

# Dane medyczne w pracy lekarza

stan obecny & pożądane zmiany



raport Sieci Lekarzy Innowatorów  
Naczelnej Izby Lekarskiej  
2023 rok

## Partner raportu

Sano - Centrum Zindywidualizowanej Medycyny Obliczeniowej  
Międzynarodowa Fundacja Badawcza



## Patronat honorowy



Ministerstwo  
Zdrowia

## Patroni



Polska Izba  
Informatyki Medycznej



## Lider projektu

**dr Paweł Kaźmierczyk**

kancelaria Domański Zakrzewski Palinka

## Autorzy

**dr Paweł Kaźmierczyk**

kancelaria Domański Zakrzewski Palinka

**dr Dagmara Lukosek**

kancelaria Domański Zakrzewski Palinka

**Michał Czarnuch**

kancelaria Domański Zakrzewski Palinka

**Aleksander Horyń**

kancelaria Domański Zakrzewski Palinka

## Konsultacja

**Jakub Chwiećko**

Partner Zarządzający, NIL IN

**Michał Gontkiewicz**

Przewodniczący Zespołu ds. E-zdrowia, NIL

**Michał Kozik**

Radca Prawny NIL

**Maja Więckiewicz**

Dyrektor Operacyjny, Sano – Centrum Zindywidualizowanej Medycyny Obliczeniowej -  
Międzynarodowa Fundacja Badawcza

**Wioletta Niwińska**

Legal Counsel, Sano – Centrum Zindywidualizowanej Medycyny Obliczeniowej -  
Międzynarodowa Fundacja Badawcza

**Piotr Nowakowski**

Scientific Programmers Manager, Sano – Centrum Zindywidualizowanej Medycyny  
Obliczeniowej - Międzynarodowa Fundacja Badawcza

**Michał Kosobudzki**

Inspektor Ochrony Danych, Sano – Centrum Zindywidualizowanej Medycyny  
Obliczeniowej - Międzynarodowa Fundacja Badawcza

**Dr hab. inż. Prof. AGH Maciej Malawski**

Prezes - Sano – Centrum Zindywidualizowanej Medycyny Obliczeniowej -  
Międzynarodowa Fundacja Badawcza

**Dariusz Adamusiński**

Dyrektor Zarządzający, MedTech Polska

**Katarzyna Starostawska**

Innovation Manager, IQVIA Commercial Poland

**Michał Zalewski**

Koordynator Projektów Analitycznych, Asseco Poland S.A.

**Jan Pachocki**

Prezes Zarządu, Fundacja Telemedyczna Grupa Robocza

**Andrzej Osuch**

Wiceprezes Zarządu, Fundacja Telemedyczna Grupa Robocza

**Roman Radomski**

Prezes Polskiego Stowarzyszenia HL7

**Tomasz Judycki**

Prezes Zarządu, Polska Izba Informatyki Medycznej

# Spis treści



<b>1. Podsumowanie</b>	<b>09</b>
1.1. Kluczowe wnioski i rekomendacje	09
1.1.1 Dane medyczne w pracy lekarza	09
1.1.2 Potrzebne zmiany o systemowych charakterze	10
1.1.3 Główne kierunki przyszłych zmian	11
1.1.4 Wyzwania związane z implementacją nadchodzących zmian prawnych	16
1.1.5 Wyzwania systemowe	18
<b>2. Wprowadzenie</b>	<b>23</b>
2.1 Dlaczego przygotowaliśmy raport?	23
2.2 Co zawiera raport i czemu ma służyć?	23
2.3 Kto przygotował raport?	25
<b>3. Dane medyczne – stan obecny i perspektywa zmian</b>	<b>27</b>
3.1 Wprowadzenie	27
3.2 Wybrane elementy stanu obecnego – punkt wyjścia w obszarze danych medycznych	28
3.2.1 Zarys podstaw prawnych systemu e-zdrowia w Polsce	28
3.2.2 Pojęcie danych medycznych	29
3.2.3 Podstawowe źródła danych medycznych	31
3.2.4 Zasady dostępu do danych medycznych	33
3.2.5 Główne gwarancje prawne jakości i interoperacyjności danych medycznych	34
3.2.6 Wymogi związane z bezpieczeństwem przetwarzania danych medycznych	35
3.3 Plany rozwoju obszaru danych medycznych w Unii Europejskiej i w Polsce	37
3.3.1 Wprowadzenie	37
3.3.2 Europejska strategia w zakresie danych	37
3.3.3 Krajowy Plan Odbudowy	38

3.3.4 Program rozwoju e-zdrowia w Polsce do 2027 r.	38
3.3.5 Polityka rozwoju sztucznej inteligencji w Polsce	41
3.4 Kolejny krok w kierunku otwartości danych – akt w sprawie zarządzania danymi	42
3.4.1 Podstawowa charakterystyka	42
3.4.2 Wybrane wyzwania	44
3.5 Jeszcze większy dostęp do danych – akt w sprawie danych	46
3.5.1 Podstawowa charakterystyka	46
3.5.2 Wybrane wyzwania	47
3.6 Zdrowie jako priorytet - europejska przestrzeń danych dotyczących zdrowia	49
3.6.1 Podstawowa charakterystyka	49
3.6.2 Wybrane wyzwania	50
3.7 Jakie inne regulacje wpłyną na obszar danych medycznych?	53
3.7.1 AI Act - podstawowa charakterystyka	53
3.7.2 Regulacje krajowe – ustawa o jakości w opiece zdrowotnej i bezpieczeństwie pacjenta	56
<b>4. Dane medyczne w pracy lekarza – jak być powinno?</b>	<b>57</b>
4.1 Świadomość	57
4.2 Dostępność	58
4.3 Funkcjonalność	58
4.4 Bezpieczeństwo	59
4.5 Rozwój	60
<b>5. Kluczowe wyzwania i kierunki potencjalnych zmian</b>	<b>61</b>
5.1 Wprowadzenie	61
5.2 Dostęp do danych	61
5.2.1 Zakres danych medycznych dostępnych dla lekarza	61
5.2.2 Zasady dostępu lekarzy do danych przetwarzanych w podmiotach leczniczych	74
5.3 Postępowanie z danymi medycznymi	79

5.3.1	Podejście oparte o dane	79
5.3.2	Bezpieczeństwo przetwarzania	85
5.3.3	Narzędzia wykorzystywane do przetwarzania danych medycznych	90
5.3.4	Jakość danych- jakość leczenia	95
5.3.5	Udostępnianie danych	104
5.3.6	Udostępnienia i przetwarzanie danych w celach naukowych	113
5.3.7	Dopuszczalność ograniczenia RODO	120

# Wykaz używanych skrótów



## Akty prawa UE<sup>1</sup>

1. **AI Act** – projekt Rozporządzenia Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii<sup>2</sup>. Projekt aktu prawnego jest przedmiotem dalszych prac legislacyjnych;
2. **DA** – projekt Rozporządzenia Parlamentu Europejskiego i Rady w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania (akt w sprawie danych)<sup>3</sup>. Projekt aktu prawnego jest przedmiotem dalszych prac legislacyjnych;
3. **DGA** - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z dnia 30 maja 2022 r. w sprawie europejskiego zarządzania danymi i zmieniające rozporządzenie (UE) 2018/1724 (akt w sprawie zarządzania danymi)<sup>4</sup>. Projekt aktu prawnego jest przedmiotem dalszych prac legislacyjnych;
4. **EHDS** – projekt Rozporządzenia Parlamentu Europejskiego i Rady w sprawie europejskiej przestrzeni danych dotyczących zdrowia<sup>5</sup>. Projekt aktu prawnego jest przedmiotem dalszych prac legislacyjnych;
5. **RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.)<sup>6</sup>;

## Akty prawa krajowego<sup>1</sup>

6. **BadKlinU** - Ustawa z dnia 9 marca 2023 r. o badaniach klinicznych produktów leczniczych stosowanych u ludzi (Dz. U. poz. 605);
7. **DokMedR** - Rozporządzenie Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (t.j. Dz. U. z 2022 r. poz. 1304 z późn. zm.);
8. **JakZdrU** - Ustawa z dnia 16 czerwca 2023 r. o jakości w opiece zdrowotnej i bezpieczeństwie pacjenta (Dz.U. z 2023 r. poz. 1692);
9. **KrSystCyberU** - Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2023 r. poz. 913);

1. Zaznaczamy, że część ze wskazanych aktów prawnych w momencie powstania dokumentu była na etapie procesu legislacyjnego a i nie stanowiła jeszcze obowiązującego prawa. Na potrzeby raportu uwzględniono je w analizie w najbardziej aktualnej wersji na dzień opracowania raportu.

2. <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52021PC0206>

3. <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52022PC0068>

4. <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32022R0868>

5. <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52022PC0197>

6. <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016R0679>

10. **OtwDanU** - Ustawa z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. poz. 1641 z późn. zm.);
11. **PrPacjU** - Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzecznik Praw Pacjenta (t.j. Dz. U. z 2022 r. poz. 1876 z późn. zm.);
12. **SystInformOchrU** - Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (t.j. Dz. U. z 2022 r. poz. 1555 z późn. zm.);
13. **ŚOZŚrPubU** - Ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (t.j. Dz. U. z 2022 r. poz. 2561 z późn. zm.);
14. **ZarządDanU** - Projekt ustawy o zarządzaniu danymi (UC146);

## Inne

1. **AOTMIT** - Agencja Oceny Technologii Medycznych i Taryfikacji
2. **EROD** - Europejska Rada Ochrony Danych
3. **ISO** - Międzynarodowa Organizacja Normalizacyjna
4. **NFZ** - Narodowy Fundusz Zdrowia
5. **NIK** - Najwyższa Izba Kontroli
6. **NIL** - Naczelna Izba Lekarska
7. **NIL IN** - Sieć Lekarzy Innowatorów
8. **PUODO** - Prezes Urzędu Ochrony Danych Osobowych

## Zastrzeżenia

1. Raport należy traktować przede wszystkim jako analizę o charakterze prawnym. Nie jest to analiza medyczna, techniczna, ani informatyczna. Przedstawione w raporcie zagadnienia zostały wskazane w celach informacyjnych, na potrzeby dalszej, ustrukturyzowanej dyskusji.
2. Raport nie wyczerpuje tematu danych medycznych. Zawiera zwięzłe przedstawienie wybranych, kluczowych wyzwań w tym zakresie, które powinny być dalej rozwijane w interdyscyplinarnym gronie ekspertów w celu wypracowania optymalnych rozwiązań. Jako taki podejmuje próbę wskazania głównych nurtów i podstawowych tematów do dalszej dyskusji.
3. W momencie powstawania raportu część przywoływanych w jego treści aktów prawnych wciąż znajdowała się na etapie procesu legislacyjnego. Na potrzeby prac na raporcie uwzględniono ich najbardziej aktualną wersję. Wnioski wynikające z analizy należy skonfrontować z finalną treścią przyjętych w przyszłości aktów prawnych.
4. W zakresie omawianych aktów normatywnych, raport został opracowany na podstawie stanu prawnego obowiązującego w Polsce w dniu 16 października 2023 r., z zastrzeżeniem faktu, iż część przepisów znajdowała się na etapie procedowania i ich ostateczny kształt mógł ulec zmianie.



# 1. Podsumowanie



## 1.1 Kluczowe wnioski i rekomendacje

### 1.1.1 Dane medyczne w pracy lekarza

- W polskim systemie e-zdrowia działają podstawowe systemy umożliwiające gromadzenie i wykorzystywanie danych medycznych, które usprawniają proces opieki nad pacjentem i wspomagają lekarzy w ich pracy. Planowany jest ich dalszy rozwój, a więc coraz więcej danych medycznych będzie dostępnych w formie cyfrowej.
- Projektując kolejne rozwiązania dotyczące obszaru danych medycznych należy pamiętać, że **jednym z ich głównych odbiorców jest lekarz**<sup>7</sup>, który wykorzystuje je w codziennej pracy z pacjentem. Dalsze działania w tym zakresie powinny uwzględniać podstawowe wartości: dostępność, jakość i funkcjonalność, bezpieczeństwo, rozwój i świadomość.
  - **Dostępność** - lekarz powinien mieć łatwy i szybki dostęp do danych pacjentów pochodzących z różnych źródeł, w tym m.in. danych z innych podmiotów wykonujących działalność leczniczą, systemu centralnego (tzw. systemu P1), wyrobów medycznych.
  - **Jakość i funkcjonalność** - lekarz powinien móc w ergonomiczny sposób korzystać z danych, a także aplikacji i programów, które pomogą mu łatwo zebrać w jednym miejscu, przeanalizować oraz wykorzystać wysokiej jakości dane w procesie opieki nad pacjentem. Dokumenty i systemy IT stosowane w ochronie zdrowia powinny cechować się interoperacyjnością.
  - **Bezpieczeństwo** - lekarz powinien mieć dostęp do narzędzi, które zapewniają bezpieczeństwo korzystania z danych. Ważna jest kategoryzacja danych medycznych pod kątem ich jakości i wiarygodności.
  - **Rozwój** - lekarz powinien móc wykorzystać dane medyczne w celach naukowych i badawczych.
  - **Świadomość** - lekarz powinien mieć świadomość, jakie możliwości stwarzają dane i jaki jest ich potencjał.

7. Raport prezentuje temat pod kątem potrzeb i wyzwań dla wykonywania zawodu lekarza i lekarza dentystry, jednak zawarte w nim oceny i propozycje pozostają aktualne także pod kątem innych zawodów medycznych.

### 1.1.2 Potrzebne zmiany o systemowym charakterze

- Aby zrealizować postulaty związane z kierunkami rozwoju obszaru danych medycznych, które uwzględnić będą rolę lekarza jako jednego z kluczowych odbiorców danych, **potrzebne są zmiany o systemowym charakterze.**
- Program rozwoju e-zdrowia w Polsce do 2027 r. oraz Krajowy Plan Odbudowy i Zwiększania Odporności (KPO) przewiduje konkretne cele związane z danymi medycznymi. Plany związane z tym obszarem ma także Unia Europejska. Kluczową rolę odgrywa w nich projekt rozporządzenia w sprawie europejskiej przestrzeni danych dotyczących zdrowia (European Health Data Space), który zawierać będzie nowe wymogi związane z pierwotnym i wtórnym przetwarzaniem danych medycznych. **Najbliższe lata będą okresem wypracowywania wspólnego podejścia do wykorzystywania danych na poziomie UE, w tym danych medycznych, które obowiązywać będzie także Polskę.**
- Z uwagi na poziom skomplikowania tego obszaru, a zarazem jego ogromny potencjał, zasadne jest **wyodrębnienie go jako dedykowanego obszaru polityki publicznej w ochronie zdrowia,** a także zapewnienie spójności z innymi politykami publicznymi pod kątem wykorzystywania danych w celach naukowych.
- Mając na uwadze dużą dynamikę zmian związanych z obszarem technologii, które wptywają także na kwestie związane z przetwarzaniem danych, a także perspektywę szeregu zmian na poziomie Unii Europejskiej, **zasadne jest wyodrębnienie dedykowanego zespołu ds. danych medycznych** jako organu doradczo-opiniotawczego dla Rady Ministrów. Zespół powinien mieć charakter międzyresortowy, w jego skład powinni wchodzić co najmniej przedstawiciele ministra właściwego do spraw zdrowia (przy czym to właśnie Ministerstwo Zdrowia powinno pełnić kluczową, lidorską rolę w pracach zespołu i nadawać im tok), ministra właściwego do spraw informatyzacji, ministra właściwego do spraw szkolnictwa wyższego i nauki, a także reprezentanci samorządów zawodów medycznych, towarzystw naukowych, organizacji pacjenckich, organizacji zajmujących się cyberbezpieczeństwem i ochroną danych osobowych, a także innych organizacji branżowych, które dzięki swoim doświadczeniom będą w stanie wspomóc pracę grupy w zakresie wykorzystywania nowych technologii.
- Potrzebne jest przygotowanie kompleksowego **planu dalszego rozwoju systemu gromadzenia i wykorzystywania danych medycznych** uwzględniającego cały szereg zagadnień i uwarunkowań prawnych i technologicznych związanych z tym obszarem. Zadaniem zespołu ds. danych medycznych byłoby opracowanie planu oraz stały nadzór nad jego realizacją oraz potrzebą adaptacji do nowych uwarunkowań prawnych i faktycznych.
- Kluczowym zadaniem jest zapowiadane w Programie rozwoju e-zdrowia w Polsce do 2027 r. przygotowanie **ustawy o danych medycznych** regulującej cały obszar danych medycznych i dokumentacji medycznej w jednym akcie prawnym. Ustawa powinna uwzględnić i adresować co najmniej kwestie, które zostały wskazane w raporcie jako priorytetowe.

### 1.1.3 Główne kierunki przyszłych zmian

- **Rozwój systemu przetwarzania danych medycznych jest złożonym zagadnieniem**, które wymaga szeregu szczegółowych zmian oraz uwzględnienia takich kwestii jak:
  - jakość danych,
  - zapewnienie interoperacyjności,
  - możliwość i warunki dostępu dla lekarzy i szeregu interesariuszy przy zachowaniu ich poufnego charakteru,
  - gwarancja wysokiego poziomu ochrony i cyberbezpieczeństwa,
  - stworzenie zachęt i ułatwień związanych z badaniami naukowymi oraz pracami badawczo-rozwojowymi opartymi o wykorzystanie danych.

