, https://www.saluscoop.org/acerca (dostęp: 5.03.2022).

[209] *Licencia*, Salus Coop 2021, https://www.saluscoop.org/licencia (dostęp: 5.03.2022).

Rekomendacje

Głównym celem poprawy jakości zarządzania danymi w Polsce powinno być wytworzenie Wspólnej Wartości Społecznej (*Shared Social Value*) w taki sposób, by przez dzielenie się danymi dotyczącymi zdrowia polepszyć jakość oferowanych usług medycznych. W tym celu konieczny jest symultaniczny rozwój triady wartości, na których opiera się zarządzanie danymi: interoperacyjności, dostępności danych i transparentności funkcjonowania instytucji zarządzających, z zachowaniem inkluzywności i poszanowania zasad prawnych i etycznych.

I. Zwiększenie interoperacyjności danych zdrowotnych przez ujednolicenie standardów

a. Ramy czasowe: 1–2 lata

Mając na uwadze nierównomierne zaawansowanie techniczne, należy umożliwić podmiotom przystosowanie techniczne do wyznaczonych norm w odpowiednio długim czasie. Jednocześnie dalszy horyzont czasowy mógłby spowodować nadmierne „rozprężenie" wśród obowiązanych podmiotów, w rezultacie czego wiele z nich mogłoby ulec pokusie implementowania standardów w pośpiechu, co miałoby niekorzyst-

ne skutki dla faktycznie zamierzonego celu.

b. Konieczność zmian instytucjonalnych

Wypracowanie Wspólnej Wartości Społecznej wymaga od wszystkich podmiotów z danego sektora działania zgodnie z interesem publicznym. W tym celu należy wprowadzić obowiązek stosowania międzynarodowo wypracowanych standardów zarówno przez instytucje publiczne, jak i prywatne. W tak newralgicznych obszarach rynku, jak ochrona zdrowia, konieczna jest twarda harmonizacja standardów i wybranie jednego lub dwóch standardów interoperacyjności, np. formatów wypracowanych przez Integrating the Healthcare Enterprise: HL7 (Health Level 7) oraz DICOM (Digital Imaging and Communications in Medicine).[210]

c. Konieczność zmian prawnych

Do tej pory wymagania co do interoperacyjności danych obowiązywały jedynie na poziomie zaleceń, a jeśli były określone w wiążącym akcie prawnym, dotyczyły jedynie podmiotów z sektora publicznego. Ze względu na transgraniczny charakter usług, zwłaszcza medycznych, ujednolicenie standardów interoperacyjności powinno dotyczyć nie tylko wymiany między sektorem publicznym i prywatnym, ale też między podmiotami z różnych państw UE. Ujawniony niedawno wyciek zawierający informacje dotyczące nowej propozycji Komisji Europejskiej w zakresie wykorzystywania danych medycznych dla rozwoju nowych technologii musi zawierać zatem takie mechanizmy prawne, które ułatwią wdrażanie przyjętych ram interoperacyjności w wyznaczonym czasie i ewentualne egzekwowanie braku ich wdrożenia.

II. Utworzenie wspólnicy danych zdrowotnych

a. Ramy czasowe: 2–3 lata

Wspólnica danych zdrowotnych to projekt wymagający współdziałania wielu czynników w tym samym czasie: istnienia odpowiednich regulacji prawnych, uprawniających do gromadzenia danych dotyczących zdrowia, organizacji zarządzającej wspólnicą, odpowiednich zabezpieczeń technicznych itd. Konieczne jest zapewnienie infrastruktury, zespołu specjalistów oraz przygotowanie istniejącego oprogramowania do interoperacyjności silnej, m.in. w dialogu z interesariuszami sektora zdrowia.

b. Konieczność zmian instytucjonalnych

Z uwagi na innowacyjność projektu większość jego elementów będzie wymagała stworzenia ram instytucjonalnych od

[210] K. Bourquard, *eHealth Interoperability in Poland. Report on profile recommendations for e-Referral and exchange of medical documentation* (P1/Increment 2 & 3), IHE 2017.

początku – w oparciu o ideę ekosystemu zaufania dla cyfrowych danych, konieczne będzie stworzenie przestrzeni pluralistycznych instytucji mających u podstaw zasady wspólnego dysponowania danymi,[211] którymi zarządzać będzie niezależny, demokratyczny operator wspólnicy. Ze względu na istniejące regulacje prawne może to być repozytorium naukowe lub organizacja zajmująca się pracami badawczo-rozwojowymi. We wspólnicach gromadzone będą dane dotyczące zdrowia, pochodzące m.in. z Centrum Systemów Informacyjnych Ochrony Zdrowia, Narodowego Funduszu Zdrowia, Państwowej Inspekcji Sanitarnej, Państwowej Inspekcji Farmaceutycznej, szpitali, praktyk lekarskich, fundacji, prywatnych sieci medycznych i ubezpieczeń, aptek, a także aplikacji zdrowotnych i inteligentnych urządzeń.

Demokratyczna kontrola nad zarządzaniem wspólnicami umożliwi wgląd obywateli w personalne zestawy danych, z możliwością ich modyfikacji lub usunięcia (zgodnie z RODO). Odpłatność za korzystanie ze zgromadzonych danych będzie zależała od typu podmiotu ubiegającego się o możliwość przetwarzania danych. Darmowy dostęp będzie przewidziany dla organizacji pożytku publicznego i naukowców, start-upy będą miały dostęp jedynie do „piaskownicy" wspólnicy, czyli ograniczonego zasobu danych, a podmioty komercyjne zostaną zobowiązane do uiszczenia stosownej opłaty i wykazania zgodności celu i zakresu przetwarzania z regulaminem wspólnicy (*terms and conditions*). Udzielenie tym ostatnim dostępu do danych zgromadzonych we wspólnicy będzie uprawniać ją do 10-proc. udziału w zyskach i kontrolowania w określonym zakresie wytworzonych praw własności intelektualnej.[212]

Aby uniknąć transferu danych i ewentualnej zmiany jurysdykcji, koncepcja wspólnic zostanie oparta na idei przenoszenia algorytmu do danych (MIT OPAL), a więc prowadzenia bezpośrednich obliczeń na danych zgromadzonych we wspólnicy z wykorzystaniem algorytmu przekazanego przez klienta. Następnie będą mu przekazywane wyniki operacji na danych. Możliwe również, że potencjalna wspólnica musiałaby oferować bezpieczną „piaskownicę" do obliczeń, czyli konkretne serwery przystosowane do uczenia maszynowego.

c. Konieczność zmian prawnych

Reformy będą wymagały przepisy dotyczące ochrony danych osobowych i wykorzystywania ich do celów badań naukowych. Dla prawidłowego funkcjonowania całego ekosystemu konieczne

[211] G. Mulgan, V. Straub, *The new ecosystem of trust: How data trusts, collaboratives and coops can help govern data for the maximum public benefit*, Nesta 2019, https://www.nesta.org.uk/blog/new-ecosystemtrust/.

[212] J.J. Zygmuntowski, L. Zoboli, P.F. Nemitz, *Embedding European values in data governance: a case for public data commons*, Internet Policy Review. Journal on internet regulation 2021, https://policyreview.info/pdf/policyreview-2021-3-1572.pdf.

jest ułatwienie dostępu do danych zdrowotnych pacjentów przez wprowadzenie wyjątku od konieczności uzyskania zgody pacjenta na przetwarzanie, jeżeli będzie chodziło o wspólnicę zarządzaną przez wymieniony w ustawie instytut prowadzący badania naukowe, albo uproszczenie procedury udzielania zgody danych i promowanie tego rozwiązania w sposób „miękki", z jednoczesnym zachowaniem prawa do rezygnacji („opt-out") z trzymania danych we wspólnicy.

Do dokonania tych zmiany niezbędna będzie reforma ustaw sektorowych, w szczególności ustawy o prawach pacjenta, a także nałożenia na firmy prywatne, znacząco wpływające na rynek cyfrowy, ustawowego obowiązku przekazywania danych do wspólnic, szczególnie w branżach związanych z interesem publicznym.

Ważne jest również stworzenie regulaminu wspólnicy, zawierającego nie tylko postanowienia dotyczące warunków technicznych korzystania z jej zasobów, czasu trwania umowy czy sposobów jej rozwiązania, ale też oświadczenia i obowiązki stron w zakresie odpowiedniego, etycznego korzystania ze zbiorów danych, wraz z zachowaniem wcześniej wyznaczonego poziomu bezpieczeństwa i przejrzystości, a także obustronne klauzule poufności (NDA).

III. Zatrudnienie asystentów i podnoszenie kompetencji zarządzania danymi

a. Ramy czasowe: 1–1,5 roku

To kluczowy element łączący interoperacyjność danych z gromadzeniem ich w ramach wspólnic. Z jednej strony horyzont czasowy nie powinien więc być nadmiernie wydłużony, pozostawiając racjonalny czas na przeprowadzenie szkoleń i dostosowanie podmiotów do nowych wymogów.

b. Konieczność zmian instytucjonalnych

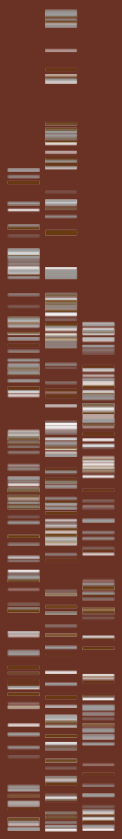
Do zatrudnienia dużego grona osób jako asystentów zajmujących się wprowadzaniem danych konieczne będzie przeprowadzenie wstępnego testu w formie projektu pilotażowego, obejmującego platformy wymiany wiedzy, kursy i szkolenia. Konieczne może okazać się również wprowadzenie przedmiotu nie tylko na studiach w zakresie cyberbezpieczeństwa czy zarządzania podmiotami leczniczymi dla osób mogących pełnić funkcje asystenta, ale też na studiach medycznych przygotowujących do wykonywania zawodów, w ramach których istnieje obowiązek prowadzenia dokumentacji medycznej.

Asystenci powinni nie tylko zdobyć wiedzę na temat interoperacyjności danych, wykorzystywanych formatów i działania wspólnic, ale też być osobami pierwsze-

go kontaktu dla sceptycznie nastawionych pacjentów, swoistymi „ambasadorami" całego projektu. Będzie to sprzyjać zwiększaniu przejrzystości procesów i polepszaniu stanu świadomości społecznej w zakresie dzielenia się danymi. Powodzenie projektu zależy bowiem od odpowiednio wysokiego poziomu zaufania publicznego do wspólnic danych i dalszego jego pogłębiania.

c. Konieczność zmian prawnych

Zatrudnianie asystentów mogłoby odbywać się na podstawie standardowej umowy o pracę. Stworzenie szkoleń czy kursów w tym zakresie nie wymaga również szczególnych zmian regulacyjnych.



06

MICHAŁ BEDLICKI

p.o. dyrektor, Centrum Monitorowania Jakości w Ochronie Zdrowia

Cyfryzacja a bezpieczeństwo opieki medycznej

Przez wiele lat podstawowy paradygmat związany z bezpieczeństwem medycyny „Primum non nocere" odnosił się bezpośrednio do czynności wykonywanych przez lekarza, a później również przez przedstawicieli innych zawodów medycznych. Wraz z postępem cywilizacyjnym jego zakres rozszerzono na funkcjonowanie systemu opieki zdrowotnej. Naturalne stało się, że kwestie bezpieczeństwa odnoszą się już nie tylko do sposobu wykonania konkretnej czynności czy zakresu udzielanej porady, ale również do kwestii organizacji systemu opieki zdrowotnej, higieny czy epidemiologii.

Wraz z pojawieniem się w zakładach opieki zdrowotnej pierwszych narzędzi informatycznych stało się oczywiste, że również sposób organizacji tego obszaru ma wpływ na bezpieczeństwo pacjentów, a w wyniku rozwoju informatyki będzie to wpływ coraz większy.

Pierwotnie wdrażane rozwiązania informatyczne stanowiły próbę zmiany sposobu prowadzenia dokumentacji medycznej z formy papierowej na zapisy elektroniczne, które z natury zapewniały czytelność wpisu, wymuszały podanie określonych zakresów danych. Z pewnością już zapewnienie czytelności wpisów ma wpływ na poprawę bezpieczeństwa, dzięki zagwarantowaniu jednoznaczności zapisanej informacji, czytelnej dla wszystkich uczestników opieki nad pacjentem. Przyglądając się jednak bliżej problemom bezpieczeństwa w opiece zdrowotnej, należy wskazać, że informatyzacja ma bardzo duży wpływ na bezpieczeństwo, a dotyczy on kilku płaszczyzn.

Bezpieczeństwo danych

Pierwszą z nich jest kwestia bezpieczeństwa samego systemu informatycznego, rozumianego jako bezpieczeństwo danych gromadzonych przez podmiot na poziomie lokalnym.

W trosce o zapewnienie bezpieczeństwa opieki medycznej pod kątem informatyki organizacje opieki medycznej opracowały specjalne procedury i wytyczne. Jednym z najważniejszych dokumentów w tej dziedzinie jest standard HIPAA (Health Insurance Portability and Accountability Act), który określa wymagania dotyczące ochrony prywatności i bezpieczeństwa informacji medycznych w Stanach Zjednoczonych.

W ramach standardu HIPAA placówki medyczne muszą zapewnić, że informacje medyczne są przechowywane w sposób bezpieczny i poufny. Wymaga to m.in. stosowania systemów informatycznych zabezpieczających dostęp do danych, uwierzytelniania użytkowników, monitorowania działań na systemie oraz stosowania szyfrowania dla ochrony informacji podczas przesyłania jej między różnymi systemami.

Innym ważnym standardem w tej dziedzinie jest ISO 27001, który określa wymagania dotyczące zarządzania bezpieczeństwem informacji. Podmioty medyczne, które stosują ten standard, muszą przestrzegać ścisłych zasad związanych z zarządzaniem bezpieczeństwem informacji, takich jak stosowanie polityki bezpieczeństwa informacji, przeprowadzanie audytów bezpieczeństwa informacji czy też regularne szkolenia pracowników w zakresie ochrony prywatności i bezpieczeństwa informacji.

Również w systemach akredytacyjnych znajdziemy bezpośrednie odniesienia do tak rozumianego bezpieczeństwa. Zarówno w najstarszym systemie amerykańskim, prowadzonym przez Joint Commission on Accreditation of Healthcare Organizations, jak i w systemie kanadyjskim oraz wielu innych znajdziemy wymogi dotyczące bezpieczeństwa systemu informatycznego.

Przykładowo, standardy Joint Commisssion International wymagają, aby szpitale miały systemy informatyczne, które umożliwiają przechowywanie, udostępnianie i przetwarzanie informacji o pacjentach w sposób bezpieczny i zgodny z obowiązującymi przepisami. Ponadto standardy JCI określają warunki dotyczące szkoleń personelu medycznego w zakresie korzystania z systemów informatycznych oraz regularnych audytów systemów informatycznych w celu zapewnienia zgodności z wymaganiami dotyczącymi bezpieczeństwa i prywatności pacjentów.

Podobnie obowiązujące w Polsce standardy, opracowane przez Centrum Monitorowania Jakości w Ochronie Zdrowia i zatwierdzone przez ministra zdrowia, poruszają tę problematykę (patrz: ramka Standardy akredytacyjne 2009, dział „Zarządzanie informacją").

Warto również zauważyć, że istnieją różne rodzaje zagrożeń związanych z informatyką w opiece medycznej. Jedno z największych stanowią cyberataki, w wyniku których może dojść do kradzieży danych medycznych lub zablokowania systemów informatycznych. Warto zatem inwestować w systemy zabezpieczeń antywirusowych, zaporę ogniową oraz regularne aktualizacje oprogramowania.

W ostatnim czasie mieliśmy do czynienia z atakami hakerskimi. Stanowiły zagrożenie dla sprawnego funkcjonowania jednostki i olbrzymie ryzyko narażenia na utratę dobrego wizerunku przez firmę.

Tym większe znaczenie ma właściwe zabezpieczanie zgromadzonych danych medycznych: przechowywanie na odrębnych fizycznie serwerach, systematyczne wykonywanie kopii zapasowych i stałe doskonalenie mechanizmów zabezpieczających przed atakiem.

STANDARDY AKREDYTACYJNE 2009, DZIAŁ „ZARZĄDZANIE INFORMACJĄ"

ZI 1 W szpitalu opracowano system gromadzenia danych i przetwarzania informacji.

ZI 1.1 Szpital określił osoby odpowiedzialne za bezpieczeństwo informacji na terenie jednostki.
ZI 1.2 Szpital określił zasady dostępu do sieci rozleglej dla pracowników i pacjentów szpitala.
ZI 1.3 Szpital określił zasady dostępu do zewnętrznych medycznych baz danych dla pracowników medycznych.

ZI 2 Szpital określił zasady bezpieczeństwa dotyczące informacji medycznej, w tym sposób postępowania w sytuacjach krytycznych.

ZI 3 Dokumentacja medyczna jest zabezpieczona.

ZI 3.1 Wersja papierowa dokumentacji medycznej jest zabezpieczona.
ZI 3.2 Archiwalna dokumentacja medyczna przechowywana jest bezpiecznie.
ZI 3.3 Archiwalna dokumentacja medyczna jest dostępna.
ZI 3.4 Zasady dokonywania wpisów i autoryzacja dokumentacji medycznej w wersji elektronicznej są określone.
ZI 3.5 Wersja elektroniczna dokumentacji medycznej jest zabezpieczona.

ZI 4 Dokumentacja medyczna jest czytelna, kompletna i autoryzowana.

ZI 5 W szpitalu wdrożono mechanizmy zapewniające regularną ocenę zawartości, kompletności oraz autoryzacji dokumentacji medycznej.

ZI 6 W szpitalu opracowano procedurę komunikacji z pacjentem w przypadku uzyskania wyników badań po wypisie.

W tym aspekcie coraz częstsze staje się pytanie dotyczące nakładów inwestycyjnych na zabezpieczenie danych i kwestii, czy dane powinny być zabezpieczone na poziomie lokalnym czy przez służące do tego celu rozwiązania serwerów zewnętrznych.

Bezpieczeństwo realizowanych procesów medycznych

Dobrze zaprojektowany system informatyczny poprawia efektywność opieki na wielu poziomach. Wydaje się, że praktycznie nie ma już obszarów funkcjonowania placówek ochrony zdrowia, które w większym lub mniejszym stopniu nie byłyby objęte informatyzacją. Dotyczy to zarówno części „szarej", służącej administracji jednostki do rozliczania procedur, zarządzania jednostką, m.in. personelem medycznym, jak i części „białej", ściśle związanej z opieką nad pacjentem. Kluczowe wydają się jednak dwa aspekty:

1. Właściwa integracja poszczególnych modułów – powinna zapewnić sprawną wymianę danych, bez względu na to, czy w jednostce stosowany jest jeden wielofunkcyjny system, czy też złożony z kilku modułów dostarczonych przez różnych producentów.
2. Ergonomia rozwiązań – nakierowana na to, by praca z wykorzystaniem narzędzi informatycznych była mniej obciążająca niż z wykorzystaniem tradycyjnego papieru. Efekty wdrożenia systemu informatycznego powinny przewyższać uzyskiwane w przypadku dotychczasowej formy, a nie stanowić dodatkowe utrudnienie dla personelu medycznego.

Jednym z najlepszych przykładów wpływu cyfryzacji na bezpieczeństwo jest obszar leków. Informatyka ma wiele zastosowań w kontekście poprawy bezpieczeństwa leków, zwłaszcza w zakresie identyfikacji, monitorowania i zapobiegania błędom medycznym, związanym z lekami. Nowoczesne rozwiązania umożliwiają lekarzom i pielęgniarkom elektroniczne zamawianie i podawanie leków (*e-prescribing*). Dzięki temu minimalizowane są błędy ludzkie, takie jak nieprawidłowe odczytanie pisma lekarza lub nieporozumienia przy zamawianiu. W Polsce takim rozwiązaniem jest e-recepta, która rozpowszechniła się w czasie pandemii COVID-19 i stała się rozwiązaniem powszechnie obowiązującym.

Kolejnym przykładem są rozwiązania stanowiące elektroniczne profile medyczne. Systemy informatyczne pozwalają na przechowywanie elektronicznych profili medycznych pacjentów, które zawierają informacje na temat ich chorób, leków, które przyjmują, i inne ważne dane. Dzięki temu lekarze i personel medyczny mają łatwy dostęp do dokładnych informacji na temat pacjenta, co minimalizuje ryzyko błędów.

W jednostkach opieki zdrowotnej zyskały swoje miejsce (ale wciąż są rozwijane) systemy zarządzania lekami, takie jak apteczka oddziałowa, magazyn leków, apteka

szpitalna. Umożliwiają one personelowi medycznemu monitorowanie leków: dat ważności, składu i ilości. W efekcie minimalizuje się liczbę błędów medycznych, takich jak podawanie przeterminowanych lub niewłaściwych leków.

Niektóre szpitale wykorzystują również technologie informatyczne, np. kodowanie kreskowe lub RFID, systemy unit-dose, które umożliwiają łatwe i szybkie identyfikowanie leków, co pomaga zapobiegać błędom medycznym związanym z nieprawidłowym podawaniem lub zamawianiem leków. Mają one również znaczenie dla ekonomiki wykorzystania leków, wpływając na minimalizację zapasów przechowywanych na oddziałach. Systemy informatyczne umożliwiają również monitorowanie skutków ubocznych leków i szybkie reagowanie w przypadku ich wystąpienia.

Drugim obszarem, w którym informatyzacja dokonała olbrzymich postępów, jest diagnostyka obrazowa. Tomografia komputerowa, rezonans magnetyczny, ultrasonografia nie byłyby możliwe, gdyby nie technologie informatyczne, które są ich częścią. Jednak rozwój w zakresie maszynowego uczenia się i automatycznej analizy obrazu pozwala na automatyzację procesów diagnostycznych i poprawę jakości opieki zdrowotnej oraz ułatwia diagnozowanie chorób i urazów pacjentów. Ponadto cyfryzacja obrazu umożliwiła łatwe ich przekazywanie na odległość. Teleradiologia stała się w ostatnim dziesięcioleciu faktem.

Informatyka ma również ogromne znaczenie w planowaniu zabiegów radioterapii, jednego z najskuteczniejszych sposobów leczenia nowotworów, ale wymaga precyzyjnego i skomplikowanego procesu planowania. W planowaniu zabiegu radioterapii systemy informatyczne zapewniają m.in. stworzenie dokładnego modelu anatomicznego pacjenta, wykorzystywanego do opracowania planu leczenia. Pozwalają także na symulowanie rozkładu dawki promieniowania w tkankach, co ułatwia precyzyjne dostosowanie dawki do kształtu i rozmiaru guza, minimalizując dawkę dla otaczających tkanek zdrowych. Umożliwiają także sprawdzanie dawki promieniowania, kontrolowanie przemieszczania się pacjenta w trakcie zabiegu oraz monitorowanie wykonywania zabiegu przez personel medyczny.

Cyfryzacja znalazła zastosowanie również w pracy chirurga. Jednym z przykładów jest wykorzystanie systemów informatycznych do planowania i kontrolowania zabiegów. Dzięki temu chirurdzy mogą precyzyjnie zaplanować każdy etap operacji, wcześniej wykrywać problemy oraz reagować na nieprawidłowości występujące podczas zabiegu, co ma szczególne znaczenie w operacjach wieloetapowych. Systemy informatyczne umożliwiają również monitorowanie stanu pacjenta

w trakcie operacji, co pozwala na szybkie wykrycie komplikacji i pomaga anestezjologom w sprawowaniu opieki nad pacjentem podczas zabiegu i po nim.

Innym przykładem zastosowania IT jest chirurgia robotyczna, która pozwala na bardziej precyzyjne wykonywanie operacji, co wpływa na zmniejszenie ryzyka powikłań i skrócenie czasu rekonwalescencji pacjentów. W Polsce rozwijane są aktualnie ośrodki specjalizujące się w tego typu operacjach.

Informatyka zapewnia również szybsze korzystanie z wyników badań laboratoryjnych i, podobnie jak w radiologii, sprzyja interpretacji nie tylko pojedynczego badania, ale całej ich serii, ułatwia dostęp do zarchiwizowanych wyników i analizowanie ich, bez względu na miejsce ich wykonania. Systemy informatyczne upraszczają też ocenę jakości procedur laboratoryjnych przez śledzenie trendów wyników próbek kontrolnych.

Cyfrowa komunikacja z pacjentem

Cyfryzacja jest wsparciem w zakresie komunikacji z pacjentem, a tym samym przyczynia się do poprawy jego bezpieczeństwa. Systemy pozwalające na zebranie wywiadu online, ocenę dolegliwości czy aktualnych i starszych wyników opieki medycznej (PROSMS) wpływają na szybsze stawianie diagnozy, optymalizację procesów medycznych i umożliwiają ocenę efektów stosowanej terapii w dużych grupach pacjentów.

Wykorzystywanie stron internetowych podmiotów również stało się częścią informatyzacji służącą bezpieczeństwu. Wyjaśnienia dotyczące praw pacjentów, zakresu wykonywanych zabiegów, elementów edukacji dotyczących poszczególnych jednostek chorobowych umieszczane na stronach przez szpitale i poradnie stanowią dla pacjentów źródło informacji i jednocześnie odciążają personel. Decydujące znaczenie ma tu jakość tych informacji.

Technologia informatyczna, mająca wpływ na bezpieczeństwo pacjentów, stała się częścią badań opinii pacjentów. Przykładem takiego rozwiązania jest system PASAT OPEN, opracowany przez Centrum Monitorowania Jakości w Ochronie Zdrowia, który gromadzi również dane dotyczące poczucia bezpieczeństwa podczas hospitalizacji i pozyskiwane bezpośrednio od pacjentów informacje o zdarzeniach niepożądanych.

Dotykamy tu kolejnego obszaru, a mianowicie wykorzystania cyfryzacji do poprawy jakości opieki.

Informatyka a poprawa jakości opieki zdrowotnej

Wpływ cyfryzacji na poprawę jakości opieki możemy zaobserwować na różnych poziomach. Najważniejsze jest jednak dostarczanie jednostkom danych pozwalających na ocenę ich własnej sytuacji oraz umożliwienie porównań z wynikami uzyskiwanymi przez innych.

Możliwe to jest w odniesieniu do:

1. **Standardów akredytacyjnych** – ocena uzyskiwanego wyniku ogólnego, wyniku w odniesieniu do działów standardów czy poszczególnych standardów pozwala na wyciągnięcie wniosków mówiących zarówno o kondycji całego systemu opieki zdrowotnej, jak i poszczególnych szpitali.
2. **Wskaźników jakości** (analizy danych dotyczących najważniejszych wskaźników jakości). Wskaźniki jakości służą do mierzenia skuteczności, efektywności i bezpieczeństwa opieki medycznej, a ich monitorowanie pozwala na wczesne wykrycie problemów i podjęcie działań mających na celu ich rozwiązanie. Monitorowanie tych wskaźników to kluczowy element procesu poprawy jakości, dostarczający danych ułatwiających podejmowanie działań naprawczych.
3. **Rejestru zdarzeń niepożądanych** – należy jednak pamiętać o założeniach stanowiących fundament takiego systemu. Jego celem powinna być edukacja i wyciąganie wniosków dla uniknięcia podobnych zdarzeń w przyszłości. System powinien być nierepresyjny i zachowywać anonimowość pracowników ochrony zdrowia. Zdarzenia niepożądane to sytuacje, w których pacjenci doznają szkody lub uszczerbku na zdrowiu w wyniku błędów lub zaniedbań personelu medycznego, ale również systemów informatycznych. Przykładowo: w wyniku nieprawidłowego przetwarzania informacji medycznych przez system informatyczny może dojść do błędów w podawaniu leków lub diagnozowaniu chorób, co ma niepożądane skutki zdrowotne dla pacjentów.
4. **Rejestrów medycznych** – które są niezwykle ważne dla całego systemu zarządzania opieką zdrowotną i zapewnienia bezpieczeństwa pacjentów. Pozwalają na przechowywanie i udostępnianie kluczowych informacji o pacjentach, m.in. historii chorób, przyjmowanych leków, wyników badań diagnostycznych, procedur medycznych. Umożliwiają też wyciąganie wniosków w oparciu o długookresową ocenę całej populacji, której dotyczy wybrany problem medyczny. Dają więc szansę na wnioskowanie o efektach alternatywnych

ścieżek postępowania z pacjentem. Wymiana danych między rejestrami pozwala obserwować zależności związane z wielochorobowością. Kluczowe dla rejestrów jest jednak zarządzanie nimi zapewniające zasilanie danymi i walidacja.

Podsumowanie

Bez wątpienia cyfryzacja przeniosła kwestię bezpieczeństwa opieki zdrowotnej na zupełnie inny poziom. Otworzyła i wciąż otwiera nowe możliwości. Szczególnie wyraźnie widać to w zakresie wykorzystania sztucznej inteligencji, analizy dużych zbiorów medycznych i edukacji personelu medycznego z wykorzystaniem cyfrowych materiałów edukacyjnych oraz komunikacji online. Należy jednak wspomnieć o jednym z największych zagrożeń, jakie niesie ze sobą cyfryzacja w odniesieniu do bezpieczeństwa: nieupoważnionym dostępie do najbardziej wrażliwych danych zarówno z perspektywy pacjentów, jak i placówek ochrony zdrowia.

Przechowywanie danych w rejestrach medycznych wymaga odpowiedniego zabezpieczenia przed nieuprawnionym do nich dostępem i kradzieżą. Ważne jest stosowanie różnych metod ochrony, takich jak kryptografia, autoryzacja, uwierzytelnianie i audytowanie, które mają na celu zapobieganie nieautoryzowanemu dostępowi do danych medycznych. Ważne jest również, aby zwracać uwagę na zgodność z przepisami o ochronie danych osobowych, takimi jak RODO. Rejestry medyczne muszą być zgodne z prawnymi zasadami przetwarzania, a pacjenci muszą mieć prawo korzystania ze swoich danych medycznych i kontrolowania ich, a także pewność, że nie zostaną wykorzystane w sposób nieuprawniony.

Szeroka dyskusja o zakresie dostępu i wykorzystaniu danych medycznych powinna być jednym z elementów działań na rzecz bezpieczeństwa, bowiem nieuprawnione ich wykorzystanie może również przynieść szkodę i to nie tylko pojedynczemu pacjentowi, ale całym grupom.

07

MARIA LIBURA

Przewodnicząca Zespołu ds. Studiów Strategicznych OIL Warszawa,
Kierownik Zakładu Dydaktyki i Symulacji Medycznej,
Collegium Medicum, Uniwersytet Warmińsko-Mazurski

Cyfrowe nierówności w zdrowiu

Dynamiczny rozwój technologii cyfrowych i ich rosnąca dostępność coraz silniej wpływają na usługi opieki zdrowotnej na całym świecie. Narzędzia cyfrowe testowanie są w systemach ochrony zdrowia i zabezpieczenia społecznego z nadzieją na zwiększenie ich efektywności oraz poprawę jakości świadczeń.[213] Dotychczasowe doświadczenia z wdrażaniem e-zdrowia wskazują jednak, że narzędzia te, wprowadzane bez odpowiedniego przygotowania, pogłębiają istniejące nierówności w zdrowiu oraz wytwarzają nowe, często początkowo trudne do identyfikacji obszary wykluczenia i dyskryminacji.[214]

Wykorzystanie technologii cyfrowych staje się na naszych oczach podstawą świadczenia opieki zdrowotnej. Termin „zdrowie cyfrowe" lub e-zdrowie (ang. *digital health*) obejmuje użycie dostępnych technologii informacyjnych i komunikacyjnych w celu zapewnienia pacjentom usług profilaktycznych, leczenia i edukacji, a także monitorowania i kontroli chorób oraz poprawy dostępu do usług opieki zdrowotnej.[215] Elektroniczna dokumentacja medyczna, usługi telemedyczne, robotyka, a także zdrowie mobilne, wspierane przez wykorzystanie smartfonów, urządzeń ubieralnych, aplikacji mobilnych i różnych urządzeń monitorujących stan zdrowia, to przykłady znanych zastosowań e-zdrowia.[216]

Oczywistym obszarem nierówności jest dostępność rozwiązań cyfrowych, zarówno fizyczna, jak i finansowa. Skuteczne wykorzystanie wielu narzędzi cyfrowych wymaga bowiem posiadania odpowiedniej jakości urządzeń, takich jak smartfony, kamery internetowe, czujniki czy urządzenia ubieralne, umiejętności posługiwania się nimi, a także łącza internetowego odpowiedniej prędkości i jakości. Co więcej, zalew rozwiązań cyfrowych we wszystkich dziedzinach życia powoduje, że umiejętności cyfrowe i łączność z Internetem nabierają charakteru „superdeterminantów" społecznych zdrowia, ponieważ już dziś wpływają na wszystkie pozostałe społeczne i ekonomiczne uwarunkowania zdrowia.[217] Drugim obszarem o rosnącym znaczeniu w kontekście sprawiedliwego dostępu do opieki medycznej stają się zastosowania sztucznej inteligencji w praktyce klinicznej oraz zarządzaniu ochroną zdrowia, a w perspek-

---

[213] A. Sheikh, M. Anderson, S. Albala, B. Casadei, B.D. Franklin, M. Richards, D. Taylor, H. Tibble, E. Mossialos, *Health information technology and digital innovation for national learning health and care systems*. „Lancet Digital Health" 2021 Jun;3(6):e383-e396.

[214] F. Mougin , K.F. Hollis, L.F. Soualmia. *Inclusive Digital Health.* „Yearbook of Medical Informatics" 2022 Aug;31(1):2-6.

[215] *WHO guideline: recommendations on digital interventions for health system strengthening*, World Health Organization, 2019, https://apps.who.int/iris/bitstream/handle/10665/311941/9789241550505-eng.pdf?ua=1.

[216] B.K. Scott, G.T. Miller, S.J. Fonda, R.E. Yeaw, J.C. Gaudaen, H.H. Pavliscsak, et al. *Advanced digital health technologies for covid-19 and future emergencies*, „Telemedicine Journal and E-Health" 2020;26(10):1226-1233.

[217] C. Gibbons, *Digital Access Disparities: Policy and Practice Overview. Panel Discussion, Digital Skills and Connectivity as Social Determinants of Health* w: Sheon, A.: C*onference Report: Digital Skills: A Hidden „Super" Social Determinant of Health*. Interdisciplinary Association for Population Health Science, 2018.

RYSUNEK 15. UMIEJĘTNOŚCI CYFROWE A SPOŁECZNE UWARUNKOWANIA ZDROWIA[218]

tywie – także w kształtowaniu polityki zdrowotnej.[219]

Technologie cyfrowe niosą ze sobą obietnicę zwiększenia efektywności opieki zdrowotnej. Przedstawiane są jako zwinne (z j. ang. *agile*) rozwiązania, dostosowujące się szybko do zmieniających się uwarunkowań opieki zdrowotnej, wspomagające pracę lekarzy i innych pracowników sektora w zadaniach organizacyjnych i klinicznych, a obywatelom zapewniające lepsze usługi medyczne. Badania wykazały, że cyfrowe technologie zdrowotne mogą podnieść poziom wiedzy o zdrowiu, a także poprawić efektywność opieki zdrowotnej, zwłaszcza u pacjentów z chorobami przewlekłymi.[220] Być może dlatego opiekę skoncentrowaną na pacjencie zrównuje się coraz częściej z szerokim wprowadzeniem narzędzi zdrowia cyfrowego do codziennej praktyki klinicznej.[221] W zamyśle cyfryzacja ma umożliwić

[218] L.A. Celi, J.Cellini, M. Charpignon, E.C. Dee, F. Dernoncourt, R. Eber, W.G. Mitchell, L. Moukheiber, J. Schirmer, J. Situ, J. Paguio, J. Park, J.G. Wawira, S. Yao; for MIT Critical Data, *Sources of bias in artificial intelligence that perpetuate healthcare disparities-A global review*. „PLOS Digital Health" 2022 Mar 31;1(3):e0000022.

[219] C.J. Sieck, A. Sheon, J.S. Ancker, et al., *Digital inclusion as a social determinant of health*. npj „Digital Medicine" 4, 52 (2021).

[220] D. Lupton, Digitized health promotion: personal responsibility for health in the web 2.0 era w: To fix or to heal: patient care, public health, and the limits of biomedicine, red. J.E. Davis, A.M. Gonzalez, New York University Press; 2016:152–176.

[221] L.D. Sherman, S.W. Grande, Building better clinical relationships with patients: an argument for digital health solutions with black men, „Health Service Insights" 2019;12:1178632919834315

pacjentom przejęcie kontroli nad własnym zdrowiem i leczeniem, wzmacniając rolę samoopieki zarówno w zakresie profilaktyki, jak i leczenia. Dzięki temu obywatele mieliby niebawem zostać „menedżerami" własnego zdrowia, jak głosi zyskujący na popularności slogan. Władze publiczne i ubezpieczyciele liczą, że takie umocnienie pacjentów przyniesie zarazem oszczędności, podobnie jak przejęcie wielu zadań przez klientów bankowości elektronicznej przełożyło się na redukcję kosztów banków, związaną z obsługą klienta w tradycyjnych placówkach.

Nic zatem dziwnego, że większość państw i organizacji ochrony zdrowia przykłada coraz większą wagę do zdrowia cyfrowego. Liczba dokumentów kierunkowych i raportów dotyczących e-zdrowia stale rośnie. Także polskie władze przyjęły Program rozwoju e-Zdrowia na lata 2022–2027[222] oraz Strategię Centrum e-zdrowia 2023–2027.[223] Dokumenty te wytyczają kierunki i priorytety cyfrowej transformacji w naszym kraju w duchu, który nazwać można technoentuzjazmem. Nie ujmując niczego szansom, jakie otwierają przez sektorem zdrowia narzędzia cyfrowe w zakresie diagnostyki, leczenia i organizacji ochrony zdrowia, warto jednak uzupełnić tę perspektywę o zagrożenia, wśród których niebagatelną rolę odgrywają właśnie rysujące się nowe wzorce dyskryminacji. Niniejszy rozdział jest próbą uzupełnienia tej luki, gdyż z dotychczasowych doświadczeń na całym świecie można wnosić, że szybkie i bezrefleksyjne wdrożenie cyfryzacji w ochronie zdrowia doprowadza do pogłębienia się nierówności, przejawiających się w istotnych różnicach w stanie zdrowia różnych populacji oraz w niesprawiedliwej dystrybucji zasobów opieki zdrowotnej.[224]

Nierówności w dostępie do e-zdrowia

Nierówności w zdrowiu odnoszą się do różnic w zakresie stanu zdrowia lub dystrybucji zasobów opieki zdrowotnej wśród różnych populacji, powstałych ze względu na uwarunkowania społeczne, takie jak miejsce urodzenia, dorastania, zamieszkania lub zatrudnienia obywateli.[225] Szybko wprowadzane cyfrowe technologie zdrowotne zakładają powszechność dostępu do Internetu i urządzeń mobilnych, marginalizując osoby, które mają trudności z korzystaniem z nowych technologii: osoby starsze, o niskich

[222] https://www.gov.pl/web/zdrowie/program-rozwoju-e-zdrowia-na-lata-2022-2027.

[223] https://cez.gov.pl/sites/default/files/paragraph.attachments.field_attachments/2023-02/strategia_centrum_e-zdrowia_na_lata_2023-2027_1.pdf.

[224] R. Yao, W. Zhang, R. Evans, G. Cao, T. Rui, L. Shen, *Inequities in Health Care Services Caused by the Adoption of Digital Health Technologies. Scoping Review* „Journal of Medical Internet Research" 2022;24(3):e34144 doi: 10.2196/34144.

[225] R. Klein, D. Huang, *Defining and measuring disparities, inequities, and inequalities in the healthy people initiative*, Center for Disease Control and Prevention. 2010. https://www.cdc.gov/nchs/ppt/nchs2010/41_klein.pdf.

dochodach oraz zamieszkujące tereny bez łatwego dostępu do szerokopasmowych łączy.[226] Nierówności w dostępie do technologii dotyczą także osób z niepełnosprawnością, mniejszości etnicznych i migrantów, dla których stanowią dodatkową cyfrową przeszkodę w korzystaniu z usług zdrowotnych.[227] Najbardziej oczywistym problemem jest zatem niesprawiedliwe wdrażanie nowych technologii, które są powszechnie dostępne jedynie dla dobrze sytuowanych, wykształconych, młodszych pacjentów z wielkich miast oraz dla miejskich i akademickich ośrodków medycznych.[228]

Pandemia COVID-19 przyspieszyła masowe testowanie rozwiązań cyfrowych i opieki zdalnej, ukazując ich potencjał i ograniczenia. W okresie obostrzeń obejmujących ograniczenia w poruszaniu się i odbywaniu wizyt stacjonarnych część pacjentów czuła się wykluczona cyfrowo ze względu na:

- brak zainteresowania nowymi technologiami,
- brak umiejętności cyfrowych,
- wiek,
- niepełnosprawność,
- brak zaufania do władz publicznych i dostawców technologii,
- trudności językowe.[229]

Co więcej, w cytowanych badaniach zauważono cyfrowy efekt św. Mateusza: ci, którzy już wcześniej obeznani byli z technologiami cyfrowymi, zyskiwali na ich szerszym wprowadzeniu, a wykluczeni cyfrowo – tracili. Osoby, które stać na korzystanie z technologii i posiadają odpowiednie umiejętności, doceniały zalety cyfrowej opieki zdrowotnej i były chętne do inwestowania w rozwój swoich możliwości cyfrowych. Przykładowo osoba z niepełnosprawnością, mająca problemy z poruszaniem się, uaktualniła podczas pandemii swój pakiet szerokopasmowy i kupiła kamerę internetową, która potrafi rozpoznawać mowę, co znacznie ułatwiło jej interakcje cyfrowe. Natomiast ograniczenia finansowe i początkowe niskie kompetencje zniechęcały do ucyfrowienia. Dla przykładu: osoba wynajmująca małe mieszkanie uznała, że nie ma wystarczająco dużo miejsca na komputer. Wielu nie stać było na akcesoria, takie jak kamery internetowe czy czytniki ekranu dla osób z dysfunkcją wzroku, które ułatwiłyby im korzystanie z platform internetowych. W konsekwencji jeszcze bardziej zniechęciły się do korzystania z usług internetowych.[230]

---

[226] A. McAuley, *Digital health interventions: widening access or widening inequalities?* „Public Health" 2014;128(12):1118-1120.

[227] H.J. Krouse, C*OVID-19 and the widening gap in health inequity*, „Otolaryngology - Head Neck Surgery" 2020;163(1):65-66.

[228] T.C. Veinot, H. Mitchell, J.S. Ancker, *Good intentions are not enough: How informatics interventions can worsen inequality*, "Journal of the American Medical Informatics Association" 2018:1080–1081.

[229] https://www.healthwatch.co.uk/report/2021-06-16/locked-out-digitally-excluded-peoples-experiences-remote-gp-appointments

[230] Ibidem.