#### 1.1.3.1 Obszar dostępności

- **Potrzebne jest zapewnienie kompletności danych pacjenta** w środowisku cyfrowym w procesie opieki medycznej, co przyjmując obecną architekturę systemu e-zdrowia, oznacza w pierwszej kolejności pełność wymaganego zestawu danych przetwarzanych w systemie centralnym (Platforma P1)<sup>8</sup>. Należy **zwiększyć zakres dokumentacji medycznej prowadzonej w postaci elektronicznej**. W pierwszej kolejności konieczne jest zapewnienie przestrzegania już obowiązujących wymogów w tym zakresie. Okazją do dalszej poprawy sytuacji jest np. ustawa o jakości w opiece zdrowotnej i bezpieczeństwie pacjenta, która umożliwia włączenie dodatkowych, nowych wymogów do standardów akredytacyjnych. Mając na uwadze rosnącą skalę cyfryzacji należy pamiętać o konieczności zapewnienia adekwatnych możliwości technicznych, w tym przestrzeni do koniecznej do zapisywania danych, co stanowić będzie wyzwania np. w kontekście danych obrazowych.
- Lekarz powinien mieć zapewniony **dostęp do tak gromadzonych danych i dokumentów medycznych pacjentów, którym udziela świadczeń zdrowotnych**. Zasadne jest przeprowadzenie szerszej społecznej dyskusji na temat modelu dostępu lekarza do danych pacjenta. Potencjalnie możliwe jest przyjęcie różnych rozwiązań, w szczególności modelu opartego o zgodę pacjenta (tzw. model opt-in) lub modelu zakładającego domyślny dostęp z możliwością zgłoszenia sprzeciwu przez pacjenta (tzw. model opt-out). Możliwe jest także przyjęcie rozwiązań, w których łączy się różne modele, a część lekarzy ma z mocy prawa zapewniony bezwzględny dostęp do danych. Niezależnie od przyjętego modelu, pacjent powinien mieć możliwość uzyskania informacji na temat tego, kto i kiedy miał dostęp do jego danych<sup>9</sup>. Z związku z tym potrzebny jest jasny standard dostępu lekarza do różnych zbiorów danych oraz wsparcie w dostępie do danych przetwarzanych w różnych systemach IT.

8. Związany z tym zagadnieniem jest architektura systemu e-zdrowia. Dostęp do danych i dokumentów może być realizowany przez systemy centralne (np. e-recepta), jak i wymogi oraz standardy zapewniające integrację w modelu rozproszonym. Kierunki rozwoju centralnych systemów e-zdrowia mogą być dyskusyjne, podobnie jak praktyczna przydatność części z nich dla poprawy systemu ochrony zdrowia. Podstawowym zagadnieniem jest budowanie systemów centralnych jako zamkniętych rozwiązań zamiast udostępniania usług aplikacyjnych, z których mogą korzystać systemy lokalne.

W raporcie skupiamy się jednak na pożądanym z punktu widzenia lekarza efekcie działania takiego systemu, niezależnie od przyjętej architektury, której kształt powinien być przedmiotem osobnej dyskusji. Z uwagi na praktyczne znaczenie w codziennej pracy lekarza, w ramach raportu przedstawiliśmy uwagi i rekomendacje odnoszące się jedynie do już funkcjonujących systemów i rozwiązań oraz ewentualnych zmian związanych z ich rozwojem.

9. W świetle wyjaśnień Ministerstwa Zdrowia, funkcjonalność taka działa już w IKP.

- **Uporządkowanie i standaryzacja zasad dostępu do danych medycznych**, możliwie w ramach jednej ustawy. Nowy system powinien opierać się na siatce pojęciowej i zasadach, które wynikać będą z ostatecznie przyjętej wersji EHDS.
- Należy przy tym ustanowić na poziomie ustawowym jasne i wyraźne cele przetwarzania danych medycznych w systemach administrowanych przez stronę publiczną oraz związane z nimi funkcjonalnie **zasady dostępu do poszczególnych zbiorów danych przez organy władzy publicznej**. Nie powinno dochodzić do sytuacji, w których dostęp do danych jest nadużywany, a dane medyczne wykorzystywane są niezgodnie z ich ustawowym przeznaczeniem. Aby mieć możliwość kontroli w tym zakresie, potrzebne jest powołanie funkcji niezależnego pełnomocnika do spraw kontroli przetwarzania danych, który otrzymałby uprawnienia kontrolne oraz obowiązek przedstawiania publicznie dostępnych sprawozdań. Naruszenia w tym zakresie powinny być zagrożone dedykowanymi sankcjami.
- Należy rozpocząć dyskusję nad **powołaniem krajowego podmiotu odpowiedzialnego za przyznawanie dostępu do danych medycznych**. Powinien być on niezależny oraz mieć możliwości techniczne i organizacyjne umożliwiające pełnienie jego zadań.
- **Zwiększenie interoperacyjności dokumentacji medycznej** poprzez zapewnienie przestrzegania już obowiązujących wymogów w tym zakresie<sup>10</sup>, dalszy rozwój i scalenie standardów takich jak Polska Implementacja Krajowa HL7 CDA, jasne zasady publikacji obowiązujących standardów oraz dokonywania ich zmian, a także oraz określenie ram prawnych zapewniających utrzymanie specyfikacji interoperacyjności oraz otwartość interfejsów komunikacyjnych dla dostawców oprogramowania. Wymogi na rzecz wysokiej jakości standardów, w tym ewentualnych przyszłych zmian wynikających z EHDS, powinny zostać włączone do systemu jakości wynikającego z ustawy o jakości w opiece zdrowotnej i bezpieczeństwie pacjenta, np. jako element fakultatywnego systemu akredytacji. Ponadto, warto rozważyć rozbudowę istniejącego modelu danych medycznych w systemie P1 opartego na standardzie HL7 FHIR. Systemy takie jak np. LOINC<sup>11</sup> będą mogły wspierać zbieranie informacji – w przypadku przywołanego systemu o badaniach diagnostycznych - z wielu miejsc, gdzie były one zlecone, co pozwoli lekarzowi na uzyskanie szerszej wiedzy o sytuacji pacjenta.
- Wypracowanie **standardów dotyczących anonimizacji i pseudonimizacji danych medycznych** poprzez przyjęcie dedykowanych regulacji prawnych lub jasnego standardu w zakresie przeprowadzenia anonimizacji i pseudonimizacji danych medycznych.

10. Przykładowo, zgodnie z art. 8b SystInformOchrU podmioty wykonujące działalność leczniczą i podmioty prowadzące rejestry medyczne są obowiązane zapewniać zgodność swoich systemów teleinformatycznych z minimalnymi wymaganiami technicznymi i funkcjonalnymi zamieszczonymi w Biuletynie Informacji Publicznej ministra właściwego do spraw zdrowia, w terminie 9 miesięcy od dnia ich zamieszczenia. Dalsze wymogi z tym związane zostały przedstawione w dalszej części raportu.

11. LOINC jest bazą danych, która udostępnia uniwersalny system kodowania dla raportowania obserwacji medycznych. Dla każdej obserwacji baza danych zawiera kod, długą nazwę formalną, krótką 30-znakową nazwę oraz synonimy. Klasyfikacja w swoim kodowaniu łączy nie tylko typ, ale również określa inne wymiary np. miejsce powstania dokumentacji, autora itp.

Źródło: <https://ezdrowie.gov.pl/portal/home/interoperacyjnosc/klasyfikacje?modSingleId=80521>

### 1.1.3.2 Obszar jakości i funkcjonalności

- Zasadne jest odejście od podejścia opartego na pojęciu dokumentacji medycznej na rzecz **podejścia opartego o dane medyczne** - dostosowanie dotychczasowych oraz nowych zasad do podejścia prezentowanego w EHDS, które skupia się na danych. Kluczowe pod kątem zasad dostępu i wykorzystywania tych danych jest rozróżnienie zbiorów danych osobowych i nieosobowych.
- Wypracowanie **zasad postępowania z danymi generowanymi poza kontrolą lekarza** (lub podmiotu wykonującego działalność leczniczą), np. przez zdalne wyroby medyczne lub inne rozwiązania IT niebędące wyrobami medycznymi, np. aplikacje lifestylowe. Możliwe jest przyjęcie wytycznych i rekomendacji w tym zakresie, a docelowo - wprowadzenie wzorem EHDS znakowania zbiorów danych pod kątem ich jakości, wiarygodności i użyteczności.
- Przyjęcie wymogów dotyczących otwartych interfejsów umożliwiających pracę lekarza tylko na jednym systemie informatycznym (**zasada jednego konta**), z którego będzie w stanie przysyłać dane do innych systemów i realizować obowiązki sprawozdawcze, tzw. **zasada jednej klawiatury**.
- Zapewnienie **możliwości lub ułatwień wykorzystywania rozwiązań uprawniających pracę z danymi medycznymi**, w tym w szczególności pracę z danymi w czasie rzeczywistym. W tym celu zasadne jest ujednoczenie regulacji dotyczących zasad przetwarzania danych medycznych i przechowywania dokumentacji medycznej w chmurze przez różne kategorie podmiotów leczniczych, zaadresowanie podstawowych pytań i wątpliwości związanych ze stosowaniem nowych technologii w ochronie zdrowia, takich jak np. AI, w formie wytycznych i rekomendacji, wypracowanie kryteriów jakości danych medycznych uwzględniających ich kluczowe cechy takie jak wiarygodność, aktualność, kompletność i interoperacyjność oraz włączenie ich do systemu jakości wynikającego z ustawy o jakości w opiece zdrowotnej i bezpieczeństwie pacjenta, np. jako element fakultatywnego systemu akredytacji.
- Stworzenie standardu dla opracowywania **planów zarządzania danymi** (Data Management Plans), które wspierać będą procesy gromadzenia wysokiej jakości danych medycznych oraz ich wykorzystywania w praktyce.
- Zapewnienie **systemowego podejścia do rozwoju rejestrów medycznych** poprzez powołanie specjalnej rady ds. rejestrów, która wyznaczy strategiczny plan rozwoju systemu rejestrów medycznych, a także wprowadzenie środków technicznych i organizacyjnych służących ułatwieniu i automatyzacji przekazania danych do rejestrów medycznych, mechanizmów dodatkowego premiowania świadczeniodawców za wywiązywanie się ze związanych z tym obowiązków, a także zliberalizowanie zasad ich tworzenia, prowadzenia i finansowania rejestrów.

### 1.1.3.3 Obszar bezpieczeństwa

- Konieczne jest spełnienie przez podmioty udzielające świadczeń zdrowotnych wymogów niezbędnych dla zapewnienia wysokiego poziomu ochrony danych o stanie zdrowia. Kluczowe pod tym kątem jest **kontynuowanie programów wsparcia finansowego**, które byłyby dedykowane zakupom towarów i usług związanych z ochroną danych medycznych oraz **zrealizowanie działań w obszarze bezpieczeństwa** takich jak te przewidziane w Programie rozwoju e-zdrowia w Polsce do 2027 r.
- **Aktywności edukacyjne skierowane do pacjenta** i przewidziane w Programie rozwoju e-zdrowia w Polsce do 2027 r. powinny zawierać komponent dotyczący podstawowych zasad z zakresu cyberbezpieczeństwa. Warto uzupełnić je o kampanię informacyjną, która promować będzie korzystanie z bezpiecznych narzędzi przy korzystaniu z teleporad, logowaniu się na IKP lub inne serwisy, w tym konta pocztowe, w których dostępne są dane o stanie zdrowia przy zachowaniu zasad ich poufności.
- Doprecyzowanie wymogów związanych z zawieraniem **umów powierzenia przetwarzania danych osobowych** z podmiotami wykonującymi działalność leczniczą oraz wskazanie uznanych sposobów realizacji zasad ogólnych dotyczących przetwarzania danych osobowych, co najmniej w formie rekomendacji lub wytycznych.

### 1.1.3.4 Obszar rozwoju

- **Doprecyzowanie przesłanek udostępniania dokumentacji medycznej i danych medycznych w celach naukowych i badawczo-rozwojowych** tak, by nie budziły one wątpliwości pod kątem RODO, oraz dostosowanie katalogu podmiotów, które mogą ją uzyskać, do katalogu podmiotów uprawnionych do dostępu do danych wynikającego z DGA oraz finalnie z EHDS. Zasady dostępu powinny przewidywać możliwość uzyskania danych w różnej postaci, tj. danych anonimowych, danych spseudonimizowanych, a także danych umożliwiających identyfikację osoby, której dotyczą (jeżeli np. są udostępniane w takiej postaci za jej świadomą zgodą). Wraz ze wzrostem możliwości dostępu do danych potrzebne są mechanizmy ich ochrony przed nadużyciami w tym zakresie lub próbami nieuprawnionego dostępu.
- Ograniczenie pozostałych wątpliwości interpretacyjnych występujących w tym obszarze na gruncie RODO poprzez opracowanie wytycznych, które udzielać będą praktycznych wskazówek jak dokładnie należy **postępować przy przetwarzaniu danych medycznych w celach naukowych i badawczo-rozwojowych**, tj. jakie podstawy stosować i jakie wymogi spełnić. Zasadne jest także utworzenie ram prawnych dotyczących przetwarzania danych osobowych w celach badawczych, by poszerzyć możliwość wykorzystywania art. 9 ust. 2 lit. j RODO<sup>12</sup>, czyli niezbędności przetwarzania do celów badań naukowych, jako podstawy prawnej.

12. Potencjalnie też art. 9 ust. 2 lit. i RODO, czyli interes publiczny w dziedzinie zdrowia publicznego.

- Standaryzacja zasad postępowania z danymi uczestników badań klinicznych poprzez przyjęcie wytycznych, które wskazywać będą, przy spełnieniu jakich warunków lekarz jako badacz powinien pełnić rolę administratora danych, współadministratora lub podmiotu przetwarzającego. Wytyczne powinny też wskazywać, jakie mogą być podstawy prawne przetwarzania danych przez badacza będącego administratorem lub współadministratorem danych. Ponadto, wypracowanie wytycznych w zakresie postępowania z danymi osobowymi w przypadku, gdy badacz będzie dokonywał badania dla własnych celów.

#### 1.1.3.5 Obszar świadomości

- Lekarz powinien być **dobrze przygotowany do postępowania z danymi medycznymi**. Zasadne jest dokonanie rewizji programów edukacyjnych uczelni wyższych oraz promowanie kształcenia w zakresie e-zdrowia. Działania edukacyjne podejmowane przez Centrum e-Zdrowia powinny obejmować zwrócenie uwagi na szczególną rolę danych medycznych oraz podstawowe zasady postępowania z nimi.

## 1.1.4 Wyzwania związane z implementacją nadchodzących zmian prawnych

Poniższa tabela przedstawia kluczowe dla dalszego rozwoju obszaru danych medycznych akty prawne, w tym projekty aktów prawnych, a także związane z nimi główne wyzwania.

Prezentuje też kierunkowe propozycje działań.

Akt prawny	Status prac	Wybrane wyzwania	Pożądane działania	Pkt. raportu
Akt w sprawie zarządzania danymi <sup>13</sup>	Stosowany od 24 września 2023 r.	Zapewnienie sprawnego systemu udostępniania danych medycznych w trybie DGA	<ul style="list-style-type: none"> <li>• Przyjęcie krajowej ustawy o zarządzaniu danymi.</li> <li>• Powołanie sektorowego podmiotu odpowiedzialnego za dostęp do danych medycznych.</li> <li>• Wypracowanie standardów przygotowania danych medycznych do udostępnienia w trybie DGA, w tym ich anonimizacji.</li> </ul>	3.4.2.1
		Wykorzystanie nowych ram regulacyjnych usług pośrednictwa danych oraz altruizmu danych	<ul style="list-style-type: none"> <li>• Promowanie usług pośrednictwa danych medycznych i altruistycznego podejścia do danych w ochronie zdrowia.</li> <li>• Budowanie świadomości pacjentów na temat znaczenia dawstwa danych.</li> </ul>	3.4.2.2
Akt w sprawie danych <sup>14</sup>	Projekt	Identyfikacja i wykorzystanie nowych możliwości w ochronie zdrowia	<ul style="list-style-type: none"> <li>• Identyfikacja szans związanych z szerszym dostępem do nowych kategorii danych, które dotąd mogły nie być szerzej wykorzystywane.</li> <li>• Stworzenie standardów dostępu do surowych danych medycznych lub innych danych generowanych przez wyroby medyczne lub aplikacje prozdrowotne.</li> </ul>	3.5.2.1
		Dostęp władzy publicznej do danych pacjentów	<ul style="list-style-type: none"> <li>• Wypracowanie standardu dostępu władzy publicznej do danych medycznych w uzasadnionych sytuacjach.</li> </ul>	3.5.2.2
Rozporządzenie w sprawie europejskiej przestrzeni danych dotyczących zdrowia <sup>15</sup>	Projekt	Nowe podejście do definicji danych medycznych	<ul style="list-style-type: none"> <li>• Zapowiadana w Programie rozwoju e-zdrowia w Polsce do 2027 r. ustawa o danych medycznych powinna opierać nowy system na pojęciu danych medycznych, a nie dokumentacji medycznej.</li> <li>• Dostosowanie siatki pojęciowej do definicji wprowadzanych przez EHDS.</li> </ul>	3.6.2.1
		Zmiana modelu dostępu lekarza do danych	<ul style="list-style-type: none"> <li>• Oparcie zasad dostępu lekarza do danych medycznych pacjentów na wypracowanym w toku konsultacji publicznych modelu</li> </ul>	3.6.2.1

14. Wniosek - rozporządzenie Parlamentu Europejskiego i Rady w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania (akt w sprawie danych), COM/2022/68 final.

15. Wniosek - rozporządzenie Parlamentu Europejskiego i Rady w sprawie europejskiej przestrzeni danych dotyczących zdrowia, COM/2022/197 final.