Wśród wniosków, jakie nasunął nieplanowany eksperyment w formie lockdownu, należy wskazać:

- potrzebę utrzymania realnej dostępności tradycyjnych modeli opieki obok narzędzi zdalnych,
- zagwarantowanie pacjentom pomocy w wyborze najodpowiedniejszego rodzaju wizyty, adekwatnej do ich potrzeb medycznych,
- konieczność finansowania i organizacji programów podnoszących umiejętności umożliwiające dostęp do opieki zdalnej wśród grup wykluczonych,
- wzmocnienie praw pacjentów korzystających z opieki zdalnej, aby osoby z większymi potrzebami wsparcia nie były pokrzywdzone podczas korzystania z niej,
- wsparcie świadczeniodawców w odgrywaniu aktywnej roli w integracji opieki cyfrowej z modelem tradycyjnym,
- realizację włączenia cyfrowego przez traktowanie dostępu do Internetu jako prawa obywatela.[231,232]

Stronnicze algorytmy, uprzedzenia sztucznej inteligencji

Zastosowania sztucznej inteligencji wpływają na coraz liczniejsze aspekty codziennego życia. AI już decyduje o tym, jakie treści użytkownicy widzą w mediach społecznościowych, a w niektórych państwach ustala, kto otrzyma świadczenia społeczne. Technologie AI są zazwyczaj oparte na algorytmach, które dokonują predykcji w celu wsparcia lub nawet pełnej automatyzacji procesu decyzyjnego. Coraz liczniejsze badania pokazują, w jaki sposób algorytmy stają się stronnicze, prowadząc do dyskryminacji. Uzasadnia to potrzebę bardziej kompleksowej i dokładnej ich oceny, zanim zostaną wykorzystane do podejmowania decyzji, które mogą mieć istotny wpływ na życie ludzi.[233]

Systemy ochrony zdrowia i świadczeniodawcy traktują pacjentów nierówno z dwóch głównych powodów: uprzedzeń (otwarcie deklarowanych lub podświadomych) lub braku wiedzy o problemach zdrowotnych specyficznych dla określonych grup. Rola AI w zdrowiu często przedstawiana jest jako antidotum na dotychczasowe nierówności. Obie te kwestie mogłyby teoretycznie zostać rozwiązane dzięki zastosowaniu AI:[234]

- algorytmy mogłyby podejmować decyzje wolne od stereotypów właściwych dla ludzkiego sposobu myślenia i podejmowania decyzji,
- systemy AI wspierające decyzje kliniczne, które są szkolone na wystar-

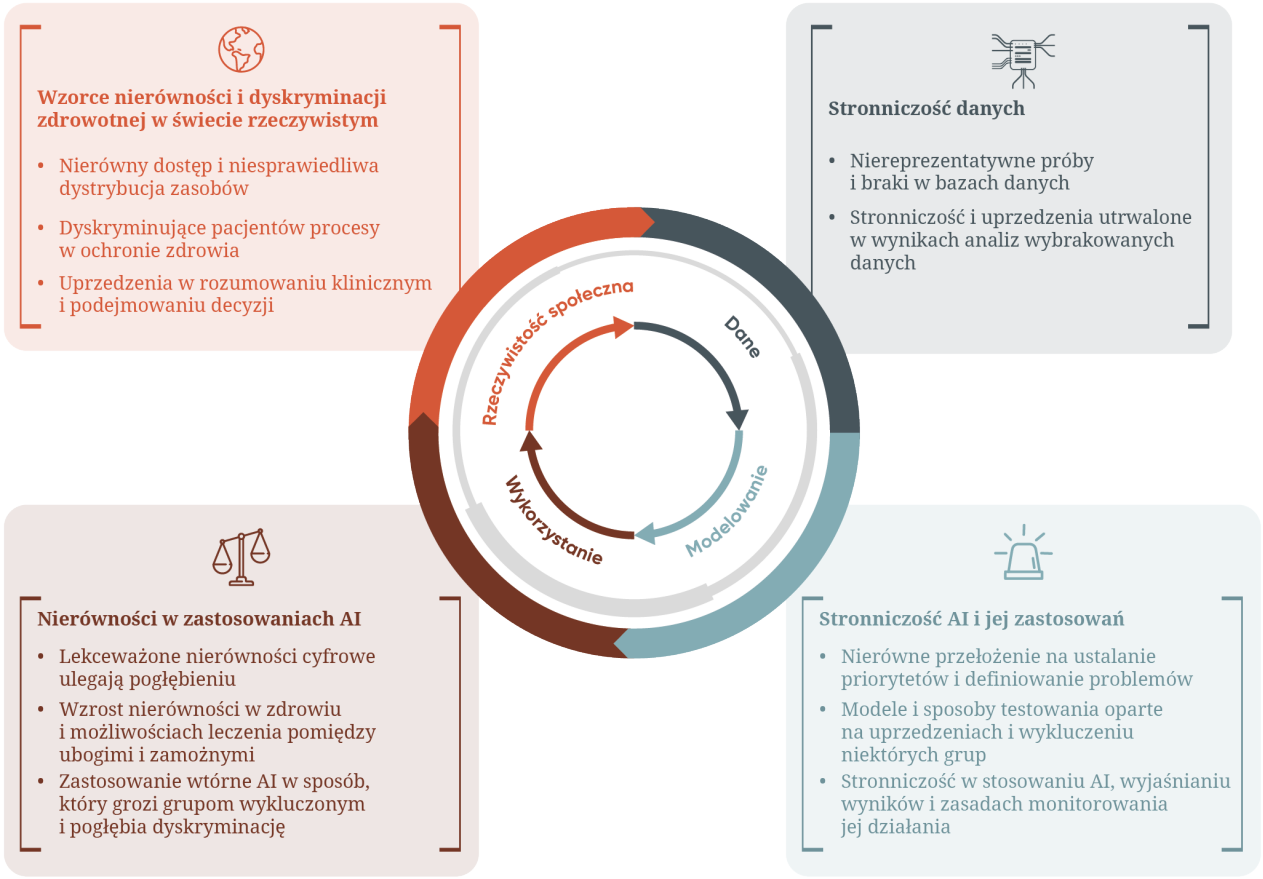
[231] Ibidem.

[232] I. Litchfield, D. Shukla, S. Greenfield, *Impact of COVID-19 on the digital divide: a rapid review*, „British Medical Journal Open" 2021;11:e053440.

[233] https://fra.europa.eu/en/publication/2022/bias-algorithm#publication-tab-0.

[234] M.A. Wójcik, *Algorithmic Discrimination in Health Care: An EU Law Perspective*, „Health and Human Rights Journal" 2022;24(1):93-103.

RYSUNEK 16. KASKADOWE EFEKTY NIERÓWNOŚCI I DYSKRYMINACJI W ZAKRESIE ZDROWIA UJAWNIAJĄ SIĘ W PROJEKTOWANIU I STOSOWANIU SYSTEMÓW SZTUCZNEJ INTELIGENCJI[235]



czająco dużym i zróżnicowanym zbiorze danych, mogłyby pomóc lekarzom w uzupełnieniu luk w wiedzy medycznej, zwłaszcza w zakresie schorzeń charakterystycznych dla mniejszości, grup zaniedbanych,

» możliwa jest korekta wyników dostosowania algorytmu do potrzeb konkretnych grup etnicznych lub rasowych,

» szerokie zastosowanie AI w opiece zdrowotnej w połączeniu z jej kompleksową regulacją na poziomie europejskim daje szansę na wzmocnienie ochrony antydyskryminacyjnej pacjentów.

„Cichym" fundamentem wiary w sprawiedliwość algorytmów są dwa przekonania:

» optymistyczne nastawienie do bezstronności algorytmów, które – w przeciwieństwie do człowieka – miałyby podejmować obiektywne decyzje

» założenie, że decyzje oderwane od ludzkich emocji, ram etycznych i kulturowych, będą same z siebie sprawiedliwe.

[235] D. Leslie et al., „British Medical Journal" 2021;372:n304.

Żadne po bliższym przyjrzeniu się nie wydaje się ani oczywiste, ani bezwarunkowo słuszne.

Dotychczasowe doświadczenia ze stosowaniem algorytmów do automatyzacji decyzji wskazują duży potencjał ich stronniczości i generowania różnie wyindukowanych uprzedzeń.[236] Dyskryminacja cyfrowa może być wynikiem sposobu, w jaki dany algorytm został zaprojektowany, ale również trenowania ich za pomocą stronniczych danych.[237] Problem dyskryminacji przez algorytmy jest szeroko badany w USA, gdzie np. banki wykorzystują systemy AI do określenia, kto kwalifikuje się do otrzymania kredytu hipotecznego lub studenckiego, a wynajmujący mieszkania używają AI do sprawdzania potencjalnych lokatorów. AI decyduje o tym, komu pomóc, a kogo ukarać lub odrzucić, na podstawie prognoz dotyczących tego, kto powinien trafić do aresztu tymczasowego, zostać przyjęty na studia lub zatrudniony. W tych przypadkach ludzie bywają traktowani niesprawiedliwie, nieetycznie lub po prostu inaczej na podstawie analizy ich danych osobowych.[238] Dzięki pracy algorytmów, w dzielnicach zamieszkanych przez ludzi o niskich dochodach oferowane są chwilówki, w marketingu internetowym kobiety są niedoszacowane o 21 proc., a reklamy internetowe sugerujące rejestry aresztowań pojawiają się częściej przy wyszukiwaniu nazwisk o „czarnym" brzmieniu niż nazwisk o „białym" brzmieniu.[239] Raport „Educational Redlining", przygotowany przez Student Borrower Protection Center, wykazał w 2020 r., że Upstart, szybko rozwijająca się platforma pożyczkowa AI, oferowała wyższe stopy procentowe i opłaty za pożyczki od pożyczkobiorców, którzy uczęszczali do historycznie „czarnego" Uniwersytetu Howarda lub w większości latynoskiego Uniwersytetu Stanowego w Nowym Meksyku, niż od tych, którzy studiowali na Uniwersytecie Nowojorskim, na którym czarnoskórzy i latynoscy studenci stanowią łącznie ok. 30 proc. populacji.[240]

Ponieważ coraz więcej zadań jest przekazywanych systemom autonomicznym, dyskryminacja cyfrowa staje się ogromnym problemem. Bardzo często powiela wzorce dyskryminacji zastane w świecie rzeczywistym, dziedzicząc uprzedzenia zawarte w zbiorach wcześniejszych decyzji lub po prostu odzwierciedlając powszechne w społeczeństwie stereotypy.[241] W skrajnych przypadkach zasto-

---

[236] N. Norori, Q. Hu, F. M., Aellen, F.D. Faraci, A. Tzovara, *Addressing bias in big data and AI for health care: A call for open science*. „Patterns" 2021;2(10), 100347.

[237] R. Schwartz, A. Vassilev, K. Greene, L. Perine, A. Burt, P.Hall, *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence, Special Publication (NIST SP)*, National Institute of Standards and Technology, Gaithersburg, MD 2022.

[238] https://gtr.ukri.org/projects?ref=EP%2FR033188%2F1.

[239] Ibidem.

[240] https://protectborrowers.org/wp-content/uploads/2020/02/Education-Redlining-Report.pdf.

[241] N. Criado, J.M. Such, *Digital Discrimination* w: *Algorithmic Regulation*, red. K. Yeung, M. Lodge, Oxford 2019.

sowanie AI może pogłębiać i utrwalać istniejące nierówności, doprowadzając do „perfekcji" niekorzystne traktowanie grup historycznie defaworyzowanych. Co więcej, decyzje algorytmów – właśnie dlatego, że otacza je nimb „nieludzkiej" obiektywności – stają się uzasadnieniem uprzedzeń żywionych przez ludzi. [242] Trenowane na obarczonych stereotypami zbiorach danych podają dyskryminacyjne rozwiązania, które stają się argumentem za utrzymaniem lub zaostrzeniem nierównego traktowania.

Także w zdrowiu, AI traktowana jak młot na uprzedzenia, może równie dobrze pogłębić istniejące podziały w świadczeniu opieki zdrowotnej. Sharona Hoffman i Andy Podgurski[243] wskazują, że podstawowym problemem jest jakość danych wejściowych. Niekompletność danych, ich selektywność i niedostateczna jakość nieuchronnie prowadzą do niezadowalających wyników pracy algorytmów. Grupy szczególnie narażone na wykluczenie są często znacznie niedoreprezentowane w bazach danych zdrowotnych, takich jak elektroniczna dokumentacja zdrowotna, ze względu na bariery językowe, ekonomiczne lub wykluczenie transportowe.[244] Gdy duże dane, na których szkolony jest algorytm, nie są reprezentatywne dla populacji pacjentów, AI wyciąga z nich czasem nietrafne wnioski, uznając brak danych za brak choroby. Przykładowo, algorytmy wdrażane w celu wykrywania chorób układu krążenia mogą osiągać gorsze wyniki w przypadku kobiet, ponieważ większość medycznych danych treningowych dotyczy mężczyzn.[245] Algorytmy trenowane do wykrywania raka skóry mogą podawać znacznie mniej precyzyjne wyniki w przypadku osób o ciemnej karnacji, gdyż trenowane były głównie na obrazach przedstawiających zmiany u białych pacjentów.[246]

Powszechne uprzedzenia wobec różnych grup, ukryte w bazach danych, mogą doprowadzić do utrwalenia zastanych wzorców dyskryminacji w algorytmie na zasadzie sprzężenia zwrotnego (*feedback-loop bias*).[247] Przykładowo, według Agencji Praw Podstawowych pracownicy służby zdrowia często podejrzewają imigrantów, osoby starsze i niepełnosprawne o wyolbrzymianie swoich problemów zdrowotnych w celu uzyskania świadczenia.[248] Problem ten jest szczególnie trudny do wykrycia, bo pozornie neutralne

---

[242] N. Criado, J.M. Such, *Digital Discrimination* w: *Algorithmic Regulation*, red. K. Yeung, M. Lodge, Oxford 2019.

[243] S. Hoffman, A. Podgurski, *Artificial intelligence and discrimination in health care*, „Yale Journal of Health Policy, Law, and Ethics" 2020;19(3):1–8.

[244] J.M. Johnson, T.M. Khoshgoftaar, *Survey on deep learning with class imbalance.* J. Big Data 2019; 6, 1–54.

[245] C. Niethammer, *AI bias could put women's lives at risk: A challenge for regulators*, „Forbes" 2020 March 2.

[246] D. Wen, S.M. Khan, A. Ji Xu, H. Ibrahim, L. Smith, J. Caballero, Zepeda L, de Blas Perez C, Denniston AK, Liu X, Matin RN. *Characteristics of publicly available skin cancer image datasets: a systematic review*, „Lancet Digit. Health" 2022 Jan;4(1):e64-e74.

[247] EU Agency for Fundamental Rights, *Bias in Algorithms. Artificial Intelligence and Discrimination*. Luxembourg: Publications Office of the European Union, Luksemburg 2022.

[248] EU Agency for Fundamental Rights, *Inequalities and multiple discrimination in access to and quality of healthcare*. Luxembourg: Publications Office of the European Union, Luksemburg 2013.

dane (takie jak miejsce zamieszkania) mogą maskować przesłanki dyskryminacji (takie jak rasa lub pochodzenie etniczne).[249] Algorytm wykorzystywany do identyfikacji pacjentów obarczonych ryzykiem niestawienia się na wizytę lekarską generował nadkomplet rezerwacji dla pacjentów ras innych niż biała, ponieważ wcześniejsze niestawienie się na wizytę było wskaźnikiem przynależności do określonej grupy socjoekonomicznej, skorelowanej z rasą.[250]

Dlatego opracowanie metod oceny, czy zbiory danych i algorytmy dyskryminują, czy nie, staje się palącą potrzebą. Prowadzone są badania nad tzw. sprawiedliwymi algorytmami, radzeniem sobie z tendencyjnymi danymi wejściowymi, ujawnianiem wyuczonych tendencji oraz mierzeniem względnego wpływu atrybutów danych, co pozwala określić ilościowo i ograniczyć zakres tendencyjności wprowadzanej przez algorytm lub zbiór danych. Pozostaje pytanie, jak skutecznie przełożyć te prawne, etyczne i społeczne oczekiwania na zautomatyzowane metody, które zweryfikują cyfrową dyskryminację w zbiorach danych i algorytmach. Próbują na nie odpowiedzieć inicjatywy takie jak Discovering and Attesting Digital Discrimination.[251]

W przypadku niektórych algorytmów uczenia maszynowego pojawia się dodatkowe zastrzeżenie: generowane przez nie dane wyjściowe nie są w pełni przewidywalne, a czasami nie można wyjaśnić, dlaczego i w jaki sposób algorytmy podjęły decyzję. Tego rodzaju wsparcie podejmowania decyzji w opiece zdrowotnej zyskało określenie „medycyna czarnej skrzynki".[252] Wydaje się ono szczególnym wyzwaniem, gdyż algorytmy, bazujące na nieznanych wcześniej korelacjach, są zdolne do dyskryminacji na nowe, abstrakcyjne sposoby, czyniąc cechy prawnie chronione mało użytecznymi.[253] Dyrektywy antydyskryminacyjne mają małe szanse na rozwiązanie tego problemu, ponieważ zostały zaprojektowane z myślą o ludzkim sprawcy: jako ludzie używamy zdrowego rozsądku, by rozpoznać dyskryminacyjne wzorce w zachowaniu innych.[254] Dlatego w prawie dyskryminacja i sprawiedliwość są pojęciami „kontekstowymi", a ich ustaleniem kieruje logika sądowa; niestety, te same narzędzia nie są równie skuteczne wobec dyskryminacji algorytmicznej.[255]

---

[249] M.A. Wójcik, op.cit.

[250] M. Samorani, L.G. Blount, *Machine learning and medical appointment scheduling: creating and perpetuating inequalities in access to health care*, „American Journal of Public Health" 2020;110(4):440.

[251] Ibidem.

[252] W.N. Price II, *Artificial intelligence in health care: Applications and legal implications*, „SciTech Lawyer" 2017;14:10.

[253] M.A. Wójcik, op.cit.

[254] Ibidem.

[255] Ibidem.

Specyficzny charakter stronniczości algorytmicznej utrudnia ustalenie, że istnieje dyskryminacja: w rzeczywistości jest bardzo możliwe, że ofiary algorytmicznej stronniczości nigdy nie dowiedzą się, że były dyskryminowane.[256] Co więcej, pacjenci pochodzący z grup szczególnie narażonych na dyskryminację często powstrzymują się od jej zgłaszania właśnie dlatego, że trudno ją udowodnić.[257] Problem dyskryminacji pośredniej wymyka się ramom prawnym, opartym na konkretnych cechach prawnie chronionych, a nasila się w przypadku opieki zdrowotnej, gdzie chronione cechy są ograniczone do trzech: rasy, pochodzenia etnicznego i płci.[258]

Dyskryminacja algorytmiczna, trudna do identyfikacji i interpretacji, może stawiać pod znakiem zapytania użyteczność AI w polityce społecznej.[259] W przypadku opieki zdrowotnej stawka jest szczególnie wysoka, gdyż dotyczy zdrowia i życia.[260] Szerokie zastosowanie AI w opiece medycznej i kształtowaniu polityki zdrowotnej sprawi, że sprawiedliwa alokacja środków na opiekę medyczną zależeć będzie od dostępności danych odzwierciedlających potrzeby medyczne wszystkich populacji, także tych narażonych na wykluczenie.[261]

Zapobieganie zautomatyzowanej dyskryminacji wymaga wypracowania nowych narzędzi i ram prawnych, ale także świadomości społecznej i nowego cyfrowego społeczeństwa obywatelskiego.[262] Z jednej strony mamy próby zaproponowania standardu technicznego w rozwoju AI, który pozwoli twórcom technologii na wczesne wykrywanie zautomatyzowanej dyskryminacji, z drugiej – prawnicy wskazują kierunek rozwoju doktryny, która złagodzi związek między tożsamością ofiary a chronionymi cechami, pozwoli na szersze rozpoznanie bezpośredniej dyskryminacji bez dowodu rzeczywistej szkody dla konkretnych ofiar, gdy grupy chronione są bezpośrednio celem działań dyskryminujących.[263] Takie zmiany zmniejszą trudność dochodzenia swoich praw przez pacjentów i wprowadzą elastyczność do sztywnych ram cech prawnie chronionych.[264]

---

[256] Ibidem.

[257] S. Wachter, B. Mittelstadt, C. Russell, *Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI*, „Computer Law and Security Review" 2021;41:11.

[258] M.A. Wójcik, op.cit.

[259] B. Mittelstadt, *From individual to group privacy in big data analytics*. „Philos Technol" 2017; 30:475–494.

[260] M.A. Wójcik, op.cit.

[261] Z. Obermeyer, B. Powers, C. Vogeli, S. Mullainathan, *Dissecting racial bias in an algorithm used to manage the health of populations*. „Science" 2019; 366:447–453

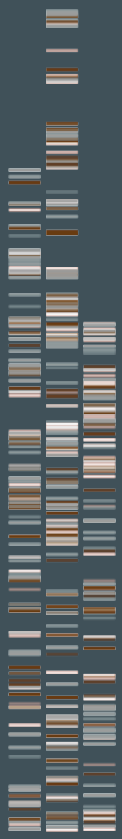
[262] C. O'Neil, *Weapons of math destruction. How big data increases inequality and threatens democracy*, Crown, New York 2016.

[263] M.A. Wójcik, op.cit.

[264] R. Xenidis, *Tuning EU equality law to algorithmic discrimination: Three pathways to resilience*, „Maastricht Journal of European and Comparative Law" 2020;27(6):736–739–741.

Podsumowanie

- *Dyskryminacja cyfrowa obejmuje nie tylko nierówny dostęp do łączy szerokopasmowych, ale także nierówne możliwości faktycznego korzystania z tych łączy, jak również dostępność urządzeń pozwalających na swobodne korzystanie z narzędzi cyfrowych dla wszystkich pacjentów.*
- *Dyskryminacja cyfrowa może wystąpić bez względu na to, czy w grę wchodzą intencje dyskryminacyjne.*
- *Zwalczanie dyskryminacji cyfrowej wymaga większej przejrzystości istniejących baz danych, gromadzenia dodatkowych danych oraz ich monitorowania.*
- *Obywatele powinni mieć możliwość dochodzenia swoich praw w ramach przejrzystych procedur antydyskryminacyjnych, uwzględniających cyfrowe uwarunkowania zdrowia.*
- *Potrzebne jest wypracowanie standardów technicznego rozwoju AI, z równoczesnym dostosowaniem ram prawnych do nowych, „nie-ludzkich" wzorców dyskryminacji generowanych przez algorytmy.*



SEBASTIAN SIKORSKI

Profesor Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie, doktor habilitowany nauk prawnych, Wydział Prawa i Administracji, Instytut Nauk Prawnych, Katedra Prawa Administracyjnego i Samorządu Terytorialnego; adwokat specjalizujący się w obszarze prawa medycznego i administracyjnego

MICHAŁ FLORCZAK

Doktor nauk medycznych, specjalista chorób wewnętrznych, specjalista medycyny ratunkowej, dyrektor medyczny Jutro Medical. Starszy asystent w Klinice Immunologii, Transplantologii i Chorób Wewnętrznych Warszawskiego Uniwersytetu Medycznego

08

Sztuczna inteligencja w ochronie zdrowia oraz standardy telemedyczne – zagadnienia wybrane

Wprowadzenie

Rozwiązania z obszaru szeroko rozumianej sztucznej inteligencji (ang. *artificial intelligence* – AI) stanowią szybko rozwijającą się grupę technologii, mogących przynosić wiele korzyści społeczno-ekonomicznych w praktycznie wszystkich branżach i obszarach działalności społecznej. Rozwiązania tego typu umożliwiają lepsze prognozowanie, optymalizację operacji, przydzielanie zasobów oraz personalizację świadczonych usług, dając w ten sposób przedsiębiorstwom – a w skali makro całej europejskiej gospodarce – zasadniczą przewagę konkurencyjną. Obszar ochrony zdrowia stanowi szczególny przykład, w którym tego typu rozwiązania mogą być wdrażane. Z perspektywy praw pacjenta niezwykle istotne jest, aby systemy oparte na AI gwarantowały prawo do informacji oraz respektowały wolę pacjenta w zakresie dostępu do informacji – bądź jego braku – z wyłączeniem sytuacji, gdy brak informacji mógłby wywołać poważne ryzyko dla zdrowia innych osób. W przypadku każdego systemu AI (nie dotyczy to tylko ochrony zdrowia) ważne jest także, aby jego użytkownicy mieli możliwość potwierdzenia, że mają do czynienia z takim właśnie systemem.[265] AI to nie tylko jednak szanse, ale i zagrożenia. Warto w tym miejscu zacytować Stephena Hawkinga, który wskazywał, że pojawienie się sztucznej inteligencji może być „najgorszym wydarzeniem w historii naszej cywilizacji", chyba że społeczeństwo znajdzie sposób na kontrolowanie jej rozwoju.[266]

W literaturze szczególnie podkreślane są zagadnienia dotyczące wykorzystania algorytmów głębokiego uczenia opartych na sieciach neuronowych.[267] Początkowo algorytmy AI najczęściej były wykorzystywane w radiologii do diagnostyki obrazowej, gdzie wykazały niezwykły postęp w zadaniach rozpoznawania obrazów.[268] Obecnie coraz częściej dyskusja toczy się nad wykorzystaniem AI do konsultacji pacjentów, kiedy wyzwaniem staje się wsparcie lekarzy w analizowaniu objawów chorobowych i wyników badań dodatkowych podczas konsultacji (diagnostyka różnicowa). Na rynku jest już kilka narzędzi, które mogą temu służyć. Przykładowo Infermedica, która ułatwia wstępną diagnostykę medyczną oraz kierowanie ruchem pacjentów,[269] natomiast algorytmy te nie uwzględniają

[265] M. Świerczyński, Z. Więckowski, *Prawo do zdrowia a sztuczna inteligencja w systemie ochronnym tworzonym przez organizacje międzynarodowe* w: Internet. Cyberpandemia. Cyberpandemic, red. A. Gryszczyńska, G. Szpor, Warszawa 2020.

[266] *Stephen Hawking ostrzegał świat przed sztuczną inteligencją*, businessinsider.com.pl (dostęp: 23.03.2023).

[267] K. Niewęgłowski, N. Wilczek et al., *Applications of Artificial Intelligence (AI) in medicine*, „Medycyna Ogólna i Nauki o Zdrowiu", vol. 27 (3) 2021, s. 213–219, https://doi.org/10.26444/monz/142085.

[268] A. Hosny, C. Parmar, J. Quackenbush et al., *Artificial intelligence in radiology*, „Nature Reviews Cancer" 2018, vol. 18, s. 500–510, https://doi.org/10.1038/s41568-018-0016-5.

[269] https://infermedica.com/.

jeszcze analizy stwierdzanych odchyleń w badaniu przedmiotowym i wyników badań dodatkowych. Za przykład innego zastosowania służy Glass Digital Notebook, który może istotnie pomóc lekarzom w diagnostyce różnicowej i ustalaniu planu leczenia.[270]

Szeroko ujmowany rozwój usług i produktów opartych na AI lub ją wykorzystujących pociąga za sobą konieczność przygotowania stosownej regulacji prawnej.[271] Od kilku lat obserwujemy na poziomie Unii Europejskiej wzmożoną aktywność w tym zakresie, która stara się utrzymać wiodącą pozycję w sferze technologii, dbając przy tym, aby nowe technologie funkcjonowały w poszanowaniu unijnych zasad i wartości, ze szczególnym uwzględnieniem praw podstawowych. W doktrynie podkreślany jest dotychczasowy unijny dorobek w obszarze AI na etapie prac koncepcyjnych.[272] Punktem odniesienia dla rozważań zawartych w tym rozdziale będzie projekt rozporządzenia z 21 kwietnia 2021 r. Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze Unii[273] (dalej: projekt).[274] To właśnie przez pryzmat tego projektu wskazane zostaną kluczowe zagadnienia dotyczące regulacji AI z odniesieniem do ochrony zdrowia. Zawężenie perspektywy do jednego sektora jest uzasadnione nie tylko ze względu na temat całości pracy, ale też konieczność wskazania szans i zagrożeń z perspektywy osób posługujących się tego typu rozwiązaniami, a w konsekwencji także bezpieczeństwem pacjentów.

Ze względu jednak na wyznaczone ramy możliwe będzie jedynie zasygnalizowanie wybranych aspektów tej regulacji, co zostało zaznaczone w tytule niniejszego rozdziału.

Kolejnym zagadnieniem, będącym przedmiotem rozważań, są regulacje dotyczące standardów telemedycznych, które mają zasadnicze znaczenie dla zapewnienia bezpieczeństwa i ochrony pacjentów, a także personelu medycznego. Pierwsze standardy zostały już wyznaczone w ramach rozporządzeń wykonawczych wydanych przez ministra zdrowia w oparciu o delegację ustawową zawartą

---

[270] https://glass.health/.

[271] Zob.: *Administracja w demokratycznym państwie prawa. Księga jubileuszowa Profesora Czesława Martysza*, red. A. Matan, WKP 2022.

[272] M. Świerczyński, Z. Więckowski, *Prawo do zdrowia a sztuczna inteligencja w systemie ochronnym tworzonym przez organizacje międzynarodowe…*, s. 313; zob.: też J. Mazur, *Unia Europejska wobec rozwoju sztucznej inteligencji: proponowane strategie regulacyjne a budowanie jednolitego rynku cyfrowego*, „Europejski Przegląd Sądowy" nr 9 2020, s. 13–18.

[273] Projekt rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze Unii (COM(2021) 206 final – 2021/106 (COD)).

[274] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52021PC0206.

na gruncie ustawy z 15 kwietnia 2011 r. o działalności leczniczej[275] (dalej: u.d.l.). W ramach prowadzonej analizy wskazane zostaną te rozwiązania, które mają najistotniejsze znaczenie dla udzielania świadczeń w opiece ambulatoryjnej.

Rozwiązania z obszaru sztucznej inteligencji

Przyjęcie regulacji prawnej dotyczącej sztucznej inteligencji na poziomie prawa europejskiego, w drodze automatycznie wchodzącego w życie rozporządzenia, znajduje swoją podstawę przede wszystkim w przepisie art. 114 Traktatu o funkcjonowaniu Unii Europejskiej (dalej TFUE),[276] w którym przewidziano przyjęcie środków mających na celu zapewnienie ustanowienia i funkcjonowania rynku wewnętrznego. Rozporządzenie jest aktem, który zgodnie z art. 288 TFUE ma bezpośrednie zastosowanie. Szczególnego podkreślenia wymaga *ratio legis* przyjęcia rozwiązań prawnych w zakresie AI właśnie na poziomie prawa europejskiego. Niektóre państwa członkowskie UE rozważają już bowiem wprowadzenie przepisów w tym zakresie na poziomie krajowym, co grozi uniemożliwieniem swobodnego obrotu towarami i usługami z zastosowaniem technologii AI oraz spowodowaniem fragmentaryzacji wspólnego rynku. Ramy regulacyjne na poziomie UE z jednej strony mogą więc zapewnić równe warunki działania i ochrony obywateli, z drugiej zaś wzmocnić konkurencyjność przemysłową Europy w tym obszarze, zwiększając siłę oddziaływania na kształtowanie regulacji dotyczących AI na poziomie globalnym.[277]

Na wstępie oceny tego projektu należy zgodzić się ze stanowiskiem, że brakuje w nim jednoznacznego określenia jego stosunku do innych aktów prawnych. Zasadnicze znaczenie ma bowiem doprecyzowanie projektu w taki sposób, aby z jednej strony uzupełniał istniejące, z drugiej zaś nie wyłączał bądź nie powtarzał treści zarówno obowiązujących, jak i równolegle projektowanych regulacji.[278]

Zasadnicze znaczenie ma samo zdefiniowanie sztucznej inteligencji. Zgodnie z przepisem art. 3 ust. 1 projektu: »system sztucznej inteligencji« oznacza oprogramowanie opracowane przy użyciu co

---

[275] DzU z 2022 r., poz. 633 ze zm.

[276] Traktat o funkcjonowaniu Unii Europejskiej, Dz.Urz. UE C 202 z 2016 r., s. 47.

[277] K. Rębisz, *Wybrane zagadnienia prawa cywilnego w propozycjach regulacyjnych dotyczących sztucznej inteligencji w Unii Europejskiej*, „Europejski Przegląd Sądowy", nr 10/2021, s. 22–27.

[278] R. Bieda, P. Budrewicz, D. Lubasz, M. Namysłowska, M. Nowakowski, R. Pająk, D. Szostek, M. Świerczyński, Z. Więckowski, I. Wochlik, M. Wróblewski, *Analiza wybranych aspektów projektu aktu w sprawie sztucznej inteligencji*, 13.12.2021 r., AI Law Tech, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiuqcaEqdj9AhVmlosKHdJ9CVIQFnoECA4QAQ&url=https%3A%2F%2Fwww.gov.pl%2Fattachment%2Ffa12287b-09c6-47d1-b0d6-7286c53d6917&usg=AOvVaw3Hivqy-3H4ZbOYt-oTUKFP (dostęp: 13.03.2023), s. 8.

najmniej jednej spośród technik i podejść wymienionych w załączniku I, które może – dla danego zestawu celów określonych przez człowieka – generować wyniki, takie jak treści, przewidywania, zalecenia lub decyzje wpływające na środowiska, z którymi wchodzi w interakcję". Immanentnym elementem definicji jest więc brzmienie załącznika I, zgodnie z którym do „technik i podejść" należy zaliczyć: „a) mechanizmy uczenia maszynowego, w tym uczenie nadzorowane, uczenie się maszyn bez nadzoru i uczenie przez wzmacnianie, z wykorzystaniem szerokiej gamy metod, w tym uczenia głębokiego; b) metody oparte na logice i wiedzy, w tym reprezentacja wiedzy, indukcyjne programowanie (logiczne), bazy wiedzy, silniki inferencyjne i dedukcyjne, rozumowanie (symboliczne) i systemy ekspertowe; c) podejścia statystyczne, estymacja bayesowska, metody wyszukiwania i optymalizacji".[279] Takie zdefiniowanie ma kilka konsekwencji. Przede wszystkim definicja obejmuje również uczenie maszynowe, z rozróżnieniem na uczenie nadzorowane, bez nadzoru oraz uczenie z wykorzystaniem szerokiej gamy metod, w tym uczenia głębokiego. Biorąc pod uwagę stan rozwoju rozwiązań obecnie funkcjonujących w sektorze ochrony zdrowia, takie szerokie ujęcie można ocenić pozytywnie. Zapewne wraz z rozwojem technologii definicja ta będzie ulegać modyfikacjom. Ma ona jednak pewne mankamenty. Wskazanie bowiem, że jej zakresem objęte są również „metody oparte na logice i wiedzy" powoduje, że do tego typu rozwiązań można zaliczyć znaczną ilość wykorzystywanego już oprogramowania.[280] Wydaje się, że nie taki był cel projektodawcy. Jednocześnie już w samej definicji dokonano zróżnicowania na uczenie maszynowe nadzorowane i niewymagające nadzoru. Mimo że kwestia nadzoru jest przedmiotem odrębnej regulacji, zawartej w art. 14 projektu, warto zaznaczyć, że zasadne byłoby podkreślenie sprawowania ostatecznego nadzoru przez człowieka przy każdym rozwiązaniu kwalifikowanym do AI. Na ten aspekt, jako kluczowy, wskazuje też Europejski Komitet Ekonomiczno-Społeczny, podkreślając konieczność zachowania niektórych decyzji wyłącznie w gestii człowieka, w szczególności gdy „obejmują aspekt moralny i konsekwencje prawne lub wpływ na społeczeństwo", w takich dziedzinach jak opieka zdrowotna.[281]

---

[279] Niestety, definicja AI zastosowana w projekcie jest bardzo szeroka. Obejmuje nie tylko oprogramowanie oparte na mechanizmach uczenia maszynowego, lecz także np. bazy wiedzy oraz metody wyszukiwania, które same w sobie nie muszą mieć nic wspólnego ze sztuczną inteligencją. Projektowana definicja AI, przez uwzględnienie w niej technik i podejść określonych w załączniku I do projektu, ma być z założenia okresowo aktualizowana. M. Kupis, Stosowanie przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/745 do sztucznej inteligencji, „Przegląd Prawa Medycznego" nr 1 (9)/2022, s. 101.

[280] Tak też: M. Kupis, *Stosowanie przepisów*..., op.cit., s. 102.

[281] Opinia Europejskiego Komitetu Ekonomiczno-Społecznego Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze Unii (2021/C 517/09).

W doktrynie opisywany jest podział na wąskie systemy AI, czyli takie, które mogą wykonać jedno lub kilka określonych zadań, oraz ogólną AI ujmowaną jako superinteligencja czy samoświadoma AI. Na obecnym poziomie rozwoju techniki mamy do czynienia z rozwiązaniami w ujęciu wąskim AI. Jednak trudno zgodzić się z twierdzeniem, że świadoma AI pozostaje na razie jedynie pewną hipotezą, a nawet być może taka silna AI nigdy nie powstanie.[282] Na zasadzie sformułowania hipotezy, którą zweryfikuje dopiero przyszłość – być może odległa – należy przyjąć, że nie jest kwestią, czy takie rozwiązania będą możliwe, ale raczej kiedy się pojawią, bo wówczas prawo będzie musiało im sprostać. Trudne byłoby zapewne projektowanie regulacji prawnej z takim wyprzedzeniem, jednak już teraz zasadne wydaje się podkreślanie konieczności pozostawienia zawsze ostatecznej decyzji w rękach człowieka.

Już na tym etapie rozwoju AI należy podkreślić, że tego typu rozwiązania powinny pełnić jedynie rolę wspierającą lekarza w procesie diagnozowania i leczenia pacjenta. Nie powinno się natomiast dążyć do zastąpienia konsultacji lekarskich wyłącznie AI. Nawet platformy AI bardzo często zalecają[283] właśnie konsultację lekarską po analizie objawów pacjenta. Można tutaj wskazać tzw. narzędzie ChatGPT, którego algorytmy pozwoliły nawet na zdanie egzaminu lekarskiego (Medical Board Exam) z wynikiem 60 proc.[284] Badacze z Massachusetts General Hospital i AnsibleHealth uważają, że w przyszłości ChatGPT i inne generatywne modele konwersacyjne mogą pomóc w szkoleniu przyszłych lekarzy, a z kolei zastosowania takie jak tłumaczenie technicznych wyników medycznych na język bardziej zrozumiały dla pacjentów za pomocą ChatGPT – to projekt, który AnsibleHealth już realizuje.[285]

Rozwiązania z zakresu AI w ochronie zdrowia są faktem i należy przyjąć, że skala ich zastosowania, a także zaawansowanie będzie się sukcesywnie zwiększać. Dlatego warto na rozwiązania tego typu patrzeć z wielu perspektyw. Z jednej strony personel medyczny – szczególnie lekarze – dzięki wykorzystaniu tych narzędzi będzie mógł szybciej i skuteczniej rozpoznawać choroby przewlekłe na wczesnym etapie oraz ich zaostrzenia. Przykładem może być reumatologia. Skąpość objawów, nietypowy i podobny kliniczny przebieg takich chorób jak

---

[282] *Sto lat polskiego prawa handlowego. Księga jubileuszowa dedykowana Profesorowi Andrzejowi Kidybie*, t. 2, red. M. Dumkiewicz, K. Kopaczyńska-Pieczniak, J. Szczotka, WKP 2020; zob.: N. Bostrom, *Superintelligence. Paths, dangers, strategies,* Oxford 2014, ale por. także: M. Tegmark, Life 3.0, London 2021.

[283] Zalecenie to na tym etapie nie ma charakteru autonomicznego, lecz wynika z zastosowania określonego filtra.

[284] *ChatGPT Passes Medical Board Exam*, https://aibusiness.com/verticals/chatgpt-passes-medical-board-exam (dostęp: 13.03.2023).

[285] *AI Bot ChatGPT Passes US Medical Licensing Exams Without Cramming – Unlike Students*, https://www.medscape.com/viewarticle/987549 (dostęp: 13.03.2023).

toczeń rumieniowaty układowy czy reumatoidalne zapalenie stawów nie pozwala na szybkie rozpoznanie. Być może w przyszłości wykorzystanie do tego celu algorytmów AI zapewni wcześniejsze postawienie rozpoznania, lepszą analizę rokowania i wcześniejsze rozpoczynanie np. celowanego leczenia biologicznego.[286] W wymienionych przypadkach mówi się już nawet o tzw. medycynie precyzyjnej.[287] Z drugiej jednak strony porusza się istotny argument przeciwko szerszemu wykorzystaniu AI w medycynie. Badacze obawiają się, że wartość badań przeprowadzanych w oparciu o algorytmy nie uwzględniałaby złożoności całego organizmu ludzkiego ani kwestii psychologicznych, niezwykle ważnych w relacji lekarz – pacjent.[288] Należy jednak przyjąć, że procesu rozwoju tej technologii i jej zastosowania w medycynie po prostu nie można zatrzymać. W konsekwencji trzeba wydobywać to, co jest pozytywne w tych rozwiązaniach, i starać się przewidywać oraz eliminować zagrożenia.

Zgodnie z przepisem art. 6 projektu określone zostały zasady klasyfikacji systemów sztucznej inteligencji wysokiego ryzyka. Podkreślono jednocześnie powiązanie rozwiązań z obszaru AI z odrębnymi produktami wskazanymi w tym przepisie. Na tym tle szczególne znaczenie ma rozróżnienie systemów wysokiego ryzyka i zaklasyfikowanie technologii AI używanej w sektorze ochrony zdrowia do owej grupy. W tym bowiem przypadku chronione są najwyższe wartości, jak zdrowie i życie człowieka, co podkreślają też projektodawcy. W motywie 28 wskazują bowiem, że systemy sztucznej inteligencji mogą przynosić szkodliwe skutki dla zdrowia i bezpieczeństwa ludzi, odnosząc te zagrożenia m.in. właśnie do sektora ochrony zdrowia, „w którym chodzi o szczególnie wysoką stawkę, jaką jest życie i zdrowie, coraz bardziej zaawansowane systemy diagnostyczne i systemy wspomagające decyzje podejmowane przez człowieka powinny być niezawodne i dokładne".

Należy zwrócić uwagę również na określoną w art. 12 projektu konieczność rejestracji zdarzeń w przypadku systemów wysokiego ryzyka – z uwzględnieniem uznanych norm lub wspólnych specyfikacji. Funkcja rejestracji zdarzeń[289] w założeniu musi także zapewniać monitorowanie działania systemu sztucznej

---

[286] A. Manrique de Lara, I. Peláez-Ballestas, *Big data and data processing in rheumatology: bioethical perspectives*, „Clinical Rheumatology" 2020, vol. 39, s. 1007–1014, https://doi.org/10.1007/s10067-020-04969-w.

[287] J.M. Guthridge, C.A. Wagner, J.A. James, *The promise of precision medicine in rheumatology*, „Nature Medicine" 2022, vol. 28 (7), s. 1363–1371, https://doi.org/10.1038/s41591-022-01880-6.

[288] J.E.H. Korteling, G.C. van de Boer-Visschedijk, R.A.M. Blankendaal, R.C. Boonekamp, A.R. Eikelboom, *Human – versus Artificial Intelligence,* „Frontiers in Artificial Intelligence" 2021, vol. 4, https://doi.org/10.3389/frai.2021.622364.