Akt prawny	Status prac	Wybrane wyzwania	Pożądane działania	Pkt. raportu
		Dostosowanie EDM i IKP do wymogów EHDS	<ul style="list-style-type: none"> <li>Wdrożenie zmian w zakresie EDM oraz funkcji IKP w celu spełnienia wymaganego przez EHDS standardu</li> </ul>	3.6.2.2
		Zapewnienie wtórnego wykorzystania danych	<ul style="list-style-type: none"> <li>Wypracowanie standardu wtórnego wykorzystania danych medycznych, w tym ich anonimizacji i pseudonimizacji</li> </ul>	3.6.2.3
AI Act <sup>16</sup>	Projekt	Stworzenie przyjaznych warunków do rozwoju AI	<ul style="list-style-type: none"> <li>Wykorzystanie „piaskownic regulacyjnych” do wspierania rozwoju AI w ochronie zdrowia</li> </ul>	3.7.1.2
		Kategoryzacja zbiorów danych medycznych	<ul style="list-style-type: none"> <li>Zapewnienie systemu gromadzenia danych medycznych pod kątem możliwości ich wykorzystania do rozwoju systemów AI</li> </ul>	3.7.1.1
Ustawa o jakości w opiece zdrowotnej i bezpieczeństwie pacjenta	Weszła w życie 8 września 2023 r. <sup>17</sup>	Stworzenie systemu rejestrów medycznych	<ul style="list-style-type: none"> <li>Poszerzenie przyjętych rozwiązań na rzecz systemowego podejścia do tworzenia rejestrów medycznych, w tym powołanie rady ds. rejestrów medycznych, liberalizacja zasad tworzenia nowych rejestrów. Utworzenie centrum kompetencyjnego rejestrów jakości w jednostce dedykowanej monitorowaniu jakości. Alternatywnie zmiana podejścia – stworzenie systemu dostępu do uporządkowanych danych z podmiotów wykonujących działalność leczniczą.</li> </ul>	3.7.2 5.3.4.2
		Wspólny standard interoperacyjności	<ul style="list-style-type: none"> <li>Zapewnienie mechanizmów umożliwiających egzekwowanie nowych wymogów.</li> </ul>	3.7.2 5.3.4.3

16. Wniosek rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii, COM/2021/206 final.

17. Z zastrzeżeniem części jej przepisów, które wejdą w życie w późniejszym terminie.

## 1.1.5 Wyzwania systemowe

Poniższa tabela przedstawia postulaty związane z wykorzystywaniem danych w pracy lekarza oraz wskazuje, jakie powinny być kierunki zmian i co należałoby zrobić, aby osiągnąć zakładane cele.

Jak być powinno?	Co jest ku temu potrzebne?	Jak można to osiągnąć?	Priorytet	P
Lekarz powinien mieć łatwy dostęp do danych medycznych pacjentów, którym udziela świadczeń zdrowotnych	<p>Zapewnienie kompletności danych przetwarzanych w systemie centralnym (Platforma P1)<sup>18</sup>.</p> <p>Poprawa jakości funkcjonalnej systemów IT tak, aby dostarczały wysokiej jakości danych oraz były łatwiejsze w obsłudze dla lekarzy.</p>	<ul style="list-style-type: none"> <li>• Poprzez zapewnienie przestrzegania już obowiązujących wymogów w zakresie raportowania zdarzeń medycznych oraz wymiany EDM.</li> <li>• W pierwszej kolejności możliwe jest włączenie obszaru sprawozdawania wysokiej jakości danych do standardów akredytacyjnych wynikających z ustawy o jakości w opiece zdrowotnej i bezpieczeństwie pacjenta.</li> <li>• Docelowo zasadne jest wyznaczenie terminu, po którym nastąpi zawężenie sposobu rozliczeń z NFZ tylko do danych przesyłanych do systemu P1.</li> </ul>	Wysoki	5
Lekarz powinien mieć zapewniony domyślny dostęp do gromadzonych w powyższy sposób danych medycznych pacjentów, którym udziela świadczeń zdrowotnych. Konieczne jest doprecyzowanie zakresu i zasad wyrażania zgody lub zgłaszania sprzeciwu względem takiego dostępu.		<ul style="list-style-type: none"> <li>• Poprzez ujednoczenie zasad dostępu do danych medycznych pacjenta, które obecnie są niespójne, rozróżniają m.in. dostęp do dokumentacji od dostępu do jednostkowych danych medycznych.</li> <li>• Doprecyzowanie zasad przekazywania dokumentacji „niezbędnej do zapewnienia ciągłości świadczeń zdrowotnych”.</li> <li>• Zasadne jest przeprowadzenie szerszej społecznej dyskusji na temat modelu dostępu lekarza do danych pacjenta. Potencjalnie możliwe jest przyjęcie np. modelu, w którym lekarz ma domyślnie dostęp do elektronicznych danych dotyczących zdrowia osób fizycznych, które leczy. Pacjent może zgłosić sprzeciw względem takiego dostępu (tzw. model opt-out), możliwość wniesienia sprzeciwu mogłaby być ograniczona, np. nie odejmować dostępu lekarza POZ. Pacjent miałby też dostęp do informacji na temat tego, kto i kiedy miał dostęp do jego danych.</li> </ul>	Wysoki	5
Należy zwiększyć zakres dokumentacji medycznej prowadzonej w postaci elektronicznej.		<ul style="list-style-type: none"> <li>• Poprzez zapewnienie przestrzegania już obowiązujących wymogów w zakresie formy prowadzenia dokumentów.</li> </ul>	Wysoki	

18. Z zastrzeżeniem uwag co do potencjalnych zmian architektury systemu e-zdrowia.

Jak być powinno?	Co jest ku temu potrzebne?	Jak można to osiągnąć?	Priorytet	P
	Zasadne jest wypracowanie wspólnego standardu nadawania upoważnień do przetwarzania danych na poziomie placówki medycznej	<ul style="list-style-type: none"> <li>• Poprzez doprecyzowanie ustawowego upoważnienia do przetwarzania danych, w szczególności tych zawartych w dokumentacji medycznej. System upoważnień powinien być bardziej precyzyjny, dostosowany do miejsca pracy, zakresu obowiązków lekarza i związanej z tym grupy pacjentów.</li> <li>• Uzupelniająco lub alternatywnie wystarczające może być przygotowanie i opublikowanie wytycznych dotyczących wspólnego standardu nadawania upoważnień.</li> </ul>	Niski	5
	Na końcu lekarz powinien mieć większą łatwość pracy na poziomie różnych systemów IT funkcjonujących w placówce medycznej	<ul style="list-style-type: none"> <li>• Poprzez zwiększenie interoperacyjności i możliwość pracy lekarza na wielu systemach z poziomu „jednego konta” oraz zasady „jednej klawiatury”, tj. raz wpisane dane służą różnym celom sprawozdawczym.</li> <li>• Kwestia interoperacyjności systemów oraz przenaszalności przetwarzanych w nich danych regulowana będzie na poziomie unijnym. Na poziomie krajowym pożądane jest wypracowanie standardu uniwersalnego uwierzytelniania lekarza w różnych systemach IT.</li> </ul>	Wysoki	5
Lekarz powinien postępować zgodnie z jasnymi zasadami postępowania z danymi z różnych źródeł	Odejście od podejścia opartego na pojęciu dokumentacji medycznej na rzecz podejścia opartego o dane medyczne	<ul style="list-style-type: none"> <li>• Poprzez dostosowanie nowych zasad do podejścia prezentowanego w EHDS, które skupia się na danych. Zgodnie z EHDS, „elektroniczna dokumentacja medyczna” oznacza właśnie zbiór elektronicznych danych dotyczących zdrowia przetwarzanych przez podmioty wykonujące działalność leczniczą.</li> <li>• Dalsze rozróżnienie zbiorów danych osobowych i nieosobowych – jest to kluczowe pod kątem zasad dostępu i wykorzystywania tych danych.</li> </ul>	Wysoki	5
	Wypracowanie zasad postępowania z danymi generowanymi poza kontrolą lekarza, p. przez wyroby medyczne lub aplikacje lifestylowe	<ul style="list-style-type: none"> <li>• Wprowadzenie wzorem EHDS znakowania zbiorów danych pod kątem ich jakości, wiarygodności i użyteczności.</li> <li>• Alternatywnie lub uzupełniająco, bez dokonywania interwencji prawnej w tym zakresie (w szczególności przed przyjęciem rozwiązań wymaganych przez EHDS), możliwe jest także wypracowanie przez środowisko, we współpracy ze stroną publiczną, wytycznych i rekomendacji w tym zakresie.</li> </ul>	Wysoki	5
Lekarz powinien być przygotowany do postępowania z danymi medycznymi	Uzupełnienie programów studiów, kształcenia podyplomowego oraz doskonalenia zawodowego o kwestie związane z danymi medycznymi	<ul style="list-style-type: none"> <li>• Poprzez dokonanie rewizji programów edukacyjnych wyższych uczelni oraz promowanie kształcenia w zakresie e-zdrowia.</li> <li>• Działania edukacyjne podejmowane przez Centrum e-Zdrowia powinny obejmować zwrócenie uwagi na szczególną rolę danych medycznych oraz podstawowe zasady postępowania z nimi.</li> </ul>	Średni	5

Jak być powinno?	Co jest ku temu potrzebne?	Jak można to osiągnąć?	Priorytet	P
Dane przetwarzane przez lekarza powinny być bezpieczne	Spełnienie wymogów koniecznych dla zapewnienia wysokiego poziomu ochrony danych o stanie zdrowia	<ul style="list-style-type: none"> <li>Zrealizowanie działań w obszarze bezpieczeństwa takich jak te przewidzianych w Programie rozwoju e-zdrowia w Polsce do 2027 r.</li> <li>Wypracowanie krajowej implementacji dyrektywy NIS 2<sup>19</sup> w konsultacji ze środowiskiem medycznym, by nowe wymogi mogły być skutecznie wdrożone przez podmioty wykonujące działalność leczniczą.</li> <li>Kontynuowanie programów wsparcia finansowego dla podmiotów wykonujących działalność leczniczą, które byłyby dedykowane zakupom towarów i usług związanych z ochroną danych medycznych.</li> <li>Stosowanie kodeksu postępowania z art. 40 RODO.</li> </ul>	Wysoki	5
	Zmiana praktyki w zakresie zawierania umów powierzenia przetwarzania danych w ochronie zdrowia	<ul style="list-style-type: none"> <li>Poprzez wydanie oficjalnych wytycznych, które zawierałyby bardziej rozbudowany katalog najbardziej typowych sytuacji, w których tego rodzaju umowy należy lub nie powinno się zawierać.</li> <li>Doprecyzowanie wymogów związanych z zawieraniem umów o powierzenie przetwarzania danych osobowych oraz umów udostępnienia danych w formie rekomendacji lub wytycznych.</li> </ul>	Niski	5
Lekarz powinien mieć możliwość korzystania z rozwiązań uprawniających pracę z danymi medycznymi	Pełniejsza możliwość wykorzystywania chmury obliczeniowej	<ul style="list-style-type: none"> <li>Poprzez ujednoczenie regulacji dotyczących zasad przetwarzania danych medycznych oraz przechowywania dokumentacji medycznej przez różne podmioty lecznicze.</li> </ul>	Wysoki	5
	Wypracowanie standardu wykorzystywania różnego rodzaju aplikacji i programów do pracy z danymi medycznymi pacjentów	<ul style="list-style-type: none"> <li>Poprzez przyjęcie wytycznych dotyczących dopuszczalności stosowania różnych narzędzi przetwarzania danych i warunków, jakie muszą być przez nie spełniane, aby lekarz mógł je wykorzystać w opiece nad pacjentem. Wytyczne powinny umożliwiać mu łatwe sprawdzenie, czy dane rozwiązanie spełnia wymagany standard.</li> </ul>	Wysoki	5
	Wypracowanie wytycznych związanych z wykorzystywaniem nowych technologii w zakresie danych medycznych	<ul style="list-style-type: none"> <li>Poprzez zaadresowanie podstawowych pytań i wątpliwości związanych ze stosowaniem AI w ochronie zdrowia w formie wytycznych i rekomendacji. Akcje podnoszenia świadomości wśród lekarzy i pacjentów o korzyściach wynikających z wykorzystywania AI w ochronie zdrowia oraz związanych z tym szansach, wyzwaniach i zagrożeniach.</li> </ul>	Wysoki	5

19. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148.

Jak być powinno?	Co jest ku temu potrzebne?	Jak można to osiągnąć?	Priorytet	P
Dane medyczne powinny nadawać się do wykorzystania przez lekarza – spełniać kryteria jakości	Stworzenie mechanizmów promujących wysoką jakość prowadzenia dokumentacji medycznej oraz sprawozdawania danych	<ul style="list-style-type: none"> <li>• Poprzez wypracowanie kryteriów jakości danych medycznych uwzględniających ich kluczowe cechy takie jak wiarygodność, aktualność, kompletność i interoperacyjność oraz włączenie ich do systemu jakości wynikającego z ustawy o jakości w opiece zdrowotnej i bezpieczeństwie pacjenta, np. jako element fakultatywnego systemu akredytacji.</li> <li>• Przy opracowywaniu ram jakości i użyteczności danych należy wziąć pod uwagę oczekiwania zawarte w akcie w sprawie sztucznej inteligencji i jego odpowiedniej dokumentacji określonej w załącznikach.</li> <li>• W dalszej perspektywie czasowej szczegółowe wymogi dotyczące jakości danych i nowy system znakowania jakości i użyteczności danych wynikać będą z regulacji unijnych. Już obecnie można jednak dookreślić takie wymogi na poziomie krajowym oraz wprowadzić podobny system znakowania np. w ramach programu pilotażowego.</li> </ul>	Wysoki	5
	Zapewnienie systemowego podejścia do rozwoju rejestrów medycznych	<ul style="list-style-type: none"> <li>• Poprzez powołanie specjalnej rady ds. rejestrów, która wyznaczy strategiczny plan rozwoju systemu rejestrów medycznych.</li> <li>• Wprowadzenie mechanizmów dodatkowego premiowania świadczeniodawców za przekazywanie wysokiej jakości danych medycznych oraz wprowadzenie środków technicznych i organizacyjnych służących ułatwieniu i automatyzacji przekazania danych do rejestrów medycznych.</li> <li>• Zagwarantowanie dodatkowych środków publicznych na stworzenie i prowadzenie rejestrów medycznych, a także zliberalizowanie zasad ich tworzenia, prowadzenia i finansowania, w szczególności popularyzacja formuły partnerstwa publiczno-prywatnego.</li> <li>• Ustalenie standardów technicznych wymiany danych pomiędzy rejestrami medycznymi oraz danymi znajdującymi się w systemie P1 oraz wprowadzenie mechanizmu łączenia danych z różnych rejestrów.</li> <li>• Alternatywnie, rozważenie budowy systemu opartego o łatwy dostęp do uporządkowanych danych z systemów podmiotów wykonujących działalność leczniczą.</li> </ul>	Średni	5
	Zwiększenie interoperacyjności dokumentacji medycznej	<ul style="list-style-type: none"> <li>• Poprzez zapewnienie przestrzegania już obowiązujących wymogów w zakresie interoperacyjności.</li> <li>• Jasne zasady publikacji obowiązujących standardów oraz dokonywania ich zmian.</li> <li>• Przestrzeganie wysokich standardów powinno zostać włączone do systemu jakości wynikającego z ustawy o jakości w opiece zdrowotnej i bezpieczeństwie pacjenta, np. jako element fakultatywnego systemu akredytacji.</li> </ul>	Wysoki	5

Jak być powinno?	Co jest ku temu potrzebne?	Jak można to osiągnąć?	Priorytet	P
Standaryzacja w zakresie anonimizacji i pseudonimizacji oraz ujednoczenie przepisów dotyczących dostępu do danych	Uporządkowanie i standaryzacja zasad dostępu do danych medycznych	<ul style="list-style-type: none"> <li>• Poprzez uporządkowanie oraz większe ujednoczenie zasad dostępu do danych medycznych, możliwie w ramach jednej ustawy.</li> <li>• Nowy system powinien opierać się na siatce pojęciowej i zasadach wprowadzanych przez EHDS, w szczególności odróżniać elektroniczne dane osobowe dotyczące zdrowia oraz elektroniczne dane nieosobowe dotyczące zdrowia, a także ich pierwotne lub wtórne wykorzystywanie.</li> </ul>	Wysoki	5
	Wypracowanie standardów dotyczących anonimizacji i pseudonimizacji danych medycznych	<ul style="list-style-type: none"> <li>• Poprzez przyjęcie dedykowanych regulacji prawnych lub jasnego standardu w zakresie przeprowadzenia anonimizacji i pseudonimizacji danych medycznych, który wskazywać będzie w jasny sposób właściwe podstawy dla wykonywania tych operacji na danych oraz rekomendowane metody.</li> </ul>	Wysoki	5
Zwiększenie wykorzystania danych w celach naukowych i badawczo-rozwojowych	Uporządkowanie i standaryzacja zasad dostępu do danych medycznych w celach naukowych i badawczo-rozwojowych.	<ul style="list-style-type: none"> <li>• Poprzez doprecyzowanie przesłanek udostępniania dokumentacji medycznej i danych medycznych w celach naukowych i badawczo-rozwojowych tak, by nie budziły one wątpliwości pod kątem RODO, oraz aktualizacja katalogu podmiotów, które mogą ją uzyskać, na wzór EHDS.</li> </ul>	Wysoki	5
	Ograniczenie wątpliwości interpretacyjnych występujących w tym obszarze na gruncie RODO	<ul style="list-style-type: none"> <li>• Poprzez opracowanie wytycznych, które udzielać będą praktycznych wskazówek - jak dokładnie należy postępować przy przetwarzaniu danych medycznych w celach naukowych, i badawczo-rozwojowych, tj. jakie podstawy prawne stosować i jakie wymogi spełnić.</li> <li>• Stworzenie kodeksu branżowego z art. 40 RODO lub wypracowanie wytycznych określających zasady dotyczące przetwarzania danych o stanie zdrowia w celach badań naukowych.</li> <li>• Utworzenie spójnych ram prawnych dotyczących przetwarzania danych osobowych w celach badawczych na poziomie krajowym, by poszerzyć możliwość wykorzystywania jako podstawy prawnej art. 9 ust. 2 lit. i oraz j RODO, czyli niezbędność przetwarzania ze względu na interes publiczny w dziedzinie zdrowia publicznego lub do celów badań naukowych.</li> <li>• W celu popularyzacji możliwości przewidzianych przez art. 8 ustawy o badaniach klinicznych produktów leczniczych stosowanych u ludzi warto wydać oficjalne wytyczne jak w praktyce należy stosować przywołane ograniczenia.</li> <li>• Poprzez wytyczne, które jasno wskazywać będą, przy spełnieniu jakich konkretnie warunków lekarz jako badacz powinien pełnić rolę niezależnego od sponsora administratora danych, współadministratora lub podmiotu przetwarzającego. Wytyczne powinny też wskazywać, jakie mogą być podstawy prawne przetwarzania danych przez badacza będącego administratorem lub współadministratorem danych.</li> </ul>	Wysoki	5

## 2. Wprowadzenie



### 2.1 Dlaczego przygotowaliśmy raport?

Rozwój technologiczny, połączony ze stopniową cyfryzacją kolejnych aspektów życia społecznego, prowadzi do **generowania coraz większych ilości danych w postaci cyfrowej**. Wykorzystanie ich stwarza szansę na szybszy postęp cywilizacyjny. Konieczność zapewnienia efektywnego, przejrzystego i bezpiecznego przetwarzania informacji uważana jest za jedno z największych wyzwań stojących przed światem w XXI. wieku. Dane stanowią swoiste paliwo dla algorytmów, w tym systemów wykorzystujących sztuczną inteligencję, umożliwiając szybsze i skuteczniejsze działania o różnym charakterze - rozwiązywanie problemów, tworzenie nowych produktów i usług, prowadzenie badań.