[289] Autorzy tego rozdziału postulowali już w 2019 r. konieczność stworzenia rejestru publicznego działających w ochronie zdrowia rozwiązań z obszaru AI – szerzej: S. Sikorski, M. Florczak, *Sztuczna inteligencja w medycynie – nowe wyzwanie w obszarze regulacji administracyjnoprawnej* w: *Innowacje w ochronie zdrowia. Aspekty prawne, ekonomiczne i organizacyjne*, red. I. Lipowicz, E. Nojszewska, S. Sikorski, Wolters Kluwer, Warszawa 2020, s. 143–158.

inteligencji wysokiego ryzyka pod kątem występowania sytuacji, które mogą skutkować tym, że system sztucznej inteligencji będzie stwarzał ryzyko w rozumieniu art. 3 pkt 19 rozporządzenia (UE) 2019/1020. W tym miejscu pojawia się pewne zastrzeżenie, ponieważ definicja zawarta w tym przepisie odnosi się do „produktu stwarzającego ryzyko" oznaczające potencjalnie niekorzystny wpływ m.in. właśnie na zdrowie.

Projekt odnosi się również w przepisie art. 13 do przejrzystości i udostępniania informacji użytkownikom. Przejrzystość rozumiana jest jako umożliwiająca użytkownikom interpretację wyników działania systemu, co wiąże się z określonymi obowiązkami użytkownika i dostawcy. Szczególnie podkreślono tutaj wymóg dołączania do systemów sztucznej inteligencji wysokiego ryzyka instrukcji obsługi zawierającej „zwięzłe, kompletne, poprawne i jasne informacje, które są istotne, dostępne i zrozumiałe dla użytkowników". Nasuwa się wątpliwość, na ile założenie to w praktyce będzie realizowane, biorąc pod uwagę złożoność rozwiązań z obszaru AI, co będzie miało także znaczenie dla zakresu odpowiedzialności.

W kontekście przywołanych uwag – konieczności kontroli przez człowieka rozwiązań AI – specjalnego znaczenia nabierają zasady nadzoru. W motywie 48 projektu bardzo wyraźnie została podkreślona konieczność projektowania i opracowywania rozwiązań AI wysokiego ryzyka w taki sposób, aby człowiek mógł efektywnie nadzorować ich funkcjonowanie. Dlatego jeszcze przed wprowadzeniem tych rozwiązań do obrotu lub ich oddaniem do użytku dostawca powinien wskazać odpowiednie środki w tym zakresie. W szczególności chodzi o rozwiązania polegające na „wbudowanych ograniczeniach operacyjnych", których AI nie jest w stanie sama obejść i musi reagować na działania człowieka – operatora systemu. Konsekwencją tak ujętego nadzoru jest brzmienie przepisu art. 14 projektu. Wyjątkowo mocno podkreślone tutaj zostały systemy sztucznej inteligencji wysokiego ryzyka, w przypadku których projekt i opracowanie muszą uwzględniać odpowiednie narzędzia „interfejsu człowiek – maszyna", które zapewniają efektywny nadzór. Nadzór ten wiąże się z zapobieganiem ryzyku dla zdrowia, bezpieczeństwa i praw podstawowych lub minimalizowaniem takiego ryzyka, przy założeniu wykorzystania systemu sztucznej inteligencji wysokiego ryzyka zgodnie z jego przeznaczeniem lub – co szczególnie istotne – w warunkach dającego się racjonalnie przewidzieć niewłaściwego wykorzystania. Z jednej strony, nadzór realizowany jest za pomocą wspomnianych wcześniej zaprojektowanych i opracowanych rozwiązań, czyli jeszcze przed wprowadzeniem systemu do obrotu lub oddaniem go do użytku. Z drugiej strony,

w ramach nadzoru zapewniony ma być odpowiedni zakres informacji dla osób realizujących ów nadzór, które pozwolą na rozumienie pełni możliwości i ograniczeń nadzorowanego systemu sztucznej inteligencji wysokiego ryzyka i wychwytywanie oznak anomalii, nieprawidłowego funkcjonowania czy nieoczekiwanych wyników działania, tak szybko, jak to tylko w danych okolicznościach możliwe. Osoby nadzorujące powinny krytycznie odnosić się do nadmiernego polegania na wyniku działania systemu sztucznej inteligencji wysokiego ryzyka (tzw. *automation bias*) i prawidłowo interpretować wyniki jego działania.

Kluczowe w tej regulacji jest określenie zasad odpowiedzialności. Zgodnie z motywem 53 projektu, odpowiedzialność za wprowadzenie do obrotu lub oddanie do użytku systemu sztucznej inteligencji wysokiego ryzyka ponosi nie tylko osoba, która zaprojektowała lub opracowała ten system, ale również dostawca. Według art. 24 projektu w przypadku systemów sztucznej inteligencji wysokiego ryzyka, które są powiązane z produktami,[290] odpowiedzialność ponosi bowiem producent podlegający obowiązkom analogicznym, jakie nałożono na dostawcę. Z kolei importerzy, zgodnie z art. 26 projektu, w przypadku tych systemów zapewniają warunki przechowywania lub transportu niezagrażające ich zgodności z określonymi wymogami. Zakres odpowiedzialności dystrybutorów został wskazany w art. 27 projektu, według którego w przypadku AI wysokiego ryzyka to dystrybutor ponosi odpowiedzialność przede wszystkim za oznakowanie zgodności CE, ale też za to, aby warunki przechowywania i transportu nie zagrażały zgodności systemu z wymogami określonymi w projekcie. Jeśli chodzi o rozwiązania z obszaru AI dotyczące ochrony zdrowia, właśnie ten aspekt zaostrzający odpowiedzialność jest szczególnie istotny, ze względu na przedmiot ochrony, tj. życie i zdrowie ludzkie.

Bardzo istotnym rozwiązaniem dla rozwoju AI jest przyjęcie tzw. piaskownic regulacyjnych (art. 53 projektu), przez które należy rozumieć utworzone przez państwo lub grupę państw członkowskich „kontrolowane środowisko ułatwiające opracowywanie, testowanie i walidację innowacyjnych systemów sztucznej inteligencji przez ograniczony czas przed ich wprowadzeniem do obrotu lub oddaniem do użytku". Na tym etapie właśnie uczestnicy tych „piaskownic regulacyjnych" ponoszą odpowiedzialność za wszelkie szkody wyrządzone w wyniku prowadzonych eksperymentów. Mamy tutaj więc kontrolowane – dzięki określeniu zasad, w tym zasad odpowiedzialności – środowisko, w któ-

[290] Do których zastosowanie mają akty prawne wymienione w załączniku II, sekcja A.

rych rozwiązania z zakresu AI mogą być bezpiecznie testowane.

Do czasu uchwalenia i wejścia w życie omawianego projektu obowiązują w polskim systemie prawnym ogólne zasady odpowiedzialności cywilnej deliktowej, a w pewnych warunkach kontraktowej, w przypadku wyrządzenia szkody w wyniku posłużenia się rozwiązaniami z obszaru AI. Zgodnie z tym, co zostało już powiedziane, oczekiwanie polskiego ustawodawcy na rozwiązania prawne na poziomie UE są racjonalnym, wręcz koniecznym wyborem. Pozostaje tylko mieć nadzieję, że regulacje w zakresie AI – w szczególności analizowany projekt – szybko wejdą w życie.

Standardy w telemedycynie

W Polsce swoistym katalizatorem rozwoju telemedycyny okazała się epidemia COVID-19.[291] Oprócz podstaw prawnych, podanych przede wszystkim w ustawie o działalności leczniczej oraz ustawach regulujących poszczególne zawody medyczne (chociaż tutaj niestety ustawodawca jest niekonsekwentny w sposobie regulacji), konieczne okazuje się określenie standardów udzielania świadczeń w ramach telemedycyny. Jest to niezbędne do zapewnienia bezpieczeństwa i ochrony pacjentów, ale również personelu medycznego. Szczególnie duże znaczenie mają standardy udzielania świadczeń z wykorzystaniem telemedycyny w opiece ambulatoryjnej, tj. podstawowej opiece zdrowotnej i opiece specjalistycznej.

Standardy udzielania świadczeń zdrowotnych powinny uwzględniać możliwość zlecania pacjentowi dodatkowych badań i podstawowych badań obrazowych, ale też informowania pacjenta o ich wynikach. Ponadto powinny zawierać zasady przeprowadzenia badania kontrolnego pacjenta po udzieleniu porady telemedycznej, z zastrzeżeniem, że badanie to może się odbywać również w ramach telekonsultacji.

Minister zdrowia w porozumieniu z ministrem właściwym do spraw informatyzacji został przez ustawodawcę

---

[291] Zob.: S. Sikorski, M. Florczak, *Telemedycyna pomaga w walce z pandemią*, „Gazeta Prawna" z 19.03.2020 r.

Potencjał rozwiązań z obszaru telemedycyny był również przedmiotem analizy i rekomendacji w projekcie zrealizowanym przez autorów tego rozdziału: S. Sikorski, M. Florczak, K. Świtała, *Wdrażanie koncepcji Smart Villages w województwie mazowieckim*, polegające na opracowaniu propozycji dedykowanych do warunków wiejskich rozwiązań z zakresu e-health, w szczególności dotyczących telemedycyny i teleopieki, jako element koncepcji Smart Villages, realizowany w ramach konsorcjum przez: Politechnikę Warszawską (Wydział Geodezji i Kartografii), Szkołę Główną Gospodarstwa Wiejskiego w Warszawie (Wydział Nauk Ekonomicznych), Instytut Ekonomiki Rolnictwa i Gospodarki Żywnościowej – PIB, Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie (Centrum Cyfrowej Nauki i Technologii oraz Wydział Prawa i Administracji), Instytut Geodezji i Kartografii (Centrum Teledetekcji), Instytut Uprawy, Nawożenia i Gleboznawstwa w Puławach – PIB, Sieć Badawczą Łukasiewicz – Instytut Lotnictwa (Zakład Teledetekcji), oraz podmioty posiadające wiedzę praktyczną oraz możliwości wdrożenia i przetestowania wypracowanych rozwiązań, w tym: Mazowiecki Ośrodek Doradztwa Rolniczego w Warszawie, Mazowiecki Park Naukowo-Technologiczny – Park Spółdzielczy – Zespół eZdrowie, Warszawa, 2019–2021.

umocowany na gruncie przepisu art. 22 ust. 3b u.d.l. do określenia szczegółowych wymagań, jakim powinny odpowiadać zarówno pomieszczenia, jak i urządzenia oraz systemy teleinformatyczne/łączności podmiotu udzielającego wyłącznie właśnie ambulatoryjnych świadczeń zdrowotnych za pośrednictwem systemów teleinformatycznych lub systemów łączności – telemedycyny, w celu zapewnienia bezpieczeństwa zdrowotnego pacjentów.

Niestety, w odniesieniu do świadczeń udzielanych z zastosowaniem telemedycyny dotychczas minister zdrowia zaledwie dwukrotnie skorzystał ze swojego umocowania, wydając rozporządzenie z 11 kwietnia 2019 r. w sprawie standardów organizacyjnych opieki zdrowotnej w dziedzinie radiologii i diagnostyki obrazowej wykonywanej za pośrednictwem systemów teleinformatycznych,[292] oraz rozporządzenie z 12 sierpnia 2020 r. w sprawie standardu organizacyjnego teleporady w ramach podstawowej opieki zdrowotnej.[293]

Zgodnie z tym, co zostało już powiedziane, szczególnie istotny jest standard teleporady w ramach ambulatoryjnie realizowanej podstawowej opieki zdrowotnej. Pozytywnie należy ocenić uregulowanie dotyczące możliwości odmowy udzielenia świadczenia w formie teleporady lub możliwości kontaktu pacjenta z właściwym personelem medycznym, choć redakcja przepisu (określenie wyjątków od tej zasady) może nasuwać zastrzeżenia co do jego czytelności.

Bardzo istotne jest określenie na gruncie tego rozporządzenia terminów realizacji teleporady, tj. co do zasady nie później niż w pierwszym dniu roboczym następującym po dniu zgłoszenia się pacjenta, z zastrzeżeniem możliwości ustalenia z pacjentem późniejszego terminu, a także uregulowanie zasad nawiązania kontaktu z pacjentem, w szczególności nałożenie obowiązku podjęcia co najmniej trzykrotnej próby kontaktu z pacjentem, w odstępie nie krótszym niż 5 minut, w celu udzielenia teleporady. Wreszcie niezwykle istotne jest sprecyzowanie zasad potwierdzania tożsamości pacjenta i dokonywanie adnotacji w dokumentacji medycznej o realizacji świadczenia zdrowotnego w formie teleporady.

Jednocześnie krytycznie należy ocenić konieczność realizacji pierwszorazowej wizyty osobiście. Nasuwa się bowiem w tym miejscu uzasadniona wątpliwość, dlaczego każdy pacjent musi udać się najpierw na wizytę osobistą, a dopiero

---

[292] Rozporządzenie ministra zdrowia z 11 kwietnia 2019 r. w sprawie standardów organizacyjnych opieki zdrowotnej w dziedzinie radiologii i diagnostyki obrazowej wykonywanej za pośrednictwem systemów teleinformatycznych, DzU z 2019 r., poz. 834.

[293] Rozporządzenie ministra zdrowia z 12 sierpnia 2020 r. w sprawie standardu organizacyjnego teleporady w ramach podstawowej opieki zdrowotnej, DzU z 2022 r.. poz. 1194.

po niej może skorzystać z teleporady. W wielu przecież przypadkach lepszym rozwiązaniem byłaby najpierw teleporada, podczas której lekarz zebrałby pełny wywiad, wydał skierowanie na badania dodatkowe, a następnie zakwalifikował pacjenta do wizyty osobistej w przychodni w celu przeprowadzenia badania fizykalnego i analizy wyników badań dodatkowych. Jednocześnie pacjent nie musiałby zgłaszać się kilkakrotnie do przychodni. Postępowanie to ograniczyłoby także ryzyko powikłań związanych z chorobami infekcyjnymi, do których może dochodzić podczas oczekiwania pacjenta pod gabinetem lekarskim. Istnieją również przypadki kliniczne, w których potrzebna jest osobista wizyta, a wtedy teleporada jest bezzasadna i niepotrzebnie generuje obciążenie dla systemu ochrony zdrowia. Analogiczne uwagi nasuwają się w przypadku innych wyjątków, przede wszystkim wyłączenia możliwości udzielenia teleporady dzieciom do 6. roku życia. Decyzję bowiem, czy potrzebna jest teleporada, czy wizyta stacjonarna, powinna podejmować każdorazowo uprawniona osoba wykonująca dany zawód medyczny (w szczególności lekarz). Jest to tym bardziej uzasadnione, że pacjent ma zagwarantowane swobodne prawo wyboru, na jaki rodzaj wizyty się decyduje. Minister zdrowia mógłby oczywiście dokonać wyłączeń takich świadczeń, ale na podstawie art. 31b ustawy z 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych,[294] czyli w ramach określania zakresu świadczeń gwarantowanych.

Według dostępnej literatury tzw. telemedycyna synchroniczna, którą należy rozumieć jako konsultację lekarza z pacjentem, a nie jedynie ocenę przez lekarza danych, które pacjent uzupełnił w formularzu (a tak to działa w przypadku receptomatów), została uznana na świecie za godną i odpowiednią formę świadczenia dla pacjentów niewymagających badania fizykalnego.[295] Często jakość usług telemedycznych oceniana jest jako porównywalna z jakością wizyt stacjonarnych, a zadowolenie pacjentów i świadczeniodawców jako wysokie.[296] Czynnikami ułatwiającymi są: odpowiednia technologia, szkolenia oraz polityka refundacji kosztów, która zapewnia parytet pod względem kosztowym między telemedycyną a opieką osobistą. Bariery obejmują kwestie techniczne, takie jak niskie umiejętności techniczne i słaba łączność internetowa w niektórych populacjach pacjentów, a także bariery

[294] DzU z 2022 r., poz. 2561 ze zm.

[295] S. Khosla, *Implementation of Synchronous Telemedicine into Clinical Practice*, „Sleep Medicine Clinics" 2020, vol. 15, s. 347–358, https://doi.org/10.1016/j.jsmc.2020.05.002.

[296] A.S. Tenforde, H. Borgstrom, G. Polich, H. Steere, I.S. Davis, K. Cotton, M. O'Donnell, J.K. Silver, *Outpatient Physical, Occupational, and Speech Therapy Synchronous Telemedicine: A Survey Study of Patient Satisfaction with Virtual Visits During the COVID-19 Pandemic*, „American Journal of Physical Medicine & Rehabilitation" 2020, vol. 99 (11), s. 977–981, https://doi.org/10.1097/PHM.0000000000001571.

komunikacyjne w przypadku pacjentów wymagających wsparcia lub innych zasobów do komunikacji.[297]

Należy również zaznaczyć brak stosownych zmian norm etycznych, szczególnie kodeksów etyki zawodowej, które powinny zawierać co najmniej podobne rozwiązania dotyczące tej formy świadczenia usług. Na przykładzie Kodeksu Etyki Lekarskiej[298] dopuszczalny jest wniosek, że aspekt teleporad został *de facto* pominięty. Dzieje się tak, ponieważ art. 9 Kodeksu Etyki Lekarskiej, który nie został do tej pory zmieniony, stanowi: „Lekarz może podejmować leczenie jedynie po uprzednim zbadaniu pacjenta. Wyjątki stanowią sytuacje, gdy porada lekarska może być udzielona wyłącznie na odległość".

Pozytywnie należy jednak ocenić stanowisko Komisji Etyki Naczelnej Rady Lekarskiej, zgodnie z którym za błędną interpretację zasad obowiązujących w telemedycynie należy uznać komercyjne wystawianie e-ZLA i e-recept online na żądanie,[299] bez zachowania zasad telemedycznego badania podmiotowego i właściwej relacji lekarz – pacjent.[300] Z tym jednak zastrzeżeniem, że aspekt ten również powinien znaleźć miejsce w standardach teleporad określanych przez ministra zdrowia w ramach rozporządzeń wykonawczych.

Podsumowanie

Początkowo rozwiązania AI najczęściej były wykorzystywane w radiologii do diagnostyki obrazowej. Obecnie zaś coraz częściej są brane pod uwagę przy analizie objawów chorobowych i wyników badań dodatkowych podczas konsultacji, czyli w diagnostyce różnicowej.

1. **Szeroko ujmowany rozwój rozwiązań opartych na Al lub je wykorzystujących pociąga za sobą konieczność przygotowania stosownej regulacji prawnej.**[301] Potrzebę taką dostrzeżono przed kilku już laty w UE. Jednocześnie

[297] Z. Lindenfeld, C. Berry, S. Albert et al., *Synchronous Home-Based Telemedicine for Primary Care: A Review*, „Medical Care Research and Review" 2023, vol. 80 (1), s. 3–15, https://doi.org/10.1177/10775587221093043.

[298] Naczelna Izba Lekarska, *Kodeks Etyki Lekarskiej*, https://nil.org.pl/uploaded_images/1574857770_kodeks-etyki-lekarskiej.pdf (dostęp: 5.10.2022).

[299] *KEL o komercyjnym wystawianiu recept online*, https://prawo.mp.pl/wiadomosci/317017,kel-o-komercyjnym-wystawianiu-recept-online (dostęp: 13.03.2023).

[300] Brakuje również wystarczających rekomendacji towarzystw naukowych, opartych na EBM dla lekarzy, które określałyby np. zasady przeprowadzania telemedycznego badania podmiotowego, kryteria kwalifikacji pacjenta do teleporady i wreszcie wytyczne, kiedy pacjentów należałoby przekierowywać po teleporadzie na wizytę stacjonarną. Najwięcej publikacji zawierających rekomendacje pojawia się w kardiologii, natomiast w wielu innych dziedzinach medycyny istnieje duża potrzeba wypracowania standardów. W efekcie w Polsce rozwinęły działalność firmy, potocznie nazywane „receptomatami", których działanie istotnie odbiega od założeń konsultacji telemedycznej. R. Piotrowicz, M. Grabowski et al., *„Baltic Declaration" – telemedicine and mHealth as support for clinical processes in cardiology. The opinion of the Committee of Informatics and Telemedicine of the Polish Society of Cardiology and Telemedicine Clinical Sciences Committee of the Polish Academy of Sciences*, „Kardiologia Polska" 2015, vol. 73 (7), https://doi.org/10.5603/KP.2015.0131.

[301] Zob.: *Administracja w demokratycznym państwie prawa…*, op.cit.

prace nad regulacją na tym poziomie mają w założeniu zapewnić swobodny obrót towarów i usług z zastosowaniem technologii AI oraz usunąć zagrożenie fragmentaryzacją wspólnego rynku, co może mieć miejsce w przypadku wprowadzenia odmiennych rozwiązań w poszczególnych krajach. Regulacja rozwiązań AI na poziomie UE z jednej strony ma więc zapewnić równe warunki działania i ochrony obywateli, z drugiej zaś wzmocnić konkurencyjność przemysłową Europy w tym obszarze.