Postępujący proces cyfryzacji był w ostatnich latach szczególnie widoczny w sektorze ochrony zdrowia. Realizacja takich inicjatyw jak system e-recepty i e-skierowania lub wdrożenie Internetowego Konta Pacjenta pokazują, że możliwości, jakie już teraz stwarzają nowe technologie w medycynie, mogą realnie wpływać na pracę lekarzy oraz ułatwiać proces leczenia pacjentów. Jednocześnie, jesteśmy dopiero na pierwszym etapie tworzenia systemu e-zdrowia – **przed nami wielkie wyzwanie związane z dalszą digitalizacją usług medycznych oraz intensyfikacją prac nad rozwojem systemów opartych o nowe technologie, takiej jak np. sztuczna inteligencja, uczenie maszynowe, przetwarzanie języka naturalnego**, które – dzięki wykorzystywaniu danych medycznych – będą wspierać lekarzy w procesie leczenia.

Przed nami nowe wyzwania, które zmuszają do refleksji – **jak rosnący potencjał analityki danych można wykorzystać w ochronie zdrowia?** Jakie regulacje prawne przyjąć, aby przyspieszyć rozwój narzędzi wykorzystujących dane medyczne w celu usprawnienia pracy lekarzy i podwyższenia jakości opieki zdrowotnej? Jak zagwarantować, by nowe technologie były bezpieczne i wzbudzały zaufanie pacjentów? Unia Europejska dostrzega wagę tych zagadnień, a swoistym zwieńczeniem dotychczasowych, wieloletnich prac w tym zakresie będzie zakończenie procesu legislacyjnego i przyjęcie EHDS, które skupia się na uregulowaniu kwestii pierwotnego i wtórnego wykorzystywania danych medycznych. Jest to przy tym tylko jedna z wielu projektowanych lub już przyjętych regulacji, która dotyka obszaru zarządzania danymi.

Procedowanie na poziomie Unii Europejskiej nowych przepisów, które z całą pewnością odgrywać będą **kluczową rolę w kształtowaniu zasad postępowania z danymi medycznymi**, daje świetną okazję do przeanalizowania najważniejszych obecnych problemów i wyzwań stojących przed sektorem ochrony zdrowia na poziomie krajowym, a także zaproponowania nowych rozwiązań wykorzystujących dane na rzecz podnoszenia jakości opieki zdrowotnej oraz wspierania pracy lekarzy.

Mając na względzie cały szereg nierozwiązanych dotąd prawnych i pozaprawnych problemów z zakresu wykorzystywania danych medycznych, w celu ich dokładniejszej identyfikacji oraz rekomendowania pożądanych działań na rzecz stworzenia w Polsce nowoczesnego, sprawnego systemu przetwarzania danych medycznych, gwarantującego poszanowanie praw pacjenta i dającego lekarzom nowe narzędzia przydatne w ich codziennej pracy, opracowaliśmy niniejszy raport.

## 2.2 Co zawiera raport i czemu ma służyć?

Raport prezentuje kluczowe z perspektywy regulacyjnej **zagadnienia dotyczące obszaru przetwarzania danych medycznych w Polsce**. Opisuje wybrane elementy obecnego stanu prawnego w tym zakresie, jak również praktykę stosowania prawa oraz deklarowane przez stronę publiczną kierunki dalszych zmian krajowego systemu e-zdrowia. W opracowaniu zawarliśmy, poza normami wynikającymi z prawa polskiego, także przepisy międzynarodowe, w tym m.in. regulacje procedowane na poziomie Unii Europejskiej. Ponadto, w celu pełniejszego ukazania omawianej problematyki, uwzględniliśmy też dokumenty o charakterze tzw. soft law (z ang. prawo miękkie), które - choć nie posiadają cech bezwzględnie obowiązującego prawa - w istotny sposób przyczyniają się do sposobu funkcjonowania sektora danych medycznych. Przybliżenie obecnego porządku prawnego stanowi fundament pod dalszą treść raportu – analizę planowanych prawnych i pozaprawnych zmian na poziomie Polski i Unii Europejskiej pod kątem ich możliwych skutków dla lekarzy.

Dane medyczne mogą spełniać, w zależności od sposobu ich wykorzystywania, zróżnicowane funkcje. W pierwszej kolejności, powinny one służyć pacjentowi, którego dotyczą. Z tego względu, prawo dostępu do dokumentacji medycznej stanowi jedno z kluczowych praw wynikających z PrPacjU. Projektowane, unijne regulacje o ustanowieniu EHDS w znacznym zakresie dotyczą właśnie „pierwotnego” wykorzystania danych medycznych, tj. wykorzystania ich w interesie i dla dobra konkretnego pacjenta. Ponadto, EHDS przewiduje „wtórne” wykorzystanie danych na rzecz rozwoju badań. **Wszelkie regulacje dot. danych medycznych powinny uwzględniać, poza samym pacjentem, również rolę lekarza<sup>20</sup>**. To właśnie lekarze – obok pozostałego personelu medycznego - są głównymi użytkownikami danych medycznych i zwykle to im pacjent powierza zadanie wykorzystania jego danych medycznych w celu postawienia diagnozy lub prowadzenia leczenia. Z tego względu, w raporcie postanowiliśmy wskazać kluczowe elementy pożądanego stanu prawnego dot. danych medycznych z perspektywy lekarzy.

20. A także innych osób wykonujących działalność leczniczą. Raport skupia się jednak na przybliżeniu tematu danych medycznych z perspektywy zawodu lekarza i lekarza dentystry.



Środowiska lekarskie, co podkreśla m.in. stanowisko wyrażone w raporcie Okręgowej Izby Lekarskiej w Warszawie im. prof. Jana Nielubowicza „Cyfryzacja zdrowia w interesie społecznym”, dostrzegają konieczność zapewnienia właściwych warunków dla rozwoju sektora wymiany danych dotyczących zdrowia. Jak podkreślono, „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. Zablockowany 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”<sup>21</sup>.

W dobie dynamicznych zmian technologicznych, postępujących również w obszarze Data Sciences (z ang. nauki o danych), a także z uwagi na projektowane na poziomie unijnym reformy, ważne jest, aby już teraz zidentyfikować kluczowe problemy regulacyjne dotyczące przetwarzania danych medycznych. W raporcie przedstawiamy najistotniejsze zagadnienia dla omawianej problematyki, by zaproponować **pożądane kierunki zmian na rzecz stworzenia systemu e-zdrowia, w którym potencjał danych medycznych będzie mógł być w pełni wykorzystywany** z myślą o interesie pacjentów oraz potrzebach osób wykonujących zawody medyczne, w szczególności lekarzy.

Głównym założeniem, którym kierowaliśmy się przy pisaniu raportu, było **zainicjowanie dialogu** środowiska lekarskiego ze stroną publiczną, organizacjami pacjentów, towarzystwami naukowymi oraz innymi interesariuszami sektora ochrony zdrowia w celu wspólnego wypracowania najlepszych zmian prawnych i pozaprawnych dotyczących danych medycznych. Żywimy głęboką nadzieję, że po zapoznaniu się z jego treścią, osoby odpowiedzialne za przyszły kształt systemu e-zdrowia w Polsce będą w stanie jeszcze lepiej zrozumieć potencjał i obecne uwarunkowania dotyczące przetwarzania danych medycznych oraz podjąć działania na rzecz dalszego rozwoju tego obszaru.

## 2.3 Kto przygotował raport?

Raport powstał w ramach inicjatywy grupy **NIL IN** działającej przy **Naczelnej Izbie Lekarskiej**. Kluczową misją NIL IN jest stworzenie sieci lekarzy innowatorów, swoistego miejsca, gdzie wszystkie zainteresowane osoby wykonujące zawód lekarza i lekarza dentysty będą mogły uzyskać niezbędne wsparcie oraz zbudować sieć kontaktów wymaganą do realizacji swoich projektów. Szczegółowe i aktualne informacje o samej inicjatywie oraz jej dotychczasowych aktywnościach dostępne są na stronie internetowej [www.nilin.org.pl](http://www.nilin.org.pl).

W ramach inicjatywy NIL IN działa grupa **ds. danych medycznych**. Jej celem jest łączenie instytucji, firm i osób zainteresowanych obszarem danych medycznych. Grupa działa na rzecz podnoszenia jakości i dostępności danych medycznych, tak by drzemiący w nich potencjał mógł być coraz skuteczniej wykorzystywany i służył szybkiemu rozwojowi innowacji w ochronie zdrowia. Procesy z tym związane powinny następować odpowiedzialnie, z poszanowaniem praw pacjenta i przy zapewnieniu wysokiego poziomu cyberbezpieczeństwa. Członkom grupy zależy na podnoszeniu świadomości na temat korzyści, które dzięki wykorzystaniu danych może odnieść pacjent, lekarz i cały system opieki medycznej w Polsce.

Grupę ds. danych medycznych tworzą następujące podmioty:

**ASSECO**

**COMARCH**  
Healthcare

**IQVIA**

**sano**

## Partnerzy raportu

Partnerem raportu Sano. Sano jest unikatową w skali kraju instytucją naukową dedykowaną rozwojowi medycyny obliczeniowej. Fundacja Sano stanowi jedno z nowo utworzonych Europejskich Centrów Doskonałości i powstała dzięki finansowaniu z europejskiego programu Teaming for Excellence (Horyzont 2020), Fundacji na rzecz Nauki Polskiej (FNP) oraz Ministerstwa Edukacji i Nauki. Głównym założeniem międzynarodowej agencji badawczej Sano są prace naukowe nad zastosowaniami nowoczesnych metod informatycznych w medycynie, w tym sztucznej inteligencji, analizy danych, symulacji komputerowych, nowoczesnych technik wizualizacji oraz przetwarzania danych dużej skali. Celem jest tworzenie systemów wspomagających decyzje lekarza w zakresie diagnostyki, wyboru terapii i monitorowania postępów w leczeniu. Wszystkie te metody wymagają dostępu do danych medycznych: zarówno na etapie prac badawczo rozwojowych, na przykład do uczenia maszynowego; wdrożeniowych, na przykład do weryfikacji i walidacji tworzonych narzędzi; jak i w końcowym użyciu – do analizy danych konkretnego pacjenta zgodnie z podejściem spersonalizowanej medycyny. Z tych powodów zainteresowanie naukowców i inżynierów informatyków z Sano aktualnym stanem prawnym w zakresie danych medycznych oraz kierunkami ich zmian w przyszłości jest niezwykle istotne. Bez odpowiedniej ilości oraz jakości danych medycznych rozwój metod sztucznej inteligencji, symulacji komputerowych i analizy dużych zbiorów danych nie jest możliwy, podobnie jak przyszłość medycyny nie jest możliwa bez nowoczesnych metod i narzędzi informatycznych, będących istotą medycyny obliczeniowej. Jesteśmy przekonani, że dzięki niniejszemu raportowi i współpracy z siecią lekarzy innowatorów, będzie można stworzyć w Polsce i w Europie warunki do rozwoju nowoczesnej medycyny z korzyścią dla pacjentów, lekarzy, oraz wspierających ich naukowców.

**Raport powstał we współpracy z zespołem Healthcare praktyki Life Sciences kancelarii DZP.**



Pełna lista autorów i konsultantów publikacji znajduje się na początku raportu.

## 3. Dane medyczne - stan obecny i perspektywa zmiany



### 3.1 Wprowadzenie

W Polsce obserwuje się dynamiczny rozwój sektora e-zdrowia. Kolejne projekty z zakresu cyfryzacji usług zdrowotnych poskutkowały wprowadzeniem takich rozwiązań jak m.in. system e-recepty, e-skierowania czy funkcjonowanie Internetowego Konta Pacjenta. Pacjenci, co jasno wynika z danych statystycznych, chcą i potrafią korzystać z systemów, które zostały wdrożone do systemu ochrony zdrowia<sup>22</sup>. W szczególności telemedycyna cieszy się ogromną popularnością, zarówno wśród świadczeniodawców, jak i pacjentów<sup>23</sup>. Rozwiązania cyfrowe, których rozwój zdecydowanie przyspieszył na skutek wybuchu pandemii COVID-19, zostały na stałe wdrożone do systemu ochrony zdrowia i stanowią fundamenty systemu e-zdrowia w Polsce.

Jednym z najważniejszych nadchodzących wyzwań jest właściwe wykorzystywanie nowych technologii, w tym AI, w procesie udzielania świadczeń zdrowotnych. Nowe technologie mogą w istotny sposób przyczynić się m.in. do wzrostu jakości leczenia oraz oszczędności czasu personelu medycznego. W celu odpowiedniego wykorzystania tych systemów, niezbędne jest jednak gromadzenie i przetwarzanie dużych zbiorów danych, które będą analizowane m.in. przez systemy machine learning, w tym algorytmy AI.

Na potrzeby raportu będziemy posługiwać się pojęciem danych medycznych, przez które należy rozumieć – podobnie jak na gruncie projektowanych definicji w EHDS - elektroniczne dane osobowe i nieosobowe dotyczące zdrowia, a także dane odnoszące się bezpośrednio do czynników warunkujących zdrowie lub dane przetwarzane pierwotnie w związku z udzielaniem świadczeń zdrowotnych, przetwarzane w formie elektronicznej przez podmioty wykonujące działalność leczniczą<sup>24</sup>. Kluczowe jest przy tym odróżnienie pojęcia danych (już obecnie SystInfOchZdrU posługuje się pojęciem jednostkowych danych medycznych) od pojęcia dokumentu, który w postaci elektronicznej należy rozumieć jako pewien zbiór danych autoryzowany podpisem przez lekarza lub inną osobę wykonującą zawód medyczny. Zagadnienie to zostało szerzej przedstawione w dalszej części raportu (por. punkt 4.2.2).

Wzrost potencjału płynącego z wykorzystywania danych medycznych został dostrzeżony także przez władze Unii Europejskiej. Na przestrzeni ostatnich lat, w systemie prawa pojawiło się wiele nowelizacji mających na celu umożliwienie bardziej efektywnego i bezpiecznego przetwarzania danych. 25 maja 2018 r. zaczęło obowiązywać RODO, które zrewolucjonizowało poziom ochrony danych dotyczących osób fizycznych, w tym danych o stanie zdrowia.

22. Fundacja My Pacjenci, Centrum e-Zdrowia; 2022; E-usługi w ochronie zdrowia.

23. OECD; 2022; Health at a Glance 2022.

24. Raport skupia się na obszarze działalności leczniczej oraz możliwościach wtórnego wykorzystywania danych z sektora ochrony zdrowia. Takie podejście nie wyklucza przyjęcia w ramach dalszych prac związanych z tym tematem szerszej perspektywy, w której dane o takim charakterze mogą być przetwarzane przez inne podmioty w innych celach.

W 2020 r. Komisja Europejska ogłosiła europejską strategię w zakresie danych, która wyznaczyła podstawowe cele związane z rozwojem uniwersalnych, jednolitych przestrzeni danych. Na kanwie strategii powstał szereg projektów aktów normatywnych, m.in. EHDS. W lutym 2022 r. Komisja opublikowała projekt rozporządzenia w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania (Data Act). Proponowane przepisy – jeżeli zostaną przyjęte – zmuszą wielu przedsiębiorców do stworzenia nowych strategii ochrony informacji. 24 września 2023 r. zaczął obowiązywać akt w sprawie zarządzania danymi (Data Governance Act), który umożliwia szersze wykorzystywanie informacji będących w posiadaniu sektora publicznego oraz ureguje rynek pośredników w udostępnianiu danych. Przed nami więc szereg zmian na poziomie unijnym, od których zależeć będzie kształt systemu przetwarzania danych medycznych.