Nadal jednak – mimo istotnej aktywności koncepcyjnej organów UE – regulacje w tym zakresie znajdują się w fazie projektów. Przepisy są jednak już na tyle skonkretyzowane, że można dostrzec rysujący się problem jednoznacznego określenia ich relacji do obowiązujących – ale też wciąż projektowanych – innych aktów prawnych. **Kluczowe jest bowiem takie doprecyzowanie projektowanych przepisów, aby z jednej strony uzupełniały regulacje już obowiązujące, z drugiej zaś nie wyłączały ich bądź nie powtarzały.**

2. W projekcie będącym przedmiotem analizy zawarto definicję „systemu sztucznej inteligencji", obejmując jej zakresem również uczenie maszynowe z podziałem na uczenie nadzorowane, bez nadzoru oraz uczenie z wykorzystaniem szerokiej gamy metod, w tym uczenia głębokiego. Mając na uwadze stan rozwoju już funkcjonujących rozwiązań typu AI w sektorze ochrony zdrowia, należy tak szerokie ujęcie ocenić jednak pozytywnie, chociaż definicja ma też mankamenty, bo obejmuje również „metody oparte na logice i wiedzy", co może spowodować, że do tego typu rozwiązań będzie się zaliczać już obecnie wykorzystywane oprogramowanie. Należy przyjąć, że nie taki był cel projektodawcy. **Wydaje się, że już teraz trzeba się niejako pogodzić z tym, że wraz z rozwojem technologii definicja „systemu sztucznej inteligencji" będzie musiała ulegać modyfikacjom. Takie ujęcie pociąga więc za sobą konieczność monitorowania poziomu rozwiązań w ujęciu technicznym.**

3. Zagadnieniem mającym zasadnicze znaczenie jest kwestia nadzoru nad rozwiązaniami kwalifikowanym do AI. Na ten aspekt, jako kluczowy, wskazuje też Europejski Komitet Ekonomiczno-Społeczny, podkreślając konieczność pozostawienia niektórych decyzji (m.in. w opiece zdrowotnej) wyłącznie w gestii człowieka, w szczególności, kiedy „decyzje te obejmują aspekt moralny i konsekwencje prawne lub wpływ

na społeczeństwo". Na tym tle bardzo trafnie dokonano zróżnicowania stopnia ryzyka poszczególnych rozwiązań. Jak już wskazano, w motywie 48 projektu bardzo wyraźnie została podkreślona konieczność projektowania i opracowywania rozwiązań AI wysokiego ryzyka w taki sposób, aby człowiek mógł efektywnie nadzorować ich funkcjonowanie. Rozróżnienie to jest wyjątkowo ważne w sektorze ochrony zdrowia. W tym bowiem przypadku chronione są najwyższe wartości, jak zdrowie i życie człowieka, co podkreślają sami projektodawcy. W motywie 28 wprost wskazano, że systemy sztucznej inteligencji mogą przynosić szkodliwe skutki dla zdrowia i bezpieczeństwa osób. Ma to szczególne znaczenie właśnie w sektorze ochrony zdrowia, w którym: „chodzi o szczególnie wysoką stawkę, jaką jest życie i zdrowie, coraz bardziej zaawansowane systemy diagnostyczne i systemy wspomagające decyzje podejmowane przez człowieka powinny być niezawodne i dokładne". Jeśli chodzi o rozwiązania z obszaru AI dotyczące ochrony zdrowia, właśnie aspekt zaostrzający odpowiedzialność jest szczególnie istotny. Dlatego jeszcze przed wprowadzeniem tych rozwiązań do obrotu lub ich oddaniem do użytku dostawca powinien wskazać odpowiednie środki w tym zakresie. **Szczególnie istotna jest konieczność wprowadzenia rozwiązań polegających na „wbudowanych ograniczeniach operacyjnych", których AI nie potrafi sama obejść i musi reagować na działania człowieka – operatora systemu. W przypadku systemów sztucznej inteligencji wysokiego ryzyka projekt i opracowanie muszą uwzględniać odpowiednie narzędzia „interfejsu człowiek – maszyna", które zapewniają efektywny nadzór.** Jest to szczególnie uzasadnione, gdyż nadzór wiąże się właśnie z zapobieganiem – minimalizacją – ryzyka dla zdrowia, bezpieczeństwa i praw podstawowych.

Należy w tym miejscu przypomnieć sformułowaną hipotezę roboczą, którą zweryfikuje dopiero być może odległa przyszłość, że pojawienie się tzw. AI ze świadomością jest kwestią czasu i wtedy prawo będzie musiało temu sprostać. Oczywiście, trudno byłoby projektować regulacje prawne z takim wyprzedzeniem. **Jednak szybkie reagowanie na postęp techniczny przez jego monitorowanie jest wręcz konieczne. Jednocześnie zasadne jest podkreślanie konieczności pozostawienia zawsze ostatecznej decyzji (dzięki nadzorowi) w rękach człowieka.**

Na tle sektora ochrony zdrowia w literaturze wskazuje się obawę, że

badania przeprowadzane w oparciu o algorytmy AI mogą nie uwzględniać złożoności całego organizmu ludzkiego ani kwestii psychologicznych, niezwykle ważnych w relacji lekarz – pacjent.[302] Trzeba jednak przyjąć, że procesu rozwoju tej technologii i jej zastosowania w medycynie po prostu nie można zatrzymać. **W konsekwencji trzeba wydobywać to, co jest pozytywne w tych rozwiązaniach, i starać się przewidywać i eliminować zagrożenia.**

4. **Bardzo istotnym rozwiązaniem dla rozwoju AI są tzw. piaskownice regulacyjne (art. 53 projektu), przez które należy rozumieć utworzone przez państwo lub grupę państw członkowskich „kontrolowane środowisko ułatwiające opracowywanie, testowanie i walidację innowacyjnych systemów sztucznej inteligencji przez ograniczony czas przed ich wprowadzeniem do obrotu lub oddaniem do użytku". Mamy tutaj więc kontrolowane – dzięki określeniu zasad, w tym zasad odpowiedzialności – środowisko, w którym rozwiązania z zakresu AI mogą być bezpiecznie testowane.**

W drugim wątku prowadzonych rozważań należy wskazać, że mimo umocowania minister zdrowia dotychczas zaledwie w dwóch przypadkach określił standardy organizacyjne udzielania świadczeń zdrowotnych za pośrednictwem systemów teleinformatycznych i systemów łączności, tj. telemedycyny.

1. Standardy udzielania świadczeń zdrowotnych z wykorzystaniem telemedycyny powinny uwzględniać możliwość zlecania pacjentowi dodatkowych badań i podstawowych badań obrazowych, ale również informowania pacjenta o ich wynikach. Ponadto powinny określać zasady przeprowadzenia badania kontrolnego pacjenta po udzieleniu porady telemedycznej, z wyraźnym zastrzeżeniem, że badanie to może się odbywać również w ramach telekonsultacji.

   Rozwiązania dotyczące teleporad mają szczególne znaczenie przy udzielaniu świadczeń zdrowotnych w opiece ambulatoryjnej. Dlatego tak ważne było wprowadzenie standardów teleporad w podstawowej opiece zdrowotnej. W przyjętym rozporządzeniu trafnie określono terminy realizacji teleporady oraz zasady nawiązania kontaktu z pacjentem, w szczególności nałożenie obowiązku podjęcia co najmniej trzykrotnej próby kontaktu z pacjentem, w odstępie nie krótszym

[302] J.E.H. Korteling, G.C. van de Boer-Visschedijk, R.A.M. Blankendaal, R.C. Boonekamp, A.R. Eikelboom, Human... op.cit.

niż 5 minut, w celu udzielenia teleporady. Wreszcie niezwykle istotne było sprecyzowanie zasad potwierdzania tożsamości pacjenta i dokonywanie adnotacji w dokumentacji medycznej o realizacji świadczenia zdrowotnego w formie teleporady.

Natomiast krytycznie należy ocenić konieczność realizacji pierwszorazowej wizyty osobiście. Pojawia się bowiem uzasadniona wątpliwość, dlaczego każdy pacjent musi udać się najpierw na wizytę stacjonarną, a dopiero po niej może skorzystać z teleporady. W wielu przecież przypadkach właściwszym rozwiązaniem byłoby przeprowadzenie najpierw teleporady, podczas której lekarz zebrałby pełny wywiad, wydał skierowanie na badania dodatkowe, a następnie zakwalifikował pacjenta do wizyty osobistej w celu przeprowadzenia badania fizykalnego i analizy wyników badań dodatkowych. Ujęcie takie ograniczyłoby także ryzyko powikłań związanych z chorobami infekcyjnymi, do których może dochodzić podczas oczekiwania pacjenta pod gabinetem lekarskim. Argumentem za takim rozwiązaniem są także względy kliniczne: kiedy zasadna jest osobista wizyta, niepotrzebna jest teleporada, która zwiększa tylko obciążenie systemu ochrony zdrowia. Analogiczne uwagi nasuwają się na tle innych wyjątków, m.in. wyłączenia możliwości udzielenia teleporady dzieciom do 6. roku życia. Decyzję bowiem, czy właściwa jest w danym przypadku klinicznym teleporada, czy wizyta stacjonarna, powinna podejmować każdorazowo uprawniona osoba wykonująca dany zawód medyczny (w szczególności lekarz). Jest to tym bardziej uzasadnione, że pacjent ma zagwarantowane swobodne prawo wyboru rodzaju wizyty. Minister zdrowia mógłby oczywiście dokonać wyłączeń takich świadczeń, ale w rozporządzeniach określających zakresy świadczeń opieki zdrowotnej finansowanych ze środków publicznych, czyli zakresy świadczeń gwarantowanych. **Należy bowiem podkreślić, że standardy powinny być uniwersalne dla wszystkich świadczeń udzielanych z wykorzystaniem telemedycyny, bez względu na źródło finansowania tych świadczeń. Natomiast minister zdrowia właśnie „rozporządzeniami koszykowymi" mógłby regulować zakres świadczeń finansowanych ze środków publicznych, zamiast *de facto* ograniczać zakres świadczeń zdrowotnych udzielanych w ten sposób.** Można też w tym miejscu zgłosić wątpliwość, czy pozbawienie możliwości wyboru pacjenta, decydującego się np. na komercyjnie finansowaną teleporadę tzw. pierwszorazową, nie narusza jego prawa do świadczeń zdrowotnych

odpowiadających wymaganiom aktualnej wiedzy medycznej określonych przecież aktem rangi ustawowej,[303] a więc aktem wyższego rzędu niż rozporządzenie.

2. Należy również w tym miejscu zaznaczyć brak stosownych zmian norm etycznych, w tym kodeksów etyki zawodowej, które powinny zawierać co najmniej podobne rozwiązania dotyczące tej formy świadczenia usług. **Na przykładzie Kodeksu Etyki Lekarskiej[304] dopuszczalny jest wniosek, że aspekt teleporad został *de facto* pominięty. Dzieje się tak, ponieważ przepis art. 9 Kodeksu Etyki Lekarskiej, który nie został do tej pory zmieniony, stanowi: „Lekarz może podejmować leczenie jedynie po uprzednim zbadaniu pacjenta. Wyjątki stanowią sytuacje, gdy porada lekarska może być udzielona wyłącznie na odległość".**

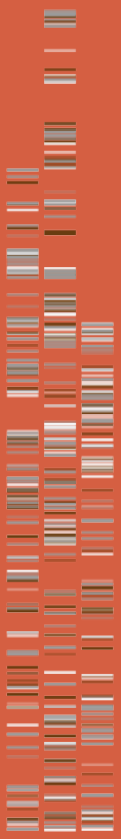
Jednocześnie pozytywnie trzeba ocenić aktywność samorządu zawodowego lekarzy – stanowisko Komisji Etyki Naczelnej Rady Lekarskiej, zgodnie z którym za błędną interpretację zasad obowiązujących w telemedycynie należy uznać komercyjne wystawianie e-ZLA i e-recept online na żądanie, bez zachowania zasad telemedycznego badania podmiotowego i właściwej relacji lekarz – pacjent. Z tym jednak zastrzeżeniem, że aspekt ten powinien również znaleźć miejsce w standardach teleporad określanych przez ministra zdrowia w ramach rozporządzeń wykonawczych.

---

[303] Ustawa z 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, DzU z 2022 r., poz. 1876 ze zm.

[304] Naczelna Izba Lekarska (NIL), *Kodeks Etyki Lekarskiej*, https://nil.org.pl/uploaded_images/1574857770_kodeks-etyki-lekarskiej.pdf (dostęp: 5.10.2022).

[305] *KEL o komercyjnym wystawianiu recept online*, https://prawo.mp.pl/wiadomosci/317017,kel-o-komercyjnym-wystawianiu-recept-online (dostęp: 13.03.2023).



ARTUR OLESCH

Ekspert digitalizacji rynku ochrony zdrowia

09

Wygoda użytkownika

User experience (UX), czyli jak poprawić doświadczenia lekarzy i pielęgniarek z pracy z systemami IT

Blisko 50 proc. czasu wizyty pacjenta lekarz spędza przez komputerem, wprowadzając dane i generując dokumentację. Aby system IT pomagał w pracy, zamiast prowadzić do frustracji, trzeba przyjrzeć się elementom wpływającym na efektywność i płynność jego obsługi.

Każdy życzyłby sobie, aby systemy informatyczne dla lekarzy i pielęgniarek były tak łatwe w obsłudze i intuicyjne jak smartfony. Sprawa nie jest jednak taka łatwa, bo to narzędzia o zupełnie innym kalibrze. Systemy IT w ochronie zdrowia są dziś rozbudowanymi i wielofunkcyjnymi rozwiązaniami, które muszą spełniać funkcje sprawozdawcze, bezpiecznie gromadzić dane, obsługiwać administracyjnie całą ścieżkę opieki nad pacjentem, tworzyć poprawnie takie dokumenty jak e-recepta czy e-skierowanie, wymieniać dane z innymi systemami, stosując standardy interoperacyjności.

Czy, potocznie mówiąc, system jest łatwy w obsłudze, czy skomplikowany, jest bardzo subiektywnym odczuciem. Wszystko zaczyna się od struktury rozwiązania: liczby kliknięć potrzebnych do wprowadzenia danych, przejrzystości interfejsu użytkownika, a nawet szaty graficznej, czcionek, wielkości pól, automatyzacji uzupełniania formularzy, przepływu danych w ramach systemu.

Za architekturę interakcji użytkownika z systemem odpowiedzialny jest tzw. UX/UI designer (*User Experience/User Interface*). Dziś niemal każda firma IT zatrudnia osoby odpowiedzialne za to, by aplikacja nie była tylko ładna i funkcjonalna, ale także maksymalnie prosta w użytkowaniu, a jednocześnie, by została zachowana dostępność niezbędnych funkcji. Jednym słowem, zadaniem takiego pracownika jest zwiększenie satysfakcji użytkownika z korzystania z systemu IT lub aplikacji mobilnej i zapewnienie pozytywnych doświadczeń.

Praca UX/UI designera zaczyna się od zbadania funkcji, jakie system musi realizować, a także wywiadów z użytkownikami, na podstawie których identyfikowane są ich potrzeby, sekwencje wykonywanej pracy, ścieżka obsługi pacjenta i przepływy pracy. Następnie powstaje mapa procesów, która jest wpasowywana w projekt graficzny. Proces zamyka projektowanie interfejsu, czyli określenie położenia poszczególnych pól, opcji, okienek itd.

Co wpływa na doświadczenie użytkownika?

Zgodnie z definicją Międzynarodowej Organizacji Normalizacyjnej (ISO), doświadczenie użytkownika (UX) to „postrzeganie i reakcje danej osoby wynikające z użycia i/lub przewidywanego użycia produktu, systemu lub usługi". Składa się z dwóch warstw: estetycznej oceny wyglądu systemu (budowy, stylu, kolorystyki, przejrzystości) oraz doświadczeń z obsługą, które powstają dopiero podczas interakcji.

Doświadczenie użytkownika jest efektem całego szeregu czynników i obejmuje m.in.: emocje, przekonania, preferencje, percepcje, fizyczne i psychologiczne reakcje, zachowania i osiągnięcia użytkowników, które występują przed, w trakcie i po zakończeniu pracy.

Do tego dochodzą jeszcze takie elementy jak wizerunek producenta, który może wpływać na wstępne, pozytywne lub negatywne, nastawienie do systemu. Nie mniej ważna jest szybkość obsługi i wydajność, ale i wcześniejsze doświadczenia, umiejętności cyfrowe, a nawet kontekst użytkowania (wielkość ekranu, pomieszczenie itd.). Sprawa jest więc o wiele bardziej zawiła i nie polega tylko na pierwszych wrażeniach zależnych od poczucia estetyki. Kiedy jednym podoba się system X, inni wybiorą system Y, mimo że nie różnią się funkcjami.

UX ma ogromny wpływ na pracę personelu

Już z definicji doświadczenia użytkownika widać, że za jego poprawę odpowiada nie tylko dostawca systemu IT, ale także – co bardzo często jest ignorowane – jego użytkownik końcowy. Klasyczny przykład stanowi wydajność i rodzaj sprzętu, na którym personel medyczny korzysta z systemu.

Zaakceptowanie takiej współodpowiedzialności pociąga za sobą odpowiedzialność, którą liczne podmioty – nie tylko w branży medycznej – wolą scedować na inżynierów i architektów systemów IT. O wiele łatwiej szukać błędów w oprogramowaniu, niż zidentyfikować i usunąć niedociągnięcia związane z zarządzaniem, zmianą czy budowaniem innowacyjnej kultury organizacyjnej. Dowodem są wdrożenia tego samego systemu IT w różnych placówkach, raz zakończone sukcesem i zadowoleniem personelu, innym razem – porażką i frustracją.

Właśnie dlatego zespół każdej placówki powinien z bliska przyjrzeć się interakcji personelu z systemem. Stawką jest czas spędzony przed komputerem, płynna praca, satysfakcja pracowników, czas na

rozmowę z pacjentem, a nawet wyniki kliniczne i biznesowe podmiotu. Na drugim biegunie znajdują się takie zagrożenia jak zaburzenia organizacyjne i chroniczny stres pracowników, prowadzący do wypalenia zawodowego, a w efekcie niska satysfakcja pacjentów.

Trzeba też przyznać, że negatywne doświadczenia personelu medycznego w pracy z systemami IT są po części uwarunkowane historycznie. Wiele systemów ma swoje korzenie w latach 90. XX w., kiedy powstawały pierwsze systemy do obsługi rozliczeń z Kasami Chorych. Wówczas liczyła się tylko funkcjonalność, a pojęcia UX/UI nawet nie były znane. W kolejnych latach do prostych systemów sprawozdawczych dokładano kolejne elementy, bez dużych zmian w architekturze. W ten sposób systemy stawały się coraz funkcjonalniejsze, ale czasochłonne i trudne w obsłudze.

Na szczęście współczesne rozwiązania IT dla ochrony zdrowia to już najczęściej nowoczesne, zintegrowane systemy budowane w oparciu o wiedzę z zakresu UX/UI, bo dostawcom oprogramowania zależy na tworzeniu konkurencyjnych, wysokiej jakości narzędzi. Jednak i oni są ograniczeni możliwościami techniki. Przykładowo, najbardziej wrażliwym elementem interakcji użytkownika z systemem IT jest klawiatura. Dane muszą być wpisywane ręcznie. Zmieni się to dopiero wówczas, gdy na rynku pojawią się godne zaufania i precyzyjne techniki transkrypcyjne oparte na sztucznej inteligencji, aby wywiad z pacjentem mógł zostać automatycznie wprowadzony do systemu, z zachowaniem uporządkowania danych.

Mimo tych ograniczeń, placówka medyczna ma wiele możliwości wpływania na sposób obsługi systemu. Dobre systemy IT posiadają zestawy opcji ułatwiające personalizację obsługi i konfigurację sposobu wprowadzania danych. Użytkownicy mogą definiować słowniki i formularze znacznie przyspieszające wprowadzenie danych. Jeśli wdraża się zintegrowane rozwiązania, dane przepływają między systemami w architekturze IT placówki medycznej i nie trzeba ich wprowadzać podwójnie.

Mierzenie i optymalizacja obsługi systemu IT

Punktem wyjścia optymalizacji doświadczeń użytkowników systemów IT jest ich pomiar. W tym celu trzeba jasno określić cel. To od niego zależy, co dokładnie będzie mierzone. Żeby skrócić czas wprowadzania danych do systemu IT, trzeba przeanalizować ścieżkę wprowadzania danych i szukać sposobów jej skrócenia albo ustandaryzowania. Ale jeśli priorytetem jest wydajność pracy, należy też uwzględnić otoczenie, w którym porusza

się lekarz lub pielęgniarka – dostępne urządzenia i sprzęt, organizację pracy.

Może się okazać, że digitalizacja jedynie „zabetonowała" nieefektywne procesy, czyli na stare przepływy pracy został nałożony system IT. Niestety, w takim przypadku oprogramowanie stanie się tak samo nieefektywne jak wspomniane procesy. System IT przez sam fakt wdrożenia nie poprawi sytuacji.

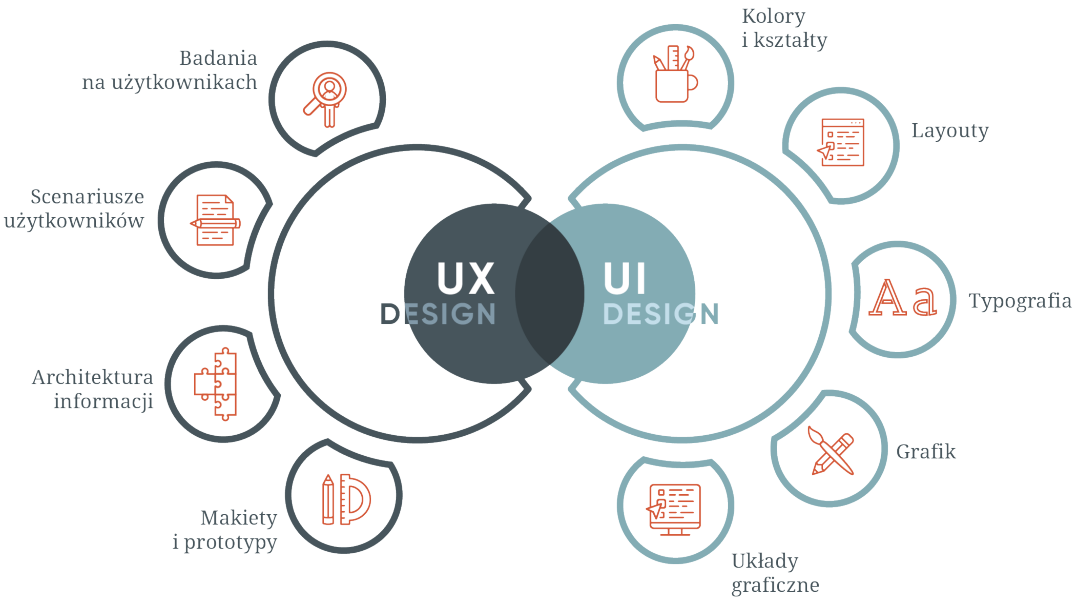
Aby tego uniknąć, menedżerowie placówek powinni sięgnąć do takich metod jak *design thinking* czy projektowanie (procesów) zorientowane na użytkownika (*user-centered design*).