W przypadku danych medycznych, obok regulacji unijnych, kluczowe są przepisy prawa krajowego. Mając na uwadze dynamikę i złożoność tematu, rekomendacje w zakresie podejmowania dalszych działań legislacyjnych dotyczących tego obszaru wymagają analizy obecnego stanu prawnego oraz dokumentów strategicznych wyznaczających przyszłość e-zdrowia. Nowe przepisy muszą tworzyć spójny system, który zapewni złoty środek pomiędzy dostępnością danych medycznych na potrzeby interesu publicznego w ochronie zdrowia a prywatnością pacjenta. W związku z powyższym, na początku prezentujemy kluczowe elementy stanu prawnego oraz polityki publicznej w obszarze danych o stanie zdrowia.

## **3.2 Wybrane elementy stanu obecnego – punkt wyjścia w obszarze danych medycznych**

### **3.2.1 Zarys podstaw prawnych systemu e-zdrowia w Polsce**

Od ponad dekady trwa w Polsce proces informatyzacji sektora opieki zdrowotnej. W 2011 r. Sejm RP przyjął SystInformOchrU, która nadała mu wyraźne ramy prawne. Do szczególnej intensyfikacji prac doszło w 2015 r. Przyjęta w tym roku nowelizacja uregulowała udzielanie świadczeń zdrowotnych za pośrednictwem systemów teleinformatycznych i systemów łączności dając podstawę do rozwoju telemedycyny. Zmieniony w ramach tej reformy art. 24 PrPacjU dopuścił też jednoznacznie możliwość tzw. outsourcingu danych medycznych, kończąc tym samym dotychczasowe wątpliwości interpretacyjne i otwierając system ochrony zdrowia m.in. na technologię chmury obliczeniowej.

Kolejne istotne zmiany nadeszły w roku 2018 r., wraz z uruchomieniem Internetowego Konta Pacjenta. Początkowo IKP stanowiło przede wszystkim fundament pod przyszłe rozwiązania, a jego funkcjonalność była bardzo ograniczona. W następnym roku wprowadzono obowiązek prowadzenia elektronicznej dokumentacji medycznej (EDM), która obejmowała początkowo tylko określone typy dokumentów (np. kartę informacyjną z leczenia szpitalnego). 8 stycznia 2020 r. wszedł w życie generalny obowiązek wystawiania recept w formie elektronicznej. DokMedR wprowadziło obowiązek prowadzenia – co do zasady – wszelkiej dokumentacji medycznej w postaci elektronicznej (w przeciwieństwie do EDM, dokumentacja medyczna w postaci elektronicznej to pojęcie szersze, co zostało szerzej wytłumaczone w punkcie 5.3.1.1 raportu).

Z uwagi jednak na wyjątki od reguły stosowania postaci elektronicznej (m.in. sytuacja, w której warunki organizacyjno-techniczne uniemożliwiają prowadzenie dokumentacji w postaci cyfrowej), w części placówek ochrony zdrowia nadal stosuje się papierową dokumentację. 8 stycznia 2021 r. nastąpił kolejny istotny etap cyfryzacji zdrowia - wprowadzono obowiązek wystawiania skierowań na część świadczeń zdrowotnych w formie elektronicznej. Podobnie jak w przypadku e-recept, również e-skierowania zostały połączone z Internetowym Kontem Pacjenta. Ponadto, od 1 lipca 2021 r. raportowanie zdarzeń medycznych jest obowiązkowe dla wszystkich podmiotów udzielających świadczeń zdrowotnych.

Na obszar e-zdrowia w Polsce wpływają także regulacje unijne, które jak dotąd skupiały się głównie na kwestiach związanych z bezpieczeństwem danych. Ogólne rozporządzenie o ochronie danych, czyli RODO wprowadziło specjalne zasady przetwarzania tzw. danych wrażliwych (sensytywnych), do których zaliczają się m.in. dane o stanie zdrowia. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii<sup>25</sup> zobowiązała państwa członkowskie do zagwarantowania minimalnego poziomu cyberbezpieczeństwa. W lipcu 2018 r. Sejm RP uchwalił KrSystCyberU, która określiła ministra właściwego ds. zdrowia jako organ właściwy do spraw cyberbezpieczeństwa dla sektora ochrony zdrowia. Wprowadzenie aktu miało na celu podjęcie działań na rzecz wykrywania, zapobiegania i minimalizowania skutków ataków na systemy teleinformatyczne, również na te, które obsługują podmioty lecznicze.

Jak wynika z powyższego – jedynie podstawowego - zarysu źródeł prawa systemu e-zdrowia w Polsce, w ochronie zdrowia przyjęto szereg regulacji związanych z usługami cyfrowymi, które wyznaczają ramy przetwarzania danych medycznych. W kolejnych punktach przedstawimy ich kluczowe elementy.

### 3.2.2 Pojęcie danych medycznych

Jak zostało to już zasygnalizowane, sformułowanie „dane medyczne” stanowi pojęcie zbiorcze. W jego skład wchodzi cały szereg danych, w tym danych prowadzonych w sformalizowanej formie dokumentacji medycznej. Przepisy prawa zawierają różne definicje, które kształtują ramy tego pojęcia.

Do 2011 r. w polskim prawie obowiązywała definicja legalna „dokumentacji medycznej”, jednak została ona derogowana z systemu wraz z uchynieniem ustawy o zakładach opieki zdrowotnej. W obecnym stanie normatywnym, PrPacjU określa w sposób ogólny minimalną treść oraz charakterystykę dokumentacji medycznej<sup>26</sup>. Istotnym jest przy tym, aby rozróżnić dokumentację medyczną w postaci elektronicznej od elektronicznej dokumentacji medycznej (EDM).

25. Obecnie zastąpiona dyrektywą Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2).

26. Zgodnie z art. 25 PrPacjU, dokumentacja medyczna zawiera co najmniej: 1) oznaczenie pacjenta; 2) oznaczenie podmiotu udzielającego świadczeń zdrowotnych ze wskazaniem komórki organizacyjnej, w której udzielono świadczeń zdrowotnych; 3) opis stanu zdrowia pacjenta lub udzielonych mu świadczeń zdrowotnych; 4) datę sporządzenia.

Ta druga definiowana jest przez art. 2 pkt 6 SystInfOchZdrU i oznacza dokumenty wytworzone w postaci elektronicznej opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym, podpisem osobistym albo z wykorzystaniem sposobu potwierdzania pochodzenia oraz integralności danych dostępnego w systemie teleinformatycznym udostępnionym bezpłatnie przez Zakład Ubezpieczeń Społecznych, które obejmują:

- **Recepty;**
- **Określone kategorie skierowań;**
- **Zlecenia na zaopatrzenie i zlecenia naprawy wyrobów medycznych;**
- **Karty Szczepień;**
- **Wyniki badania histopatologicznego;**
- **Informacje o rozpoznaniu choroby, problemu zdrowotnego lub urazu, wynikach przeprowadzonych badań, przyczynie odmowy przyjęcia do szpitala, udzielonych świadczeniach zdrowotnych oraz ewentualnych zaleceniach - w przypadku odmowy przyjęcia pacjenta do szpitala;**
- **Informacje dla lekarza kierującego świadczeniobiorcą do poradni specjalistycznej lub leczenia szpitalnego o rozpoznaniu, sposobie leczenia, rokowaniu, ordynowanych lekach, środkach spożywczych specjalnego przeznaczenia żywieniowego i wyrobach medycznych, w tym okresie ich stosowania i sposobie dawkowania oraz wyznaczonych wizytach kontrolnych;**
- **Kartę informacyjną z leczenia szpitalnego;**
- **Wyniki badań laboratoryjnych wraz z opisem oraz opisy innych badań diagnostycznych;**
- **Kartę profilaktycznego badania ucznia;**
- **Indywidualny Plan Opieki Medycznej.**

Wszelkie dane, w tym dane medyczne, możemy podzielić na dane osobowe<sup>28</sup> lub dane nieosobowe. Pojęcie danych osobowych zdefiniowane zostało w art. 4 pkt. 1 RODO i oznacza „wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej”. Szczególną kategorią danych osobowych są „dane dotyczące zdrowia” zdefiniowane w art. 4 pkt. 15 RODO jako dane o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia<sup>27</sup>.

27. RODO, motyw 35 Preambuli – „Do danych osobowych dotyczących zdrowia należy zaliczyć wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą. Do danych takich należą informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej, jak to określa dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE; numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych; informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych; oraz wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą, niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne in vitro”.

Dane nieosobowe to wszelkie inne dane niż tak zdefiniowane dane osobowe<sup>28</sup>. Podobne rozróżnienie zostaje zachowane w projektowanych przepisach EHDS, w których odróżnia się „elektroniczne dane osobowe dotyczące zdrowia”, które oznaczają dane dotyczące zdrowia i dane genetyczne w rozumieniu RODO, a także dane odnoszące się do czynników warunkujących zdrowie lub dane przetwarzane w związku z udzielaniem świadczeń zdrowotnych, przetwarzane w formie elektronicznej, a także „elektroniczne dane nieosobowe dotyczące zdrowia”, które oznaczają dane dotyczące zdrowia i dane genetyczne w formacie elektronicznym, które nie wchodzą w zakres definicji danych osobowych wynikającej z RODO (art. 2 ust. 2 lit. a i b EHDS).

W SystInformOchrU, ustawodawca zdecydował się natomiast wprowadzić definicję terminu „dane”, oznaczające litery, wyrazy, cyfry, teksty, liczby, znaki, symbole, obrazy, kombinacje liter, cyfr, liczb, symboli i znaków, zebrane w zbiory o określonej strukturze, dostępne według określonych kryteriów, w tym dane osobowe, oraz pojęcie „jednostkowych danych medycznych” stanowiące dane osoby fizycznej o udzielonych, udzielanych i planowanych świadczeniach opieki zdrowotnej oraz dotyczące jej stanu zdrowia, w tym profilaktyki zdrowotnej i realizacji programów zdrowotnych.

Konsekwencje takiej siatki pojęciowej oraz związane z nią wyzwania zostały szerzej przedstawione w punkcie 5.3.1.1 raportu.

### 3.2.3 Podstawowe źródła danych medycznych

Każde przetwarzanie danych zaczyna się od procesu ich pozyskania lub wytworzenia<sup>29</sup>. W zależności od rodzaju danego podmiotu oraz specyfiki obszaru jego działalności, będzie on gromadzić różne kategorie danych i bazować na różnych źródłach. Obecnie, wśród głównych podmiotów gromadzących dane medyczne, wymienić można:

- Podmioty udzielające świadczeń zdrowotnych (m.in. szpitale, przychodnie, indywidualne praktyki lekarskie) - podmioty te gromadzą dane bezpośrednio od pacjentów oraz przeprowadzonych badań i na bazie tak uzyskanych informacji tworzą dokumentację medyczną. Poza tym, podmioty udzielające świadczeń zdrowotnych operują także danymi rozliczeniowymi, informacjami pochodzącymi ze skarg pacjentów, przeprowadzanych ankiet itd.

28. Por. art. 3 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej.

29. Zgodnie z art. 3 pkt 2 RODO, przetwarzanie oznacza każdą operację lub zestaw operacji wykonywanych na danych lub zbiorach danych w formie elektronicznej w sposób zautomatyzowany lub niezautomatyzowany, takie jak gromadzenie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie przez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

- Rejestry medyczne<sup>30</sup> – centralne bazy danych tworzone na podstawie przepisów ustaw, w szczególności SystnformOchrU<sup>31</sup> lub w drodze rozporządzenia Ministra Zdrowia wydawanego na podstawie art. 20 ust. 1 tej ustawy<sup>32</sup>. Do tej drugiej kategorii należy obecnie 15 następujących rejestrów<sup>33</sup>:

1. Krajowy Rejestr Pacjentów z COVID-19;
2. Rejestr Hipercholesterolemii Rodzinnej;
3. Rejestr Operacji Naczyniowych;
4. Rejestr Endoprotezoplastyk;
5. Rejestr Przeznaczyniowych Ekstrakcji Elektrood;
6. Rejestr Infekcyjnego Zapalenia Wsierdza;
7. Rejestr Mechanicznego Wspomagania Krążenia;
8. Krajowy Rejestr Ablacji Podłoża Arytmii;
9. Polski Rejestr Wrodzonych Wad Rozwojowych;
10. Rejestr Nowotworów Niezłośliwych Dużych Gruczołów Ślinowych;
11. Krajowy Rejestr Operacji Kardiologicznych;
12. Ogólnopolski Rejestr Ostrego Zespołu Wieńcowego;
13. Rejestr Medycznie Wspomaganej Prokreacji;
14. Krajowy Rejestr Nowotworów;
15. Ogólnopolski kardiologiczno-kardiologiczny rejestr przezcewnikowego leczenia zastawek serca „POL-TaVALVE”.

Warto też dodatkowo zauważyć, że na poziomie krajowym i unijnym funkcjonują rejestry mogące zawierać inne przydatne dla lekarzy informacje, np. baza danych EUDAMED, dotycząca wyrobów medycznych, stanowić będzie ważne źródło danych o wyrobach medycznych, m.in. badaniach klinicznych tych wyrobów, zdarzeniach niepożądanych z nimi związanych. Informacje z niej – poprzez m.in. oprogramowanie wspomagające – mogą zostać wykorzystane przez lekarza, m.in. w celu uzyskania danych niezbędnych do leczenia, jak też implementowani odpowiedniego leczenia.

- **Institucje publiczne – gromadzące dane raportowane przez placówki medyczne:**
  - Narodowy Fundusz Zdrowia – dane rozliczeniowe związane ze świadczeniami opieki zdrowotnej. Dane o kwalifikacji świadczeniobiorców do programów lekowych i ocen skuteczności ich wykonywania, dane o uprawnieniach pacjentów do świadczeń opieki zdrowotnej finansowanych ze środków publicznych
  - Zakład Ubezpieczeń Społecznych – informacje z zakresu udzielania zwolnień lekarskich, chorobach zawodowych i wypadkach przy pracy;

30. Rejestry medyczne są przy tym źródłem wtórnym względem samych podmiotów wykonujących działalność medyczną, które przesyłają dane do rejestrów. W efekcie takiej kumulacji rejestry tworzą nowe zbiory danych.

31. m.in. Centralny Wykaz Produktów Leczniczych; Centralny Wykaz Pracowników Medycznych; Centralny Wykaz Usługodawców; Centralny Wykaz Usługobiorców

32. Rejestry tworzone w celu monitorowania zapotrzebowania na świadczenia opieki zdrowotnej, monitorowania stanu zdrowia usługobiorców, prowadzenia profilaktyki zdrowotnej lub realizacji programów zdrowotnych albo programów polityki zdrowotnej, monitorowania i oceny bezpieczeństwa, skuteczności, jakości i efektywności kosztowej badań diagnostycznych lub procedur medycznych.

33. <https://www.gov.pl/web/zdrowie/wykaz-rejestrow-medycznych>



- Główny Urząd Statystyczny – informacje administracyjne na temat populacji korzystającej ze świadczeń zdrowotnych, sprzedaży leków, działalności leczniczej i ratownictwie medycznym;
- Agencja Badań Medycznych – informacje dotyczące przeprowadzania niekomercyjnych badań klinicznych;
- Agencja Oceny Technologii Medycznych i Taryfikacji – informacje z zakresu refundowanych świadczeń opieki zdrowotnej, programów polityki zdrowotnej, refundowanych leków i wyrobów medycznych;
- Centrum Monitorowania Jakości w Ochronie Zdrowia – informacje dotyczące spełniania standardów akredytacyjnych;
- **Uczelnie, w tym w szczególności uczelnie medyczne i instytuty badawcze – informacje gromadzone na potrzeby badań naukowych, przygotowywania publikacji itp.;**
- **Firmy farmaceutyczne – informacje gromadzone w związku z prowadzonymi badaniami klinicznymi;**
- **Firmy badawcze i konsultingowe – informacje gromadzone z różnych innych źródeł w celach badawczo-rozwojowych i analitycznych;**
- **Producenci wyrobów medycznych – informacje gromadzone przez wyroby medyczne, dane o stanie zdrowia osób korzystających z wyrobów medycznych;**
- **Producenci urządzeń i aplikacji niebędącymi wyrobami medycznymi, lecz gromadzącymi dane o stanie zdrowia lub inne informacje psychofizyczne – informacje zbierane m.in. przez urządzenia typu smartwatch podczas treningów fizycznych, aplikacje monitorujące jakość snu.**

### 3.2.4 Zasady dostępu do danych medycznych

Zasady dostępu do dokumentacji medycznej, czyli podstawowego źródła danych medycznych, regulowane są przede wszystkim przez PrPacjU. Zgodnie z przepisami wspomnianego aktu, podmiot udzielający świadczeń zdrowotnych ma obowiązek udostępnić dokumentację medyczną pacjentowi, osobie przez niego upoważnionej oraz jego przedstawicielowi ustawowemu. W przypadku śmierci pacjenta, dokumentację medyczną udostępnia się osobie upoważnionej przez pacjenta za życia lub osobie, która w chwili zgonu pacjenta była jego przedstawicielem ustawowym. Ponadto PrPacjU przewiduje w art. 26 ust. 3 szerszy katalog podmiotów, które posiadają dostęp do dokumentacji medycznej bez konieczności uzyskiwania zgody osoby, której dokumentacja dotyczy. Takimi podmiotami są m.in. organy władzy publicznej w zakresie niezbędnym do wykonywania ich zadań, podmioty prowadzące rejestry usług medycznych czy też Agencja Badań Medycznych. Przepisy przewidują również obowiązek udostępnienia dokumentacji podmiotom leczniczym, m.in. przy kontynuacji leczenia, a także możliwość udostępnienia jej szkole wyższej lub instytutowi badawczemu do wykorzystania w celach naukowych.

W kwestii dostępu do danych pochodzących z rejestrów medycznych, zgodnie z art. 19 ust. 7 SystInforOchrU, mogą one być udostępniane w celu prowadzenia badań naukowych i do celów statystycznych w formie uniemożliwiającej ich powiązanie z konkretną osobą fizyczną. Na uwagę zasługuje również przepis JakZdrU, zgodnie z którym usługodawcy, administratorzy danych przetwarzanych w SIM, administratorzy danych przetwarzanych w dziedzinowych systemach teleinformatycznych, Narodowy Fundusz Zdrowia oraz podmioty prowadzące rejestry publiczne lub rejestry medyczne są obowiązani do nieodpłatnego przekazywania danych do rejestrów medycznych.

Dostęp do danych przez osoby wykonujące zawody medyczne jest zróżnicowany. Wskazany przez pacjenta lekarz podstawowej opieki zdrowotnej ma prawo dostępu do jednostkowych danych medycznych osoby, której leczenie prowadzi. Inaczej sytuacja kształtuje się w przypadku lekarzy-specjalistów. Zgodnie z art. 35 SystInforOchrU, dostęp do jednostkowych danych medycznych mają:

- **pracownik medyczny, który wytworzył daną dokumentację medyczną;**
- **pracownik medyczny wykonujący zawód u usługodawcy<sup>24</sup>, u którego została wytworzona dana dokumentacja, w związku z wykonywaniem przez niego zawodu u tego usługodawcy, jeżeli jest to niezbędne do prowadzenia diagnostyki lub zapewnienia ciągłości leczenia;**
- **lekarz, pielęgniarka lub położna udzielający usługobiorcy świadczeń opieki zdrowotnej w ramach umowy o udzielanie świadczeń opieki zdrowotnej z zakresu podstawowej opieki zdrowotnej;**
- **każdy pracownik medyczny w sytuacji zagrożenia życia usługobiorcy.**

### **3.2.5 Główne gwarancje prawne jakości i interoperacyjności dokumentacji medycznej**

Kwestie zapewnienia gwarancji jakości i interoperacyjności danych zostały w polskim porządku prawnym uregulowane przede wszystkim w SystInforOchrU. Zgodnie z art. 11 ust. 1a, elektroniczną dokumentację medyczną prowadzi się w formatach zamieszczonych w Biuletynie Informacji Publicznej ministra właściwego do spraw zdrowia. Ujednolicenie formatów prowadzenia dokumentacji ma ułatwić swobodny przepływ danych poprzez SIM – zgodnie z art. 11 ust. 1b, istnieje obowiązek wymiany elektronicznej dokumentacji medycznej zgodnie ze standardami zamieszczonymi w Biuletynie Informacji Publicznej ministra właściwego do spraw zdrowia.

Ważną rolę dla omawianego aspektu jakości i interoperacyjności dokumentacji odgrywa także DokMedR. Akt nakłada m.in. konieczność zapewnienia, aby system teleinformatyczny, w którym jest prowadzona dokumentacja, zapewniał integralność treści dokumentacji i metadanych polegającą na zabezpieczeniu przed wprowadzaniem zmian, z wyjątkiem zmian wprowadzanych w ramach udokumentowanych procedur. W kwestii ustalenia formatów danych, rozporządzenie określa, że system teleinformatyczny, w którym są przetwarzane informacje medyczne, powinien

34. Usługodawca oznacza podmiot wykonujący działalność leczniczą w rozumieniu przepisów o działalności leczniczej, inną osobę, która uzyskała fachowe uprawnienia do udzielania świadczeń zdrowotnych i udziela ich w ramach wykonywanej działalności gospodarczej, podmiot realizujący czynności z zakresu zaopatrzenia w wyroby medyczne, podmiot udzielający opieki farmaceutycznej, o której mowa w art. 4 ust. 2 ustawy o zawodzie farmaceuty.

zapewnić – w przypadku braku opublikowania właściwych standardów w Biuletynie Informacji Publicznej - możliwość prowadzenia i udostępniania dokumentacji w standardach HL7 oraz DICOM lub innych standardach i formatach.

Zgodnie z art. 8d SystInformOchrU dostawcy usług informatycznych są obowiązani zapewnić, aby ich systemy teleinformatyczne identyfikowały się wzajemnie oraz porozumiewały między sobą w sposób bezpieczny, zgodnie z wymogami dotyczącymi wspólnych, otwartych standardów komunikacji. Ponadto, ustawa przewiduje obowiązek określenia wspólnych i bezpiecznych otwartych standardów komunikacji przez ministra właściwego do spraw zdrowia poprzez ogłoszenie w Biuletynie Informacji Publicznej, mając na uwadze zapewnienie adekwatnego poziomu bezpieczeństwa komunikacji i poufności oraz integralności przekazywanych danych.

### **3.2.6 Wymogi związane z bezpieczeństwem przetwarzania danych medycznych.**

Zgodnie z art. 24 ust. 2 PrPacjU, do przetwarzania danych zawartych w dokumentacji medycznej, w celu m.in. zapewnienia bezpieczeństwa systemu teleinformatycznego w którym przetwarza się dane, są uprawnione osoby wykonujące zawód medyczny oraz inne osoby wykonujące czynności pomocnicze przy udzielaniu świadczeń zdrowotnych, a także czynności związane z utrzymaniem systemu teleinformatycznego, w którym przetwarzana jest dokumentacja medyczna, i zapewnieniem bezpieczeństwa tego systemu, na podstawie upoważnienia administratora danych. W zakresie omawianej problematyki warto także przytoczyć ponownie DokMedR. Akt ten reguluje formę dokumentacji oraz sposoby jej zabezpieczenia, m.in. przez wymienienie warunków niezbędnych do uznania dokumentacji medycznej za „zabezpieczoną” - poprzez zapewnienie jej dostępności wyłącznie dla osób uprawnionych oraz zastosowanie metod i środków ochrony, których skuteczność w czasie ich zastosowania jest powszechnie uznawana.

Podstawowe przepisy regulujące ogólny poziom bezpieczeństwa przetwarzania danych medycznych jako danych osobowych zawarte są w RODO. Zgodnie z art. 32 RODO, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa danych odpowiedni do ryzyka wystąpienia naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze. Przepisy RODO wskazują, że przy wdrażaniu odpowiednich środków bezpieczeństwa, należy brać pod uwagę również stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania. Obowiązek wyboru właściwych metod zabezpieczania danych, zgodnych z przywołanymi kryteriami, został powierzony administratorom danych. W kontekście sektora ochrony zdrowia administratorami są m.in. podmioty wykonujące działalność leczniczą, które muszą w związku z tym stale analizować ryzyko i dbać o odpowiedni dobór środków bezpieczeństwa, co wiąże się z istotnym obciążeniem organizacyjnym. Warto jednak wspomnieć, że przytoczone normy nie będą miały zastosowania do danych zanonimizowanych, które często są wykorzystywane do celów prowadzenia badań naukowych

W 2018 r. utworzono Krajowy System Cyberbezpieczeństwa. Zgodnie z art. 41 KrSystCyberU, organem właściwym do spraw cyberbezpieczeństwa dla sektora ochrony zdrowia jest, poza wyjątkami, minister właściwy do spraw zdrowia. Ustawa postuluje się pojęciem operatorów usług kluczowych, czyli podmiotów działających w szczególnie ważnych dla bezpieczeństwa państwa sektorach, na które prawodawca nałożył obowiązek wdrożenia systemu zarządzania bezpieczeństwem w systemie IT wykorzystywanym do świadczenia danej usługi kluczowej. Kategorie operatorów kluczowych są wymienione w załączniku nr 1 do KrSystCyberU, a jedną z nich są podmioty z sektora ochrony zdrowia, m.in. podmioty lecznicze. Najważniejszymi obowiązkami z zakresu cyberbezpieczeństwa, które nałożono na operatorów usług kluczowych są: zarządzanie ryzykiem, wdrożenie wymaganych środków technicznych i organizacyjnych, zbieranie informacji o zagrożeniach i podatnościach na incydenty, zgłaszanie incydentu poważnego do właściwego zespołu reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), obsługa incydentów i współpraca w tym zakresie z właściwym CSIRT, wyznaczenie osoby kontaktowej na potrzeby krajowego systemu cyberbezpieczeństwa.

Doświadczenia ostatnich lat wskazują na rosnące ryzyko związane z zagrożeniami dla bezpieczeństwa danych medycznych. Na początku lipca 2023 roku ENISA opublikowała raport na temat zagrożeń cybernetycznych dla europejskiego sektora ochrony zdrowia. Badanie wykazało, że w 2021 roku odnotowano 91 incydentów, w 2022 roku 84 incydenty, a od stycznia do końca marca 2023 roku, czyli tylko przez pierwsze trzy miesiące roku, już 40 incydentów<sup>35</sup>. Jak wynika z dostępnych danych, w Polsce liczba zgłoszonych cyberataków na placówki ochrony zdrowia wzrosła trzykrotnie w ciągu jednego roku – z 13 w 2021 do 43 w 2022 i nadal rośnie<sup>36</sup>. Atak na prywatną sieć laboratoriów medycznych z listopada 2023 r. potwierdza, jak ważne i aktualne są kwestie związane cyberbezpieczeństwem. Dodatkowo należy zwrócić uwagę na zagrożenia związane z nadużywaniem dostępu do danych medycznych i nieuprawnionym wykorzystywaniem ich w celach niezwiązanych z opieką nad pacjentem lub zarządzaniem zdrowiem publicznym i systemem ochrony zdrowia, których przykładem może być sytuacja związana z opublikowaniem danych o stanie zdrowia jednego z lekarzy przez ministra zdrowia w sierpniu 2023 r.

35. ENISA threat landscape: health sector (January 2021 to March 2023), s. 8. <https://www.enisa.europa.eu/publications/health-threat-landscape>

36. <https://forsal.pl/lifestyle/technologie/artykuly/9223343.check-point-liczba-cyberatakow-na-sluzbe-zdrowia-w-polsce-wzrosła-trz.html>

## 3.3 Plany rozwoju obszaru danych medycznych w Unii Europejskiej i w Polsce

### 3.3.1 Wprowadzenie

Ze względu na rosnącą popularność zagadnienia wymiany danych medycznych, zarówno na poziomie krajowym, jak i europejskim, instytucje publiczne opracowały szereg dokumentów zawierających strategię rozwoju w tym zakresie. Część z nich odnosi się bezpośrednio do tematyki wykorzystania danych dotyczących zdrowia, inne natomiast dotyczą ogólnych wyzwań stawianych przez rozwój data science, w tym dostosowania prawnych zasad przetwarzania informacji do potencjału płynącego z postępu technologicznego w zakresie danych. Powstały również dokumenty zawierające konkretne plany uregulowania rozwiązań opartych na sztucznej inteligencji, które mogą mieć istotny wpływ na obszar danych zdrowotnych. W niniejszym punkcie prezentujemy wybrane, kluczowe dla omawianego zagadnienia dokumenty.

### 3.3.2 Europejska strategia w zakresie danych.

Strategia stanowi dokument sporządzony przez Komisję Europejską zawierający informacje na temat kierunku zmian wprowadzanych na szczeblu unijnym w zakresie stworzenia w Europie jednolitej przestrzeni danych i jednolitego rynku otwartego na dane. Choć nie jest to akt bezpośrednio obowiązującego prawa, odgrywa on istotną rolę w procesie prac nad nowymi przepisami Wspólnoty Europejskiej. W pierwszej kolejności, twórcy strategii skupiają się na zapewnieniu bezpieczeństwa przetwarzanych danych oraz ułatwieniu przedsiębiorcom dostępu do nieograniczonej ilości wysokiej jakości informacji.

Strategia przewiduje m.in. utworzenie procedowanej obecnie, wspólnej europejskiej przestrzeni danych dotyczących zdrowia (European Health Data Space), która miałaby znacznie podnieść efektywność przepływu danych medycznych na terenie UE. Szerszy dostęp do informacji ma, według twórców strategii, przyczynić się do osiągnięcia postępów w zapobieganiu, leczeniu i wykrywaniu chorób, a także do podejmowania bardziej świadomych decyzji z myślą o poprawie dostępności, stabilności i skuteczności systemów ochrony zdrowia.

### 3.3.3 Krajowy Plan Odbudowy

Omawiana problematyka została podjęta w ramach działań związanych z realizacją Krajowego Planu Odbudowy i Zwiększania Odporności, który został oficjalnie zatwierdzony przez Komisję Europejską 1 czerwca 2022 roku. Zgodnie z zapowiedzianą w KPO reformą D1.1.2. – „Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia”, Polska ma wdrożyć trzy centralne usługi cyfrowe:

- **Repozytorium danych medycznych** - rozwiązanie będzie polegać na stworzeniu elektronicznego „banku” elektronicznej dokumentacji medycznej i, według planów wyrażonych w KPO, do 2026 r. ma obsługiwać 30% świadczeniodawców<sup>37</sup>.
- **Narzędzia wspomagające analizę stanu zdrowia pacjenta** – narzędzia mające na celu zbieranie i łączenie danych dot. zdrowia pochodzących z różnych urzędów wykonujących pomiary, które następnie trafią na Internetowe Konto Pacjenta.
- **Rozwój algorytmów sztucznej inteligencji** – umożliwienie wsparcia procesu decyzyjnego lekarza przez systemy AI. Dokumentacja pochodząca z wykonanych przez pacjenta badań będzie przetwarzana przez algorytmy sztucznej inteligencji w celu wyszukiwania nieprawidłowości i zagrożeń. Na skutek analizy, AI przygotuje raport i powiadomi personel o wykrytych problemach w stanie zdrowia pacjenta w celu wsparcia decyzji dotyczącej udzielania świadczeń zdrowotnych.

Powyższe propozycje wymagają zwiększenia poziomu digitalizacji danych medycznych zawartych w dokumentacjach pacjentów. Według celów określonych w KPO, do I kwartału 2026 r. planowane jest osiągnięcie poziomu prowadzenia dokumentacji medycznej w formie elektronicznej w wysokości 60%. W realizacji tych założeń ma pomóc utworzenie Centrum Cyfryzacji Dokumentacji Medycznej.

### 3.3.4 Program rozwoju e-zdrowia w Polsce do 2027 r.

W 2022 r. Ministerstwo Zdrowia opublikowało „Program Rozwoju e-Zdrowia na lata 2022-2027”, którego zadaniem jest podniesienie jakości opieki zdrowotnej poprzez kluczowe obszary interwencji. Dokument skupia się na zapewnieniu rozwoju zdalnej opieki w środowisku pacjenta oraz autodiagnostyki i wyznacza pięć celów szczegółowych, wśród których wyróżnia obszar danych i dostęp do właściwych informacji i wiedzy dla każdego interesariusza systemu ochrony zdrowia.

37. Zwracamy przy tym uwagę, że KPO nie wskazuje żadnych dalszych szczegółów związanych z tą inicjatywą, w tym aspektów technicznych. Repozytorium może stanowić potencjalnie wsparcia dla podmiotów leczniczych w zakresie przechowywania elektronicznej dokumentacji medycznej, może też gromadzić jednostkowe dane medyczne. Tworzenie repozytoriów opartych o przetwarzania jednostkowych danych medycznych może stworzyć większe możliwości związane z wykorzystywaniem gromadzonych w nich danych, co może w rezultacie przyczynić się do usprawnienia pracy lekarzy.

**W ramach tego program wyróżnia cztery obszary rozwoju:**

1. Dostęp do danych medycznych;
2. Wtórne wykorzystanie danych;
3. Poprawa jakości i kompletności danych;
4. Zastosowanie sztucznej inteligencji.

Program stawia na lepsze wykorzystywanie danych medycznych połączone z użyciem technologii algorytmów sztucznej inteligencji, które mają analizować m.in. dane dostępne w tzw. systemie P1 oraz dokumentację pacjenta oraz informować lekarzy, czy pojawiły się nieprawidłowości na które szczególnie warto zwrócić uwagę. Wsparcie w podejmowaniu decyzji klinicznych nie ma zastąpić ostatecznego decyzyjnego czynnika ludzkiego – lekarza. System ma za zadanie poprawić skuteczność diagnostyki poprzez podpowiedzi i nakierowywanie na wykryte problemy.

**W treści strategii podkreślono, że w celu zagwarantowania najwyższej jakości udzielanych świadczeń, należy spełnić następujące postulaty:**

- Nadanie dostępu pracownikowi medycznemu do danych szerszych niż te zawarte w dokumentacji medycznej będącej w posiadaniu danego podmiotu leczniczego;
- Umożliwienie istnienia medycyny personalizowanej poprzez możliwość połączenia danych medycznych z markerami biologicznymi;
- Zapewnienie dostępności do danych medycznych niezależnie od państwa członkowskiego UE, w którym udzielane jest świadczenie;
- Sugerowanie decyzji klinicznych na podstawie algorytmów AI;
- Wtórne wykorzystanie gromadzonych danych o stanie zdrowia w celu rozwijania polityki zdrowotnej, epidemiologii, prowadzenia badań, analizy jakości udzielanych świadczeń oraz efektywności systemu ochrony zdrowia.