Design thinking pozwala przykładowo zidentyfikować wąskie gardła obsługi pacjenta i zaprojektować od nowa ścieżkę opieki, z kolei UCD skupia się na ergonomii pracy z systemami. W przypadku IT obejmuje np. dopasowanie wielkości ekranów (duże ekrany dla lepszej analizy zdjęć medycznych), mobilności urządzeń (komputer stacjonarny czy tablety), włączenie ostrzeżeń lub powiadomień (alerty dotyczące interakcji leków lub brakujących danych) itd.

Podsumowanie

Klasyczne podejście do doświadczeń pracy z systemami IT zakładało, że to zadanie dla ich dostawców. Jak się okazuje, także placówka medyczna może wiele zrobić, aby zwiększyć zadowolenie lekarzy, pielęgniarek i personelu administracyjnego z korzystania z oprogramowania. Nie podlega dyskusji, że punktem wyjścia jest zawsze dobrej jakości system informatyczny: szybko działający, zapro-

RYSUNEK 17. ELEMENTY UX DESIGN ORAZ UI DESIGN



jektowany z myślą o intuicyjnej obsłudze, pozbawiony błędów. Tak samo ważna jest partnerska relacja z firmą – twórcą systemu i bieżące aktualizacje, dzięki którym system będzie spełniał wymagania funkcjonalne i bezpieczeństwa.

Systemy nie są statyczne. Dobre rozwiązania dają duże możliwości konfiguracyjne, dopasowania interfejsu (widoku okien), zakresu widocznych opcji i alertów ostrzegających o błędach we wprowadzaniu danych. Trzy główne zasady, które warto zapamiętać, to: po pierwsze – optymalizacja przepływów pracy, zanim wdrożony zostanie system IT (albo ich późniejsze dopasowanie, jeżeli tego nie zrobiono wcześniej); po drugie – poświęcenie czasu na analizę potrzeb użytkowników i personalizację systemu; po trzecie – systematyczne mierzenie doświadczeń i korygowanie ewentualnych zakłóceń.

10

MACIEJ MALENDA

Doctor.One

Cyfryzacja ochrony zdrowia a innowacje

Przedstawione w tym rozdziale wyzwania, pomysły narzędzi i modele to tylko wierzchołek góry lodowej wdrażania nowoczesnych rozwiązań. Jednocześnie opisane elementy stanowią podstawę nowoczesnego, cyfrowego obszaru ochrony zdrowia.

Dlaczego innowacje są ważne?

Innowacja, szczególnie w medycynie, nie jest niczym nowym. Od początku istnienia tej dziedziny nauki rozwijaliśmy ją empirycznie. Za tym idzie sprawdzanie nowych pomysłów zmian procesów, wykorzystania nowego narzędzia lub zmian organizacyjnych w jednostkach medycznych, które mogłyby wesprzeć ludzi w jeszcze lepszym dbaniu o zdrowie oraz ratowanie życia pacjentów.

Jeśli spojrzymy na to z szerszej perspektywy, właśnie opisaliśmy definicję innowacji.[306]

Innowacje są niezbędne w rozwoju, a w dzisiejszych czasach powstało na ich temat wiele mitów, są też źródłem lęku. Szczególnie w przypadku rozwiązań cyfrowych, które zmieniają nasze zachowania oraz przyzwyczajenia, jesteśmy ostrożni i staramy się obserwować wpływ, jaki mają na życie codzienne.

Niestety, dziesiątki lat wdrażania nowości nie spowodowały, że obecnie wprowadzanie zmian stało się łatwiejsze. Ludzka natura powszechnie opiera się zmianie, szczególnie w podmiotach, w których jesteśmy pracownikami. Powstało na ten temat wiele publikacji, których autorzy starają się nie tylko przybliżyć powody, ale również znaleźć sposoby rozwiązania tego problemu.[307] Wśród **podstawowych powodów oporu przed nowościami** wymieniane są:

1. **Brak pewności siebie** – szczególnie w kontekście zmiany i niepewności, jak ta zmiana wpłynie na życie jednostki
2. **Samostabilność** – rozumiana jako brak kontroli nad sobą i w rezultacie wpływanie na inne jednostki w środowisku (szczególnie w pracy)
3. **Zwiększony stres** – spowodowany jednakowo nasiloną presją na jednostkę (na przyjęcie zmiany) oraz niepewnością związaną z samą zmianą
4. **Niepewność** – wynikająca z braku informacji na temat zmiany
5. **Brak potrzeby rozwoju** – pracownicy, którzy nie chcą korzystnie zmieniać swoich wyników pracy, nie potrzebują zmian
6. **Niechęć do nowości** – wynikająca z typu osobowości
7. **Brak motywacji** – brak zrozumienia powodów, dla których mamy wprowadzić zmianę

---

[306] https://pfr.pl/slownik/slownik-innowacja.html.

[307] A.H Damawan, S.Azizah, *Resistance to Change: Causes and Strategies as an Organizational Challenge*, 2020, https://www.atlantis-press.com/proceedings/acpch-19/125932614

8. **Strach przed porażką** – występuje naturalnie u części osób wprowadzających zmianę i czujących odpowiedzialność za jej powodzenie
9. **Niska samosterowność oraz niezależność** – powoduje, że część osób nie potrafi skutecznie wdrożyć zmiany
10. **Niskie zaangażowanie** – brak chęci poświęcenia energii na wprowadzenie zmiany

Dodatkowo wymienia się **organizacyjne przyczyny braku skutecznego wprowadzania zmian**:

1. **Niezrozumienie zmiany** – brak jasnej komunikacji na temat podstaw i konieczności wprowadzenia elementów rozwojowych
2. **Brak zaangażowania** pracowników we współtworzenie i wprowadzenie zmiany – pracownicy czują się niezauważeni i opierają się wprowadzeniu zmiany
3. **Brak komfortu** – praca pod presją powoduje brak chęci i przestrzeni na wprowadzenie zmian
4. **Cynizm i brak komunikacji** – nieodpowiednie przedstawienie zmiany oraz brak wiedzy, dlaczego jest wprowadzana, powoduje, że nawet przekonane osoby nie mają możliwości wyrażenia swojej opinii i wolą nie mówić o pozytywnych efektach
5. **Brak wsparcia w zmianie** – wynika z niskiego zaangażowania pracowników w cele podmiotu i niezrozumienie, w jaki sposób zmiana wpływa na ich pracę
6. **Niesprzyjająca kultura organizacji** – brak wartości oraz kultury wprowadzania zmian i zrozumienia dla ciągłego procesu rozwoju
7. **Brak pewności utrzymania zatrudnienia** – pracownicy niepewni swojego zatrudnienia nie są chętni wdrażać zmiany, które mogą spowodować jeszcze większe problemy z utrzymaniem pracy
8. **Brak wsparcia organizacyjnego** – przez niejasne przekazy dotyczące zmiany

Jak widać, proces wprowadzania zmiany (a co za tym idzie innowacji) jest procesem trudnym, wymagającym zaangażowania interesariuszy. Wiele z wymienionych punktów występuje w placówkach publicznych i prywatnych świadczących usługi medyczne. Poza tym poruszamy się w bardzo delikatnym obszarze, w którym jeszcze mocniej zwracamy uwagę na niepopełnianie błędów, ponieważ każdy błąd może mieć wpływ na ludzkie zdrowie, a nawet życie.

Jednocześnie nie możemy pozwolić sobie, aby obszar zdrowia pozostał niezmienny. Jego rozwój przez ostatnie 100 lat jest ogromny, wręcz nie do określenia w liczbach. Od zmniejszenia śmiertelności dzieci ponad dziesięciokrotnie w krajach rozwiniętych (bazując na informacjach o sytuacji w Stanach Zjednoczonych między

1915 i 1990 r.[308]) po wydłużenie życia oraz wydłużenie życia w zdrowiu, które tylko w latach 2000–2019 r. wzrosło o 8 proc.[309]

Nasuwa się zatem pytanie: **w jaki sposób skutecznie wdrażać innowacje w ochronie zdrowia?** Specyfika tego obszaru wskazuje przede wszystkim trzy czynniki, nad którymi warto się zastanowić:

1. Zaangażowanie użytkowników nowych rozwiązań lub procesów
2. Zrozumienie pozycji wielu interesariuszy w obszarze ochrony zdrowia i wpływu na nich innowacji
3. Zapewnienie bezpieczeństwa testowania nowych rozwiązań

Poszczególne punkty rozwinięte zostaną w kolejnych akapitach tekstu.

Wdrażanie innowacji w systemie zdrowia

BUDOWANIE ZAANGAŻOWANIA UŻYTKOWNIKÓW

Mimo że projektowanie zorientowane na użytkownika (ang. *user centered design*) jest stosowane od ponad 40 lat, to w zakresie ochrony zdrowia zaczęło się pojawiać dopiero 10 lat temu[310] i nadal nie jest standardowym procesem wdrażania innowacji.

W skrócie projektowanie zorientowane na użytkownika ma na celu[311] stworzenie rozwiązań o wysokim poziomie użyteczności. Przez użyteczność rozumie się zestaw cech końcowego produktu lub procesu, które umożliwiają danej grupie użytkowników osiągnąć specyficzny cel w efektywny, satysfakcjonujący i skuteczny sposób.

W praktyce, projektując rozwiązania z użyciem UCD, wykorzystuje się trzy podstawowe zasady[312]:

1. Skoncentrowanie na użytkownikach i zadaniach – usystematyzowane zbieranie informacji od grup, dla których projektujemy rozwiązania
2. Empiryczne sprawdzanie i testowanie rozwiązań – skupienie na łatwości nauki i użytkowania produktu, a także testowanie prototypów z docelowymi użytkownikami
3. Iteracyjność projektu – ciągłe rozwijanie produktów i procesów, zgodnie z informacjami zebranymi od użytkowników. Zezwalanie na testowanie rozwiązań nawet na wczesnym etapie ich projektowania.

---

[308] A. Bhatia, N. Krieger, S.V Subramanian *Learning From History About Reducing Infant Mortality: Contrasting the Centrality of Structural Interventions to Early 20th-Century Successes in the United States to Their Neglect in Current Global Initiatives*. Milbank Q. 2019 Mar;97(1):285-345. doi: 10.1111/1468-0009.12376. PMID: 30883959; PMCID: PMC6422600.

[309] https://www.who.int/data/gho/data/themes/mortality-and-global-health-estimates/ghe-life-expectancy-and-healthy-life-expectancy

[310] https://www.researchgate.net/profile/Masitah-Ghazali/publication/286652068_User_centered_design_practices_in_healthcare_A_systematic_review/links/5894afae45851563f82bc4d8/User-centered-design-practices-in-healthcare-A-systematic-review.pdf

[311] https://www.w3.org/WAI/EO/2003/ucd

[312] J. Rubin, *Handbook of Usability Testing: How to Plan, Design, and Conduct Effective Tests,* John Wiley and Sons, Inc., 1984.

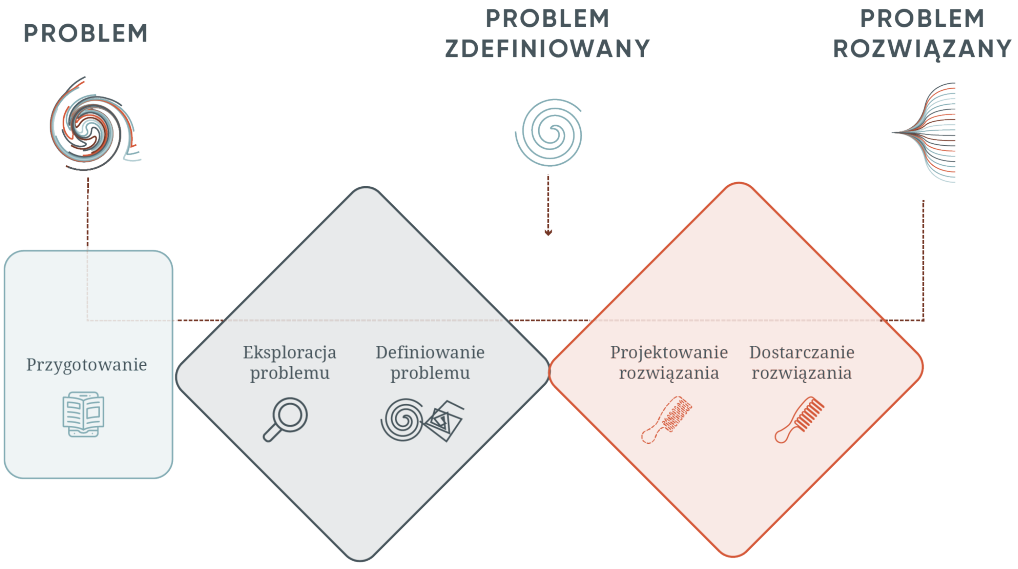
W postaci graficznej proces wprowadzania innowacji często przedstawiany jest w formie podwójnego diamentu (rysunek 18).[313]

Proces ten jest stosowany coraz szerzej w różnych dziedzinach gospodarki, stał się również nieodłącznym elementem budowania rozwiązań cyfrowych. Większość nowoczesnych produktów online powstała w oparciu o zasadę tworzenia zorientowanego na użytkownika.

W obszarze zdrowia UCD stosowane jest dopiero od kilku lat. Mimo prostych zasad, nie jest łatwe do zaimplementowania, szczególnie kiedy proces adaptacji aplikacji medycznych jest bardziej skomplikowany, a konsekwencje błędów są znacznie poważniejsze. Dlatego niewiele placówek świadczących usługi medyczne decyduje się wdrożyć taki system. Kiedy spojrzymy na wyniki, okazuje się jednak, że stosowanie projektowania zorientowanego na użytkownika umożliwia stworzenie lepiej opracowanego, a co za tym idzie bardziej użytecznego i bezpiecznego systemu cyfrowej ochrony zdrowia.[314]

Jednym z najsłynniejszych przykładów zrozumienia użytkownika i zbudowania rozwiązania opartego na jego doświadczeniu jest pomysł projektantów z GE Healthcare. Po szkoleniu z Design Thinking, przygotowanym przez organizację IDEO,[315] zaczęli projektować, stawiając

RYSUNEK 18. PROCES WPROWADZANIA INNOWACJI W FORMIE PODWÓJNEGO DIAMENTU



[313] https://blog.strefakursow.pl/content/images/2022/02/ux1.png

[314] R. Ratwani, *Developing Evidence-Based, User-Centered Design and Implementation Guidelines to Improve Health Information Technology Usability - Final Report.* (Prepared by MedStar Health Research Institute under Grant No. R01 HS023701). Rockville, MD: Agency for Healthcare Research and Quality, 2021.

[315] https://www.ideou.com/blogs/inspiration/from-design-thinking-to-creative-confidence

potencjalnych użytkowników rozwiązania w centrum. Efektem była zmiana sposobu postrzegania skanera rezonansu magnetycznego dla dzieci. Twórcy zaczęli myśleć nad nową wersją urządzenia razem z dziećmi i zrozumieli, że hałasy, sterylność i „bezosobowość" skanu jest bardzo stresująca dla małych pacjentów. Nie zmienili produktu, ale zmienili proces, który „otacza" produkt. Stworzyli scenariusze przygód, które dzieci mogą wybrać, a hałasy i konieczność pozostawania nieruchomo zamienili w zasady gry. Efektem, jaki uzyskali, stało się zmniejszenie liczby dzieci potrzebujących środków usypiających przed przystąpieniem do procedury medycznej.

ZROZUMIENIE POZYCJI INTERESARIUSZY

Każda innowacja powinna przynosić wymierne korzyści konkretnym grupom osób. W przypadku obszaru ochrony zdrowia sytuacja jest skomplikowana, ponieważ często znalezienie tylko jednej grupy stanowi wyzwanie.

Do powszechnie używanych modeli należy tzw. **model czterech „P"** (ang. 4P's – *patients, providers, payers, policymakers*) obejmujący:[316]

1. Pacjentów (ang. *patients*)
2. Dostarczycieli usług zdrowotnych (ang. *providers*)
3. Płatników (ang. *payers*)
4. Decydentów (ang. *policymakers*)

Jest on jednak niewystarczający do pełnego opisania poziomu skomplikowania i różnorodności interesariuszy w polskim systemie ochrony zdrowia. Bardziej rozbudowana lista zawiera:

1. Pacjentów – osoby, które są poddawane leczeniu w danej jednostce zdrowia
2. Opiekunów pacjentów – osoby, które odpowiadają prawnie za leczonych (np. rodzice)
3. Pracowników ochrony zdrowia – lekarzy, pielęgniarki i pozostały personel medyczny
4. Dyrektorów i kierowników lokalnych jednostek ochrony zdrowia
5. Płatnika – osobę bądź instytucję opłacającą opiekę zdrowotną
6. Decydentów – osoby lub instytucje wpływające na kształt polityki zdrowotnej lokalnie bądź na poziomie kraju.

Nie każda innowacja, którą wdrażamy, ma wpływ na wszystkich interesariuszy, ale za każdym razem, kiedy proponowane jest wprowadzenie nowego rozwiązania w zakresie medycyny, powinno się przygotować macierz interesariuszy. Taka macierz wskazuje, czyje potrzeby zaspokajamy, kogo trzeba informować oraz czyimi oczekiwaniami powinniśmy zarządzać (rysunek 19).[317]

[316] https://jln1.pressbooks.com/chapter/3-introducing-the-key-stakeholders-patients-providers-payors-and-policymakers-the-four-ps/

[317] https://i0.wp.com/kierownikprojektu.com/wp-content/uploads/2016/07/dfhgh.png?w=359&ssl=1

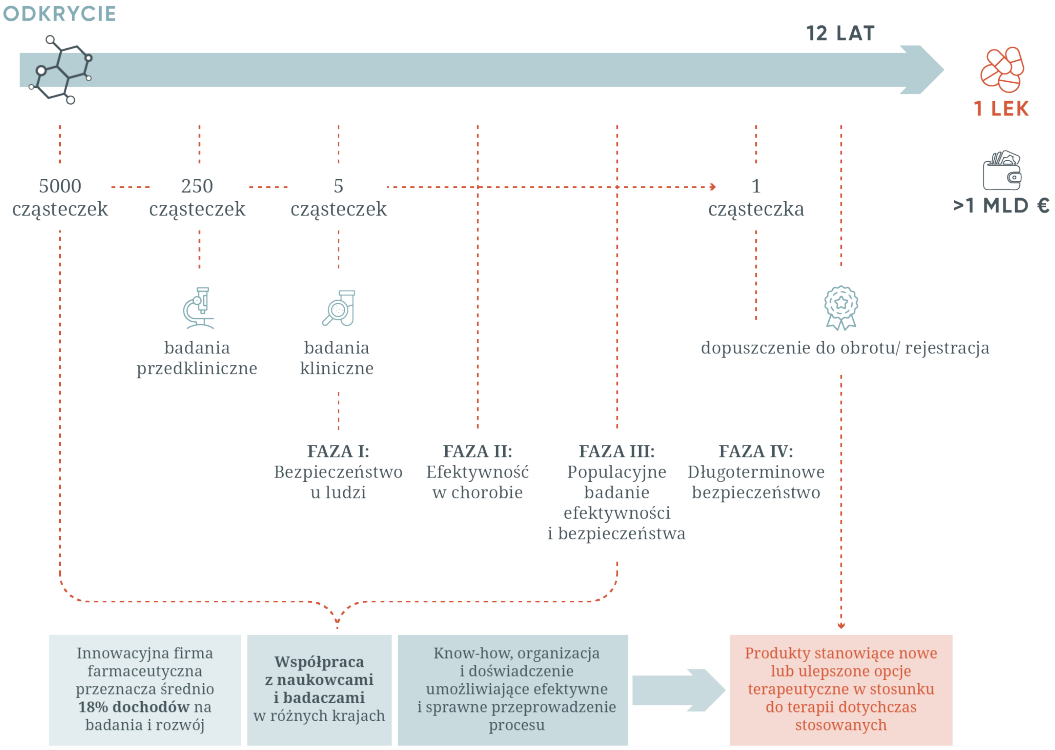
RYSUNEK 19. MACIERZ INTERESARIUSZY

BEZPIECZEŃSTWO ROZWIĄZAŃ CYFROWYCH

Innowacje w obszarze ochrony zdrowia tworzą pewnego rodzaju sprzeczność. Z jednej strony każda innowacja, zmiana i nowy projekt rodzą bardzo duże ryzyko błędów zarówno podczas wdrażania, jak i projektowania. Z drugiej, w przypadku ochrony zdrowia pojawia się konieczność myślenia o bezbłędnych, niezawodnych systemach, na szali jest w końcu życie ludzkie. Trudność połączenia dwóch światów – repetytywnego, pełnego błędów świata innowacji, oraz oprocesowanego, ustrukturyzowanego i bardzo bezpiecznego świata opieki zdrowotnej – widać w badaniach klinicznych nowych leków. Latami trwający, wieloetapowy proces zapewnia nam poczucie bezpieczeństwa, sądzimy, że stosowane medykamenty dają pozytywny efekt, bez (niewspółmiernie dużych) efektów ubocznych.