**Jako produkty realizujące cel strategii dotyczący danych medycznych, które mają zostać wprowadzone w latach 2022 -2027, wymieniono:**

**Do 2. kwartału 2023 r.<sup>38</sup>:**

- Dostęp do danych o dostępności leków – umożliwienie monitorowania dostępności produktów leczniczych i wyrobów medycznych w czasie rzeczywistym;
- Spójna polityka prywatności danych – stworzenie spójnej polityki prywatności danych pacjenta stosowanej na wszystkich poziomach systemu ochrony zdrowia;

**Do 2. kwartału 2025 r.:**

- Ramy dla zarządzania danymi zdrowotnymi – utworzenie centrum kompetencyjnego ds. danych medycznych, które zajmie się interoperacyjnością semantyczną oraz modelem danych medycznych; wprowadzenie jednolitej bazowej terminologii SNOMED CT; opracowanie logicznego modelu danych, struktury danych w postaci zasobów HL7 FHIR oraz specyfikacja MedAPI oparta na zasobach HL7 FHIR;
- Budowa platformy rejestrów medycznych – stworzenie centralnej platformy rejestrów medycznych, wspierającej poprawę jakości w ochronie zdrowia; dane do rejestrów będą pozyskiwane z systemu P1 oraz elektronicznego rekordu pacjenta;

38. Projekty nie zostały zrealizowane we wskazanym terminie.

- HTA dla m-Zdrowia i AI – powstanie zasad oceny skuteczności i bezpieczeństwa rozwiązań m-Zdrowia i AI;

#### **Do 2027 r.:**

- Predykcja (prognozowanie) zdrowia pacjenta – systemy AI będą analizować dane o stanie zdrowia pacjenta i na tej podstawie informować personel medyczny o ewentualnych nieprawidłowościach;
- Wdrożenie e-observacji pacjenta – cyfryzacja danych związanych z obserwacjami klinicznymi; wsparcie pracowników medycznych w prostszym wprowadzaniu danych elektronicznych do systemów IT, wprowadzenie zasad kompletności, integralności oraz spójności danych; udostępnienie pacjentom obserwacji klinicznej;
- Rozwój narzędzi analitycznych – do 2027 r. - powstanie plan rozwoju analizy danych, obejmujący analizy zarządcze, predykcje zdrowia pacjenta, analizy na potrzeby badań, rozwoju i rejestrów medycznych, analizy dla wskaźników jakości udzielanych świadczeń, w tym w zakresie poziomu jakości opieki onkologicznej;
- Program optymalizacji sprawozdawczości – do 2027 r. powstanie program optymalizacji sprawozdawczości, obejmujący przeprowadzenie przeglądu danych raportowanych przez usługodawców, także pod kątem użyteczności i adekwatności poszczególnych atrybutów;
- Modele sztucznej inteligencji – do 2027 r. – prowadzenie prac nad budową modeli i polityką udostępniania danych dla sektora badań i rozwoju; utworzenie i trenowanie modeli do predykcji zdrowia pacjenta na poziomie centralnym.

#### **W strategii poruszone zostały również m.in. konieczność:**

- stworzenia wymagań do sposobu składowania danych medycznych w systemach usługodawców poprzez standardy interoperacyjności;
- powołania centrum kompetencyjnego, którego zadaniem będzie zarządzanie danymi klinicznymi w polskim systemie ochrony zdrowia;
- przygotowania pełnej, kompleksowej ustawy o danych medycznych, które ureguluje cały obszar danych medycznych i dokumentacji medycznej.



### 3.3.5 Polityka rozwoju sztucznej inteligencji w Polsce.

W 2020 r. Rada Ministrów przyjęła „Politykę dla rozwoju sztucznej inteligencji w Polsce od roku 2020”, opisującą planowane przez Polskę działania i cele, które państwo ma zamiar osiągnąć w perspektywie krótko, średnio i długoterminowej. W realizacji celów krótkoterminowych w obszarze wykorzystania AI w sektorze publicznym, polityka rozwoju AI przewiduje wykorzystanie badawczego potencjału płynącego z danych medycznych celem poprawy zdrowia obywateli. Jednocześnie w programie podkreślono, że w działaniach należy uwzględnić ochronę prywatności.

**Jako narzędzia, które miałyby realizować wspomniany cel, dokument przewiduje:**

- Przeprowadzenie pilotażowych programów składowania zanonimizowanych danych medycznych;
- Wspieranie rozwoju narzędzi wykorzystujących dane medyczne;
- Analizę danych dot. zdarzeń medycznych;
- Prowadzenie działań optymalizacyjnych w ochronie zdrowia za pomocą analizy danych takich jak mapy potrzeb, podaży i popytu na świadczenia, wykorzystanie zasobów, dane z usług cyfrowych;
- Udostępnianie danych dot. zdrowia w celu badania leków i metod leczenia.

Poza przytoczonym krajowym dokumentem zawierającym ogólne podsumowanie celów rozwoju AI w Polsce, warto także wspomnieć o funkcjonującej przy Ministerstwie Cyfryzacji Grupie Roboczej ds. Sztucznej Inteligencji (GRAI), która ma pracować nad rozwiązaniami wspierającymi powstawanie odpowiednich warunków dla rozwoju zastosowań AI w sektorach prywatnym i publicznym.

Istotne z perspektywy omawianego zagadnienia są także prace legislacyjne trwające na poziomie Unii Europejskiej. Obecnie procedowane są dwa akty prawne, które w sposób obszerny uregulują funkcjonowanie sztucznej inteligencji w Europie: Rozporządzenie ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) oraz Dyrektywa w sprawie dostosowania przepisów dotyczących pozaumownej odpowiedzialności cywilnej do sztucznej inteligencji (dyrektywa w sprawie odpowiedzialności za sztuczną inteligencję). Rozwój sektora AI wymaga myślenia o danych medycznych w kategorii przyszłego ich wykorzystywania przez algorytmy sztucznej inteligencji.

#### 3.3.5.1 Inicjatywy regionalne

Na poziomie regionalnym funkcjonują tzw. regionalne platformy e-zdrowia, przez które należy rozumieć systemy teleinformatyczne tworzone przez samorządy województw. Realizują one wybrane usługi e-zdrowia dla podmiotów leczniczych i pacjentów danego województwa. Tego typu platformy nie powstały we wszystkich województwa, a poszczególne istniejące platformy różnią się skalą, liczbą interesariuszy i zakresem usług<sup>39</sup>. Dostępne wyniki kontroli NIK dotyczącej Podlaskiego Systemu Informacyjnego e-Zdrowie wykazały liczne wyzwania i trudności z realizacją podobnego projektu<sup>40</sup>.

39. Program rozwoju e-zdrowia w Polsce do 2027 r. , s. 14.

40. <https://www.nik.gov.pl/aktualnosci/nik-o-podlaskim-systemie-informacyjnym-e-zdrowie.html>

W związku z powyższym plany związane z rozwojem systemu e-zdrowia powstają także na poziomie regionalnym. Przykładowo, 23 marca 2021 r. Zarząd Województwa Mazowieckiego przyjął uchwałę w sprawie realizacji projektu własnego Województwa Mazowieckiego pn. „E-zdrowie dla Mazowsza 2” współfinansowanego ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Mazowieckiego na lata 2014-2020. Projekt zakładał m.in. budowę Mazowieckiego Centrum Obsługi Pacjenta poprzez opracowanie i wdrożenie e-usług: e-korespondencja, e-ankieta, e-rejestracja, chat z lekarzem, e-zgoda, rozbudowę Regionalnego Repozytorium Elektronicznej Dokumentacji Medycznej oraz budowę archiwum długoterminowego realizującego obowiązek przechowywania archiwalnych dokumentów medycznych w postaci elektronicznej, uruchomienie Chatbota udzielającego krótkich odpowiedzi na pytania pacjentów czy budowę Data Center na potrzeby udostępniania Partnerom usług chmurowych<sup>41</sup>. Obecnie trwają prace związane z projektem e-zdrowie dla Mazowsza 3, które przewidują działania związane m.in. z budową centrum teleradiologii z wykorzystaniem AI, modernizację data center, wsparcie w digitalizacji dokumentacji oraz podniesienie poziomu cyberbezpieczeństwa.

Warto podkreślić, że plany związane z rozwojem e-zdrowia na poziomie centralnym i regionalnym powinny być ze sobą spójne, co wymaga zaangażowania różnych interesariuszy już na etapie ich projektowania. Rozwiązania regionalne powinny uzupełniać i rozwijać systemy centralne, nie powinno dochodzić do sytuacji, w której regionalne platformy e-zdrowia powielają inicjatywy centralne lub nie są zintegrowane z systemem centralnym.

## **3.4 Kolejny krok w kierunku otwartości danych – akt w sprawie zarządzania danymi**

### **3.4.1 Podstawowa charakterystyka**

Na bazie europejskiej strategii w zakresie danych, w maju 2022 r. Rada Unii Europejskiej zatwierdziła Data Governance Act, czyli rozporządzenie w sprawie europejskiego zarządzania danymi (Akt w sprawie zarządzania danymi). DGA wprowadza nowe regulacje dotyczące korzystania z danych oraz pośrednictwa w ich udostępnianiu, które mają na celu ułatwienie wymiany informacji w Unii Europejskiej. Przepisy aktu są stosowane od 24 września 2023 r. Zmiany, które niesie ze sobą DGA, mogą w istotny sposób wpłynąć na procesy wtórnego przetwarzania danych w całej Europie. Podstawowe regulacje wprowadzane przez akt dotyczą ustanowienia warunków ponownego wykorzystywania danych będących w posiadaniu podmiotów publicznych oraz stworzenia ram prawnych dla świadczenia usług ich pośrednictwa. Ponadto, rozporządzenie reguluje status „altruistycznego” podejścia do danych oraz powoła nowy organ - Europejską Radę ds. Innowacji w zakresie danych.

41. <https://geodezja.mazovia.pl/projekty/e-zdrowie-2/projekt-e-zdrowie-2.html#oppro>

### 3.4.1.1 Warunki ponownego wykorzystywania danych

Organy publiczne gromadzą dane, które mogłyby wesprzeć rozwój sektora ochrony zdrowia. Często jednak, z uwagi na swój poufny charakter, są one poza możliwością ich wykorzystania w interesie publicznym. W związku z tym, prawodawca unijny zdecydował się na wprowadzenie mechanizmu ponownego wykorzystywania określonych kategorii danych znajdujących się w zasobach sektora publicznego. DGA nakłada na organy sektora publicznego obowiązek zapewnienia odpowiedniego poziomu prywatności i bezpieczeństwa informacji – w celu ich ponownego wykorzystywania. Może to obejmować m.in. przetworzenie wstępne, jeżeli ma ono na celu poddanie anonimizacji bądź pseudoanonimizacji danych osobowych.

Polska jest zobowiązana do ustanowienia punktu kontaktowego wspierającego naukowców i innowacyjne przedsiębiorstwa w identyfikacji odpowiednich danych. Obecnie wciąż trwają prace legislacyjne nad projektem ZarządDanU, która zawierać będzie regulacje uzupełniające względem przepisów DGA. Ich przyjęcie jest w praktyce niezbędne dla umożliwienia stosowania kluczowych rozwiązań wprowadzanych przez DGA.

### 3.4.1.2 Ramy świadczenia usług pośrednictwa danych

Prawodawca europejski dostrzega istotną rolę, jaką pełnią usługi udostępniania danych w kształtującej się gospodarce cyfrowej, w tym np. poprzez organizacje niezależnych ekosystemów wymiany informacji. Dlatego też DGA nakłada nowe obowiązki na dostawców usług udostępniania danych, m.in. na przedsiębiorców zajmujących się pośrednictwem w ich przepływie oraz tworzeniem systemów ich swobodnej wymiany.

#### Obowiązki nakładane przez DGA na dostawców to m.in.:

- Zgłoszenie wykonywanej działalności do odpowiedniego organu;
- Wykorzystywanie zebranych w ramach świadczenia danej usługi danych wyłącznie do celów rozwoju tej usługi;
- Zapewnienie ciągłości świadczenia usług, również w przypadku niewyptacalności;
- Zapewnienie przejrzystej, sprawiedliwej i niedyskryminującej procedury dostępu do danych;
- Wprowadzenie odpowiednich środków technicznych, prawnych i organizacyjnych w celu zapobieganiu niezgodnemu z prawem przekazywaniu danych.

W myśl przepisów DGA, dostawca jest zobowiązany do działania w najlepszym interesie osób, których dane dotyczą, ułatwiając im wykonywanie ich praw, w szczególności doradzając w zakresie potencjalnego wykorzystania danych i standardowych warunków związanych z takim wykorzystaniem.

### 3.4.1.3 Altruistyczne podejście do danych

DGA reguluje kwestie dobrowolnego, nieodpłatnego udostępnienia swoich danych przez osoby fizyczne lub prawne dla celów wspólnego dobra. Zjawisko to nazywane jest w rozporządzeniu „altruistycznym podejściem do danych” i opiera się na odpowiednio wysokim poziomie społeczeństwa obywatelskiego - chęci wsparcia rozwoju zdrowia poprzez udostępnienie zanonimizowanych informacji na swój temat.

Zgodnie z art. 2 pkt 10 DGA, altruistyczne podejście do danych oznacza „zgodę udzieloną przez osoby, których dane dotyczą, na przetwarzanie dotyczących ich danych osobowych lub zezwolenia innym posiadaczom danych na wykorzystywanie ich danych nieosobowych bez żądania wynagrodzenia, do celów realizowanych w interesie ogólnym, takich jak cele badań naukowych lub poprawa jakości usług publicznych”. W celu wykorzystania potencjału płynącego z altruizmu społecznego, w pierwszej kolejności DGA przewiduje stworzenie rozwiązań ułatwiających swobodną i bezpieczną wymianę informacji. Podmiotami tworzącymi system altruistycznego podejścia do danych mają być jednostki non-profit sektora społecznego, które będą miały możliwość – po spełnieniu warunków – zarejestrowania się jako uznane organizacje altruizmu danych.

### 3.4.1.4 Europejska Rada ds. Innowacji w zakresie danych

Rozporządzenie przewiduje powołanie eksperckiej grupy, która będzie pełniła rolę doradczą oraz wspierającą działania Komisji Europejskiej w zakresie danych – Europejską Radę ds. Innowacji w zakresie danych. Organ będzie złożony z przedstawicieli wszystkich państw członkowskich Unii Europejskiej oraz reprezentantów organizacji wspólnotowych.

## 3.4.2 Wybrane wyzwania

### 3.4.2.1 Przygotowanie się do obowiązku udostępniania danych

Organy sektora publicznego są zobowiązane do publicznego udostępnienia warunków wydania zezwolenia na uzyskanie dostępu do danych w celu ich ponownego wykorzystania. Warunki te powinny być niedyskryminujące, proporcjonalne i obiektywnie uzasadnione. Informacje o udostępnianiu danych oraz warunków wydania zezwolenia na uzyskanie dostępu powinny być dostępne za pośrednictwem pojedynczego punktu informacyjnego.

W udostępnianiu danych na cele ich ponownego wykorzystania, centralną rolę będzie odgrywał „podmioty właściwy”, którym – zgodnie z procedowanym projektem ZarządDanU, ma być Prezes Głównego Urzędu Statystycznego – w zakresie danych chronionych ze względu na poufność informacji statystycznych, oraz Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy – w zakresie pozostałych danych.

Wsparcie realizowane przez te podmioty będzie polegało m.in. na wsparciu technicznym poprzez udostępnienie bezpiecznego środowiska przetwarzania w celu zapewnienia dostępu do ponownego wykorzystywania danych, wsparciu technicznym w zakresie stosowania sprawdzonych technik zapewniających przetwarzanie danych w sposób chroniący prywatność informacji zawartych w danych, których ponowne wykorzystywanie jest dozwolone, w tym technik pseudonimizacji,

anonimizacji, uogólnienia, ukrywania i randomizacji danych osobowych, udzielaniu pomocy organom sektora publicznego, w razie potrzeby, w uzyskaniu zgody lub zezwolenia od podmiotów ponownie wykorzystujących dane na ponowne wykorzystywanie do celów związanych z altruistycznym podejściem do danych i innych, zgodnie z określonymi decyzjami posiadaczy danych, w tym dotyczącymi jurysdykcji, w których ma nastąpić przetwarzanie danych, a także zapewnieniu organom sektora publicznego pomocy w zakresie adekwatności zobowiązań podjętych przez podmiot ponownie wykorzystujący dane.

Ponadto, zgodnie z artykułem 8 DGA, obowiązkiem państw członkowskich jest zapewnienie, aby wszystkie istotne informacje dotyczące ponownego użycia danych będących w posiadaniu sektora publicznego były dostępne za pośrednictwem pojedynczego punktu kontaktowego. Zgodnie z procedowaną ZarządDanU, rolę tego podmiotu będzie w Polsce pełnił portal danych, o którym mowa w art. 2 pkt 13 OtwDanU, prowadzony przez ministra właściwego ds. informatyzacji. Pojedynczy punkt kontaktowy m.in. udostępnia drogą elektroniczną rejestr dostępnych zasobów danych zawierający odpowiednie informacje opisujące charakter dostępnych danych. Ostatecznie jednak – za udzielenie dostępu do danych, będą odpowiadać – w zależności od kategorii informacji - NASK lub Prezes GUS.



### Rekomendacje:

Dane o stanie zdrowia są szczególnymi kategoriami danych, które podlegają pod dedykowane regulacje prawne. Od lat proces informatyzacji sektora ochrony zdrowia prowadzony jest w pewnej autonomii od innych procesów cyfryzacji państwa przez dedykowany podmiot, którym jest Centrum e-Zdrowia (dawniej CSIOZ). Ze względu na szczególną wagę danych medycznych oraz dotychczasowe doświadczenia związane z ich wykorzystywaniem powinna zostać zapewniona pełna transparentność procesu dostępu do nich. Uzasadnione jest powołanie nowej, niezależnej jednostki, która sprawowałaby nadzór w tym zakresie. W związku z tym, a także w celu zapewnienia lepszej implementacji DGA i większego wsparcia podmiotów leczniczych, rekomenduje się aby „podmiotem właściwym”, o którym mowa w DGA, w obszarze tego rodzaju informacji był docelowo nowy, wyspecjalizowany podmiot, w skład którego wchodzić będą m.in. specjaliści w zakresie danych osobowych oraz ochrony zdrowia. Dla zapewnienia niezależności podmiot ten powinien mieć charakter ponad resortowy i podlegać Prezesowi Rady Ministrów. Alternatywnie, zamiast powoływać nowy podmiot możliwe jest wydzielenie nowego działu w strukturach już obecnie funkcjonującego podmiotu, pod warunkiem proceduralnego zapewnienia mu gwarancji niezależności.