Klasycznie proces tworzenia nowego leku zajmuje od kilku do kilkunastu lat (rysunek 20).[318]

RYSUNEK 20. PROCES OPRACOWYWANIA NOWEGO, INNOWACYJNEGO LEKU



[318] https://www.eupati.eu/pl/opracowywanie-leku/tworzenie-lekow-etap-1-okres-poprzedzajacy-odkrycie-leku/

W przypadku innowacyjnych produktów cyfrowych taki okres jest nie do przyjęcia. Czas życia rozwiązania cyfrowego i jego rozwoju liczy się w miesiącach, więc próba zastosowania mechanizmów znanych z produkcji leków kończy się porażką.

Poza tym proces wytwarzania innowacyjnych rozwiązań cyfrowych w medycynie różni się od wytwarzania nowej cząsteczki aktywnej leku. Oba wymagają wielu danych i testów, ale warunki, w których omawiane testy mogą się odbywać, są różne:

1. Testy leków zaczynają się od badań laboratoryjnych, do których wybierane są najbardziej pozytywnie oddziałujące substancje. Testy wykonywane są na komórkach, a w fazach przedklinicznych – na zwierzętach. Po tym etapie selekcjonuje się grupę osób do badań klinicznych, z zachowaniem najwyższego rygoru obserwacji zgłaszających się ochotników.
2. Testy rozwiązań cyfrowych wykonywane są w zamkniętym środowisku zaangażowanej grupy osób oraz z potencjalnymi użytkownikami, najczęściej w formie badania przeprowadzanego wspólnie z dużą instytucją medyczno-naukową.

W związku z brakiem możliwości testowania rozwiązania na wcześniejszych (przedklinicznych) etapach poziom ryzyka związanego z włączeniem nowego rozwiązania jest wyższy. Nie należy również zapominać, że zdolności finansowe nowych firm technologicznych są zdecydowanie mniejsze niż przedsiębiorstw produkujących nowe leki, co wpływa na możliwości długiego i wieloetapowego testowania nowych rozwiązań cyfrowych.

Nie oznacza to, że rozwiązania cyfrowe są nieprzydatne lub nie powinny być używane. Wręcz odwrotnie – powinno się ustalić jasne zasady testowania produktów cyfrowych, które umożliwiłyby tworzenie bezpiecznych systemowych ram dla innowacyjnych rozwiązań w ochronie zdrowia. Dodając do tego punkty z poprzednich akapitów, można podsumować: dzięki budowaniu rozwiązań zorientowanych na użytkowników i zrozumieniu, których interesariuszy (i w jaki sposób) należy zaangażować do innowacyjnego rozwiązania cyfrowego, tworzymy podstawy opracowywania innowacji dla nowoczesnej, cyfrowej ochrony zdrowia.

Systemowe rozwiązania wspierające innowacyjność w zdrowiu

Cały świat rozumie potrzebę wdrażania rozwiązań cyfrowych, dlatego poszczególne kraje oraz instytucje europejskie starają się wdrożyć nowoczesne systemy innowacji również w ochronie zdrowia.

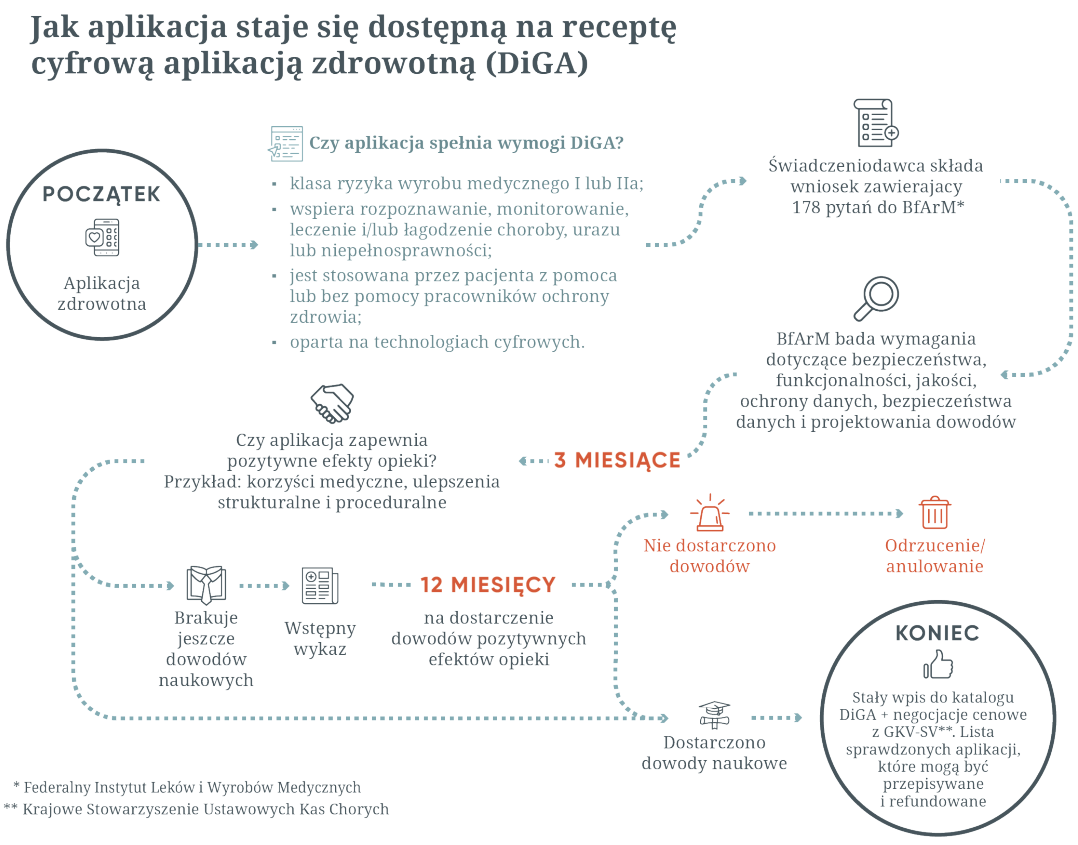
Obecnie w Polsce stoimy przed wyzwaniem stworzenia ram dla budowania i testowania nowoczesnych rozwiązań cyfrowych w zakresie ochrony zdrowia. W innym przypadku grozi nam ucieczka polskich rozwiązań na inne, bardziej przygotowane do wdrażania innowacji rynki. Warto inspirować się działaniami innych krajów oraz sektorów gospodarki w celu zbudowania systemowych rozwiązań wspierających innowacyjność w obszarze zdrowia.

Narodowe ramy prawno-instytucjonalne – przykład DiGA

Jednym z najczęściej przywoływanych przykładów dobrego podejścia do innowacji w ochronie zdrowia jest niemiecki system rozwiązań cyfrowych DiGA (niem. *Digitale Gesundheitsanwendung*), który umożliwia stosowanie (i finansowanie) rozwiązań oraz usług cyfrowych jako leczenia. W tym skomplikowanym procesie wykorzystuje się pracę lokalnej instytucji oceny technologii medycznych (BfArm) oraz wyniki badań naukowych oceniających skuteczność rozwiązania lub minimum rocznego badania udowadniającego skuteczność rozwiązania (rysunek 21).[319]

Zaletą tego rozwiązania jest skrócenie czasu wdrożenia i zaakceptowania rozwiązania cyfrowego z kilku lat do kilkunastu miesięcy, co dla wielu twórców

RYSUNEK 21. NIEMIECKI SYSTEM ROZWIĄZAŃ CYFROWYCH DIGA



[319] https://sidekickhealth.com/news/a-year-with-apps-on-prescription-in-germany/

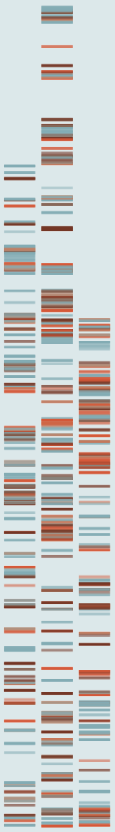
aplikacji i rozwiązań cyfrowych jest bardzo kuszące. Analizy efektywności DiGA wskazują bardzo pozytywny wpływ legislacji na pobudzenie rynku cyfrowego zdrowia, ale także braki w obecnym systemie[320]. Nie ulega jednak wątpliwości, że model jest ciekawy, więc inne kraje zastanawiają się nad wdrożeniem podobnych rozwiązań.

Stworzenie „piaskownicy" – bezpiecznego modelu testowania innowacji

Ciekawym i zdecydowanie potrzebnym rozwiązaniem dla polskiej służby zdrowia jest stworzenie „piaskownicy regulacyjnej" – modelu, który zezwalałby na przetestowanie nowoczesnych rozwiązań w zamkniętym środowisku pilotażowym, podobnie jak „piaskownica regulacyjna" Krajowego Nadzoru Finansowego dla firm zajmujących się bankowością. Oczywiście, należy zwrócić uwagę na dużo większy poziom skomplikowania takiego przedsięwzięcia jak piaskownica w ochronie zdrowia.

W przypadku ochrony zdrowia zamknięty, bezpieczny system, do którego mogłyby zgłosić się wybrane podmioty lecznicze, stanowiłby połączenie modelu oceny innowacji (jak w niemieckiej DiGA) ze stworzeniem fizyczno-digitalowej przestrzeni dla nowych rozwiązań (podobnej do „piaskownicy regulacyjnej" KNF). Zastosowanie takiego modelu, przy odpowiednim wyborze jednostek medycznych, osób odpowiedzialnych za pilotaże i kontrolę jakości, a także zamkniętych grup pacjentów, stworzyłoby równe szanse udowodnienia wartości dla wszystkich zainteresowanych twórców innowacyjnych rozwiązań.

[320] https://resource-allocation.biomedcentral.com/articles/10.1186/s12962-022-00359-y#Sec12



11

JACEK SZTAJNKE

Fundacja Parent Project Muscular Dystrophy

Paszport Pacjenta z chorobą rzadką

Pilotaż Paszportu Pacjenta to innowacyjny projekt adresowany do pacjentów z chorobami rzadkimi zrealizowany we współpracy z Centrum Chorób Rzadkich przy Uniwersyteckim Centrum Klinicznym Gdańskiego Uniwersytetu Medycznego oraz z organizacjami pacjenckimi. Paszport umożliwia szybki dostęp do skondensowanej informacji o stanie zdrowia pacjenta. Dostęp jest realizowany przy użyciu tagów NFC, które zawierają klucz dostępu do dokumentu elektronicznego, jakim jest paszport.

O chorobach rzadkich

Według definicji obowiązującej w UE, schorzenie uznaje się za chorobę rzadką, jeśli dotyka ona nie więcej niż 5 na 10 tys. osób. Dotychczas wykryto ponad 6 tys. rzadkich chorób. Uwzględniając krajowe dane demograficzne okazuje się, że na choroby rzadkie w Polsce cierpi od 2,3 do 3 mln osób.

Duża liczba jednostek chorobowych o różnych, często złożonych objawach i stosunkowo niewielka liczba pacjentów chorujących na każdą z nich powodują podstawowy problem jakim jest brak wiedzy o danej jednostce chorobowej wśród lekarzy i fizjoterapeutów.

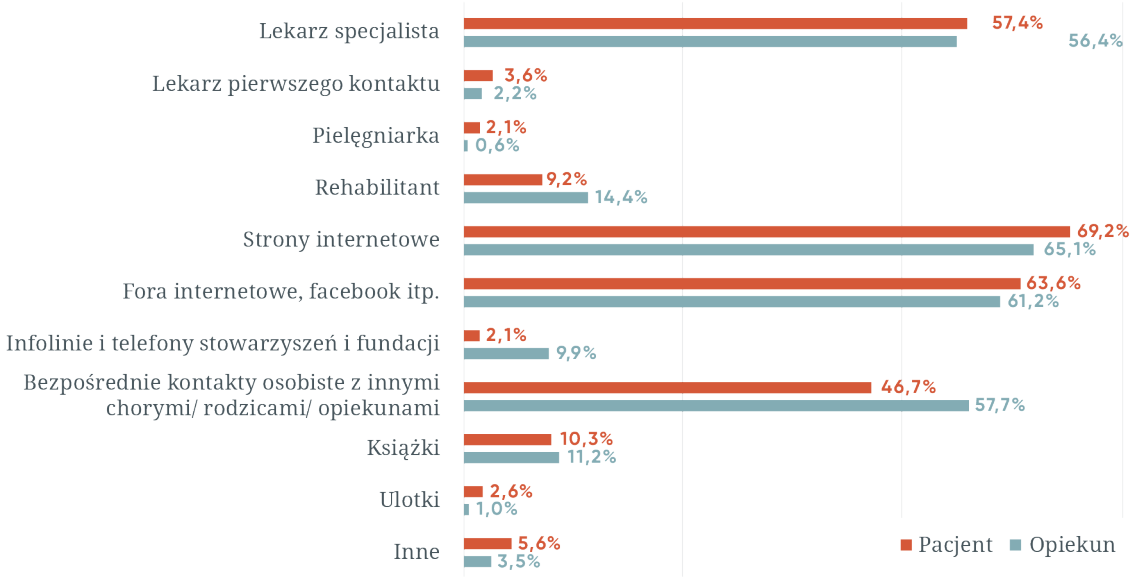
Problemem związanym z chorobami rzadkimi jest duża odległość od pacjentów do specjalistów zajmujących się ich jednostką chorobową. Pacjenci, jeżeli nawet są pod opieką specjalisty, często mają setki kilometrów do swojego ośrodka. Niemniej jednak są choroby, w których lekarzem koordynatorem powinien być ten będący blisko pacjenta, czyli rodzinny, a nie ten z centrum.

Większość chorób rzadkich ma przebieg ciężki, powodując przedwczesną śmierć pacjenta.

Skomplikowanej sytuacji w zakresie chorób rzadkich nie da się w obecnym, niewydolnym już, systemie opieki zdrowotnej. Konieczne jest innowacyjne podejście wykorzystujące nowe technologie umożliwiające dostęp do rozproszonych informacji o standardach leczenia oraz do danych zdrowotnych pacjenta. Jednak, aby rozwiązanie techniczne mogło zacząć poprawnie funkcjonować, niezbędna jest współpraca środowiska medycznego wyspecjalizowanego w chorobach rzadkich z organizacjami pacjenckimi, które zgodnie z raportem[321] mogą być cennym źródłem doświadczeń pacjentów (rysunek 22).

[321] M. Libura, M.Władysiuk. *Choroby rzadkie w Polsce. Stan obecny i perspektywy*, Uczelnia Łazarskiego, Warszawa 2016.

RYSUNEK 22. ŹRÓDŁA INFORMACJI O CHOROBIE RZADKIEJ – ODPOWIEDZI RESPONDENTÓW WEDŁUG RAPORTU[322]



Plan dla Chorób Rzadkich

Plan dla Chorób Rzadkich[323] opisuje Paszport Pacjenta z chorobą rzadką jako dokument elektroniczny udostępniony na IKP, zawierający informacje o procedurach leczenia, aktualne dane o historii choroby, leczeniu farmakologicznym i niefarmakologicznym, kartę postępowania w stanach zagrożenia życia itp. Dane zapisane w paszporcie będą dostępne dla właściwych służb medycznych – lekarzy, pielęgniarek, fizjoterapeutów, ratowników itp. W sytuacji zagrożenia życia posiadanie takiego dokumentu, przy pełnej dostępności placówek medycznych do systemów informatycznych, jest na miarę życia pacjenta.

Niestety, Plan dla Chorób Rzadkich to dla pacjentów wciąż przyszłość, rozwiązania w nim opisane jeszcze nie funkcjonują. System dla Chorób Rzadkich realizowany w Centrum e-Zdrowia jest nadal na etapie analizy.

Potrzebne jest rozwiązanie, które da się wdrożyć stosunkowo szybko.

---

[322] M. Libura, M.Władysiuk. *Choroby rzadkie w Polsce. Stan obecny i perspektywy*, Uczelnia Łazarskiego, Warszawa 2016.

[323] Plan dla Chorób Rzadkich, Uchwała nr 110 Rady Ministrów z 24 sierpnia 2021, Monitor Polski 2021, poz. 883

Pilotaż

Autorzy projektu pilotażu postawili sobie za cel stworzyć proste w użytkowaniu rozwiązanie, które umożliwi pacjentom dostęp do ich danych w dowolnym momencie. Pacjent powinien mieć możliwość udostępnienia danych lekarzowi w trakcie wizyty w ośrodku POZ. Rozwiązanie powinno również zapewniać korzystanie zdanych w sytuacji zagrożenia życia, gdy pacjent jest nieprzytomny.

Analiza możliwości technicznych wykazała, że najlepszym narzędziem będzie tag NFC jako nośnik elektronicznego klucza dostępowego do paszportu. Pacjent może nosić tag NFC w postaci plastikowej karty, opaski na rękę lub breloczka czy zawieszki na szyję. Rozwiązanie takie pozwala na rezygnację z autoryzacji użytkownika hasłem. Odczyt paszportu jest możliwy przez skanowanie smartfonem nośnika NFC.

Projekt otrzymał dofinansowanie z grantu udzielonego przez Inkubator Dostępności realizowany przez Regionalny Ośrodek Polityki Społecznej w Krakowie i Fundację Instytutu Rozwoju Regionalnego.

Przebieg projektu

Paszport Pacjenta to rozwiązanie informatyczne. Niezbędne było stworzenie systemu przechowującego dane o stanie zdrowia pacjenta zgodnie ze wszelkimi zasadami bezpieczeństwa teleinformatycznego. Ponieważ chodzi o rozwiązanie adresowane do osób z niepełnosprawnościami zespół jego twórców był zobowiązany również do zastosowania standardu dostępności WCAG 2.1. Po zaimplementowaniu zaplanowanych funkcji rozpoczęto testy.

Do testów zaproszono zespół medyczny pod kierownictwem prof. dr hab. n. med. Jolanty Wierzby oraz prof. dr hab.

RYSUNEK 23. TAGI NFC WYKORZYSTANE W PILOTAŻU PASZPORTU PACJENTA Z CHOROBĄ RZADKĄ

n. med. Roberta Śmigla oraz organizacje: Fundację Parent Project Muscular Dystrophy, Stowarzyszenie Marfan Polska oraz Stowarzyszenie zespołu Williamsa. Połączony zespół medyczno-pacjencki opracował szablony paszportów dla trzech chorób: dystrofii mięśniowych typu Duchenne'a, zespołu Marfana i zespołu Williamsa. Szablony zawierały podstawowe informacje opracowane na podstawie medycznych standardów postępowania. Szczególną uwagę zwrócono na opisy objawów, wyspecyfikowanie zaleceń, przeciwwskazań, niezalecanych leków oraz procedury ratunkowej. Szablony mają na celu skrócić proces wydawania paszportu pacjentowi. Lekarz wydając paszport wykorzystuje szablon z wstępnie przygotowanymi informacjami, które należy spersonalizować, tzn. uzupełnić o informacje dotyczące pacjenta, jego obecnego stanu, przyjmowanych leków itp. Dzięki szablonom możliwe jest wydanie paszportu zawierającego kompletne informacje o chorobie pacjenta w kilka minut podczas wizyty w gabinecie.

Rekrutację testerów przeprowadzono wśród pacjentów chorujących na wymienione choroby – dystrofię mięśniową Duchenne'a, zespół Marfana lub zespół Williamsa. Każdy z pacjentów-testerów otrzymał trzy nośniki – kartę plastikową, opaskę na rękę oraz breloczek, którymi mógł się posługiwać podczas wizyt w przychodniach, u fizjoterapeutów, w szkole i przedszkolu.

Po okresie testowym przeprowadzono ankiety i wywiady z pacjentami-testerami. Zebrane opinie wskazują, że jest to rozwiązanie bardzo potrzebne i oczekiwane przez pacjentów. Pacjenci podkreślają poczucie bezpieczeństwa wynikające już z samego faktu posiadania takiego paszportu, ale również użyteczność paszportu w kontakcie z lekarzami niebędącymi ekspertami w chorobach rzadkich. Dostrzeżono również potencjał tego rozwiązania, jako ratującego życie pacjenta w stanach zagrożenia spowodowanego chorobą rzadką. Pacjenci używający paszportu są przekonani, że opieka medyczna udzielana w placówkach POZ będzie bardziej dostosowana do ich potrzeb.

Podsumowanie

Zastosowanie innowacyjnych technologii zawsze wiąże się z ryzykiem, gdy koncepcja rozwiązania nie trafia w oczekiwania użytkowników. W przypadku projektów wdrażających innowacyjne rozwiązania warto stosować metody startupowe. Szczególnie istotne jest rozpoznanie potrzeb użytkowników, zdefiniowanie MVP, jako podstawowej wartości dostarczanej użytkownikom, oraz jak najbliższa współpraca z przedstawicielami grup użytkowników, aby zweryfikować, czy dostarczone rozwiązanie jest dobrze dopasowane do potrzeb. W przypadku projektów cyfryzacji w medycynie

użytkownikami najczęściej są pacjenci oraz kadra medyczna.

Sukces projektu pilotażu Paszportu Pacjenta przy ograniczonych środkach finansowych oparto na szczegółowym rozpoznaniu problemu, wąsko zdefiniowanej koncepcji rozwiązania i włączeniu przyszłych użytkowników w proces tworzenia i testowania. Dzięki temu potwierdzono, że użytkownicy potrzebują tego rozwiązania.

ZESPÓŁ STUDIÓW STRATEGICZNYCH
PRZY OIL W WARSZAWIE

ISBN 978-83-940620-7-1