W przypadku pojedynczego punktu kontaktowego przyjęte rozwiązanie może nie spełnić celów ujednoczenia systemu obrotu danych medycznych, a jedynie niepotrzebnie skomplikować jego strukturę. Obecnie, na poziomie Unii Europejskiej, procedowane jest rozporządzenie tworzące Europejską Przestrzeń Danych Dotyczących Zdrowia (EHDS). W związku z tym, mając na uwadze nadchodzące specjalne rozwiązanie prawne dotyczące przetwarzania danych medycznych, należy rozważyć wydzielenie osobnego podmiotu dla tego rodzaju informacji, którym mogłaby być przywołana w poprzednim akapicie jednostka.

### 3.4.2.2 Stworzenie mechanizmu zachęt do ponownego wykorzystywania danych i promowanie altruizmu

Pozytywnie należy ocenić działania prawodawcy zmierzające do wykorzystania potencjału płynącego z altruistycznego podejścia do danych. Warto podkreślić, że samo stworzenie ram prawnych nie jest wystarczające dla zapewnienia funkcjonalności systemu altruistycznego. Istotne jest podejmowanie działań zmierzających do promowania postaw pożądanых – dobrowolnego dzielenia się swoimi danymi na cele rozwoju systemu zdrowia. Ważnym zagadnieniem jest również rozwijanie świadomości społecznej na temat wartości danych zdrowotnych dla postępu technologicznego, naukowego oraz wzrostu możliwości organizacyjnych.

Doniosłą rolę w tym obszarze pełnić będzie również podmiot właściwy, którego zadaniem jest m.in. prowadzenie rejestru uznanych organizacji o altruistycznym podejściu do danych. Tym bardziej istotne jest, aby w zakresie danych zdrowotnych, takim podmiotem został nowy podmiot, w skład którego wchodzić będą specjaliści w zakresie danych osobowych oraz systemu ochrony zdrowia, stworzony specjalnie do tego celu – organ wyspecjalizowany w przetwarzaniu danych dot. stanu zdrowia.



#### Rekomendacje:

Strona publiczna powinna promować altruizm danych. Nowe regulacje stwarzają możliwość dzielenia się danymi w celu ich wykorzystania na rzecz rozwoju nauk medycznych, warto więc na różny sposób wspierać inicjatywy w tym zakresie. Aby system sprawnie działał, zasadne jest budowanie zaufania i świadomości wśród pacjentów – pacjenci powinni rozumieć, dlaczego wykorzystywanie ich danych jest tak ważne. Podmiotem, który mógłby prowadzić tego rodzaju działania mógłby być nowo powołany podmiot, o którym mowa w poprzednim podpunkcie lub Agencja Badań Medycznych, która ma już doświadczenie w akcjach podnoszenia świadomości w obszarze eksperymentów medycznych i badań klinicznych.

## 3.5 Szeroki dostęp do danych – akt w sprawie danych

### 3.5.1 Podstawowa charakterystyka

Procedowane rozporządzenie Parlamentu Europejskiego i Rady w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania (akt w sprawie danych) ma określać, kto może korzystać z danych generowanych w Unii Europejskiej. Akt ma na celu zapewnienie sprawiedliwości w środowisku cyfrowym, pobudzenie konkurencji na rynku danych oraz otwarcie się na możliwości innowacji, jakie niesie ze sobą ich wykorzystywanie.

Akt w sprawie danych sygnalizuje problemy leżące u podstaw niedostatecznego wykorzystywania danych oraz proponuje kierunki działań, które należy podjąć w celu ich rozwiązania. Wśród najważniejszych obszarów, które ma normować omawiane rozporządzenie, znajdują się m.in.:

- środki umożliwiające użytkownikom urządzeń podłączonych do sieci internetowej uzyskanie dostępu do generowanych przez nie danych, które często są gromadzone wyłącznie przez producentów tych urządzeń;
- środki umożliwiające organom sektora publicznego dostęp do danych i wykorzystanie danych, którymi dysponuje sektor prywatny i które są niezbędne w wyjątkowych okolicznościach, zwłaszcza w przypadku sytuacji nadzwyczajnych;
- środki umożliwiające klientom skuteczną zmianę dostawców usług przetwarzania danych w chmurze oraz wprowadzające zabezpieczenia przed niezgodnym z prawem przekazywaniem danych.

## 3.5.2 Wybrane wyzwania

### 3.5.2.1 Znaczenie regulacji dla sektora ochrony zdrowia

W art. 4 omawianego aktu uregulowano uprawnienie użytkowników produktów, w tym m.in. potencjalnie wyrobów medycznych, do dostępu do danych generowanych w wyniku korzystania z tych produktów. Przepis ten umożliwia złożenie wniosku do producenta poszczególnego wyrobu, aby ten wydał użytkownikowi, którego dane dotyczą, wszelkie zebrane przez wyrób medyczny informacje. W konsekwencji, po wprowadzeniu aktu w sprawie danych, może potencjalnie pojawić się możliwość korzystania z informacji gromadzonych przez producentów, które wcześniej pozostawały wyłącznie do dyspozycji przedsiębiorców wprowadzających na rynek wyroby medyczne. Warunki, na jakich posiadacze danych udostępniają informacje odbiorcom, obejmują dane definiowane jako wszelkie cyfrowe odwzorowania działań, faktów lub informacji oraz wszelkie kompilacje takich działań, faktów lub informacji, w tym w formie zapisu dźwiękowego, wizualnego lub audiowizualnego. W konsekwencji, akt w sprawie danych reguluje obowiązek udostępniania również danych dotyczących zdrowia, które np. nie mieszczą się w pojęciu dokumentacji medycznej.



#### Rekomendacje:

Prace nad DA nie mają charakteru sektorowego. Kwestią wymagającą dokładniejszej analizy pozostaje to, jaki potencjalnie nowy zasób danych stanie się możliwy do uzyskania w kontekście klinicznym oraz czy będzie miał on znaczenie dla pracy lekarza. Potencjalnie regulacje DA mogą dać pacjentom możliwość uzyskania surowych danych z wyrobów medycznych, a te mogą wносить nową wartość dla oceny stanu zdrowia pacjenta lub służyć weryfikacji wyników dostarczonych przez wyrób (co może mieć szczególne znaczenie w kontekście narzędzi wykorzystujących AI). Jeżeli wiązałyby się z tym istotna korzyść, warto rozważyć poszerzenie DA o zapewnienie tej kategorii danych dla personelu medycznego.

Mając na uwadze zmiany prawne wynikające z DA i DGA warto rozważyć wprowadzenie rozwiązań technicznych i organizacyjnych, które ułatwią egzekwowanie nowych uprawnień. Przykładowo, pacjent mógłby z poziomu IKP wyrażać zgody na udostępnianie jego danych osobowych, w tym m.in. danych surowych przetwarzanych przez dostawców wyrobów medycznych lub

innych urządzeń generujących dane związane ze zdrowiem. W związku z tym bardzo ważną pozostaje kwestia wyraźnego odróżnienia danych z różnych źródeł, które mogą różnić się jakością i wiarygodnością, co zostało szerzej omówione w dalszej części raportu (por. punkt 5.3.1.2).

### 3.5.2.2 Dostęp strony publicznej do danych medycznych przetwarzanych przez prywatne podmioty lecznicze

Akt w sprawie danych przewiduje w art. 14 obowiązek udostępniania danych podmiotom publicznym przez sektor prywatny pod warunkiem wykazania przez te podmioty istnienia wyjątkowej potrzeby skorzystania z żądanych danych. Wykaz przesłanek, które mogą stanowić „wyjątkową potrzebę” zawarty jest w artykule 15 i przewiduje sytuacje:

- gdy żądane dane są niezbędne do zareagowania na niebezpieczeństwo publiczne;
- gdy wniosek o udostępnienie danych jest ograniczony w czasie i zakresie oraz niezbędny do zapobieżenia niebezpieczeństwu publicznemu lub do pomocy w przywracaniu stanu wyjściowego po wystąpieniu niebezpieczeństwa publicznego;
- gdy brak dostępnych danych uniemożliwia organowi sektora publicznego lub instytucji, agencji lub organowi Unii realizację konkretnego zadania leżącego w interesie publicznym i wyraźnie wskazanego w prawie, przy spełnieniu co najmniej jednej z dwóch dodatkowych przesłanek<sup>42</sup>.

Z omawianej regulacji wyłączone jednak będą małe i średnie przedsiębiorstwa, które unijny prawodawca postanowił poddać szczególnej ochronie w ramach omawianego rozporządzenia.



#### Rekomendacje:

Mając na uwadze szczególnie wrażliwy charakter danych medycznych oraz ryzyko potencjalnych nadużyć związanych z dostępem do nich na podstawie klauzuli generalnej „wyjątkowej potrzeby”, pomimo zabezpieczeń przewidzianych w samej regulacji DA, zasadne jest stworzenie dodatkowego mechanizmu nadzoru nad takim dostępem. Przykładowo, mógłby on zostać poprzedzony obowiązkiem zwrócenia się przez organ władzy publicznej o wydanie opinii do co najmniej jednego niezależnego podmiotu, np. Rzecznika Praw Obywatelskich, o wystąpieniu w danej sytuacji „wyjątkowej potrzeby”. Opinia taka mogłaby mieć charakter „miękkiej” i nie być wiążąca, co nie ingerowałoby w system kreowany przez projektowane przepisy DA, a jednocześnie tworzy dodatkowy mechanizm nadzoru.

42. Wskazany przesłanka może stanowić „wyjątkową potrzebę” wyłącznie gdy:

- a) organ sektora publicznego lub instytucja, agencja lub organ Unii nie były w stanie uzyskać takich danych za pomocą alternatywnych środków, w tym w drodze zakupu danych na rynku po stawkach rynkowych lub poprzez poleganie na istniejących obowiązkach udostępniania danych, a przyjęcie nowych środków ustawodawczych nie może zapewnić terminowej dostępności danych; lub
- b) uzyskanie danych zgodnie z procedurą określoną w niniejszym rozdziale znacznie zmniejszyłoby obciążenie administracyjne posiadaczy danych lub innych przedsiębiorstw.



## 3.6 Zdrowie jako priorytet - europejska przestrzeń danych dotyczących zdrowia

### 3.6.1 Podstawowa charakterystyka

Na fundamentach europejskiej strategii w zakresie danych, przewidującej stworzenie uniwersalnych środowisk wymiany informacji w kluczowych dla rozwoju gospodarki cyfrowej obszarach, powstaje Europejska Przestrzeń Danych Dotyczących Zdrowia (ang. European Health Data Space – EHDS). 3 maja 2022 r. Komisja Europejska opublikowała projekt rozporządzenia EHDS. Akt ma w założeniu stworzyć ramy wymiany danych dotyczących zdrowia - ustanowić jasne zasady, wspólne normy i praktyki, infrastrukturę oraz ramy zarządzania w zakresie korzystania z elektronicznych danych medycznych. Beneficjentami wprowadzenia EHDS w pierwszej kolejności będą pacjenci. Otrzymają oni narzędzia, dzięki którym będą mieli możliwość lepszej i prostszej kontroli nad swoimi danymi. Zyska również sektor ochrony zdrowia – planowana „przestrzeń” umożliwi prostsze pozyskanie danych do celów ich użycia wtórnego - rozwoju badań, wprowadzania innowacji, kształtowania polityki zdrowotnej, podwyższenia poziomu bezpieczeństwa pacjentów, statystyk lub celów regulacyjnych<sup>43</sup>.

EHDS wzmacnia prawa pacjenta związane z dostępnością i kontrolą elektronicznych danych dotyczących zdrowia. Znaczna część uprawnień przewidzianych w przepisach rozporządzenia to instytucje istniejące już wcześniej w systemie prawa, które są wzmacniane i konkretyzowane poprzez proponowane regulacje. Uprawnienia pacjentów przewidziane przepisami EHDS to m.in.:

- Prawo dostępu do danych dotyczących zdrowia przez osoby których te dane dotyczą;
- Prawo do otrzymania elektronicznej kopii swoich danych;
- Prawo wprowadzania informacji do swojej elektronicznej dokumentacji medycznej;
- Prawo do żądania od posiadacza danych dotyczących pacjenta, by ten udostępnił je wskazanym podmiotom trzecim;
- Prawo pacjentów do ograniczenia dostępu pracowników medycznych do swojej dokumentacji.

EHDS ustanawia przepisy dotyczące wprowadzania do obrotu, udostępniania na rynku lub wprowadzania do używania systemów elektronicznej dokumentacji medycznej. Poprzez stworzenie uniwersalnego, europejskiego formatu wymiany elektronicznej dokumentacji medycznej, procedowane rozporządzenie przyczyni się do ujednoczenia systemów IT w których przetwarza się dane medyczne, a w konsekwencji – do zwiększenia swobody przepływu informacji dotyczących zdrowia.

Kluczowym obszarem normowanym przez omawiany akt jest wtórne wykorzystywanie elektronicznych danych dotyczących zdrowia. EHDS przewiduje rozwiązania, dzięki którym dane uzyskane pierwotnie w celu udzielania świadczeń zdrowotnych indywidualnemu pacjentowi, będą poddawane anonimizacji lub pseudoanonimizacji, a następnie ponownie wykorzystywane do celów podwyższania jakości systemu opieki zdrowotnej.

43. BRAK OPISU W WORDZIE

Możliwości, jakie niesie ze sobą EHDS, wymagają utworzenia organów centralnych na poziomie Unii Europejskiej, które będą odpowiedzialne za harmonizację procesów wymiany informacji na terenie wspólnoty. W związku z tym, zdecydowano się zobligować państwa członkowskie do utworzenia krajowych punktów kontaktowych. Na poziomie wspólnotowym natomiast powołana zostanie centralna platforma e-Zdrowia. Dane zdrowotne służące do celów ich pierwotnego wykorzystywania, czyli na rzecz indywidualnych potrzeb pacjentów, będą wymieniane za pośrednictwem międzynarodowej infrastruktury MojeZdrowie@UE (MyHealth@EU). Przepływ danych przetwarzanych w celu ich użycia wtórnego, m.in. na potrzeby badań czy organizacji systemu ochrony zdrowia, ma zapewniać natomiast infrastruktura DaneZdrowotne@UE (HealthData@EU).

## 3.6.2 Wybrane wyzwania

### 3.6.2.1 Nowe podejście do definicji danych

Zgodnie z definicją zawartą w EHDS, „elektroniczne dane osobowe dotyczące zdrowia” oznaczają dane dotyczące zdrowia i dane genetyczne w rozumieniu rozporządzenia (UE) 2016/679, a także dane odnoszące się do czynników warunkujących zdrowie lub dane przetwarzane w związku z udzielaniem świadczeń zdrowotnych, przetwarzane w formie elektronicznej.

Kwestie związane z nową siatką terminologiczną zostały szerzej omówione w punkcie 5.3.1.1 raportu.

Na tle przytaczanej definicji pojawia się pytanie o rozumienie pojęcia „danych odnoszących się do czynników warunkujących zdrowie”. W systemie prawa brak jest odpowiedniej definicji tego wyrażenia. Zgodnie z poglądem Światowej Organizacji Zdrowia, czynnikami warunkującymi zdrowie są m.in. pokój, schronienie, edukacja, żywność, dochody, stabilny ekosystem, zrównoważone zasoby oraz sprawiedliwość społeczną i równość. Podejście to zdaje się jednak być zbyt ogólne, biorąc pod uwagę cele EHDS. Niejasności w tym zakresie mogą wywołać istotny wpływ na definicję elektronicznych danych osobowych dotyczących zdrowia, która stanowi kluczowy element EHDS.



#### Rekomendacje:

EHDS wymuszać będzie zmianę utrwalonego podejścia do danych pacjentów. W Polsce skupia się ono obecnie na tradycyjnym pojęciu dokumentu, który jest opatrzony podpisem. Z kolei EHDS skupia się na danych medycznych (których zbiory mogą tworzyć dokumenty), które będą mogły funkcjonować poza tak rozumianą dokumentacją medyczną. Taka zmiana optyki – przejście od tradycyjnego systemu informacji medycznej opartego o centralne pojęcie „dokumentu”, który ma swoje źródło w papierowej dokumentacji, na system oparty o pojęcie „danych” - powinna być punktem wyjścia do uregulowania nowego systemu przetwarzania danych pacjenta – zapowiadanej w Programie rozwoju e-zdrowia w Polsce do 2027 r. ustawie o danych medycznych. Tym samym regulacje, na wzór projektowanych regulacji EHDS, powinny operować pojęciem elektronicznych danych dotyczących zdrowia (lub podobnym), których zbiory, spełniające określone kryteria oraz autoryzowane podpisem przez pracownika medycznego, stanowić będą odpowiednik obecnej dokumentacji medycznej. Zagadnienie to zostało szerzej przedstawione w punkcie 5.3.8 raportu.

### 3.6.2.2 Dostosowanie systemu EDM i IKP do standardu EHDS

EHDS przewiduje nowe uprawnienia pacjentów, które powinny zostać odpowiednio wdrożone do krajowych systemów teleinformatycznych obsługujących sektor ochrony zdrowia. Obecnie, w Internetowym Koncie Pacjenta brak jest m.in. instytucji, o której mowa w art. 3 ust. 6 rozporządzenia EHDS – uprawnienia do wprowadzania przez pacjentów danych dotyczących zdrowia do własnej elektronicznej dokumentacji medycznej lub do elektronicznej dokumentacji medycznej osób fizycznych, do których informacji dotyczących zdrowia mają dostęp.

Uzasadnione będzie także wdrożenie w mechanizmy IKP funkcji prostego i szybkiego zgłoszenia żądania sprostowania danych zawartych w systemie. Zgodnie z art. 3 ust. 7 EHDS, państwa członkowskie będą musiały zapewnić, aby przy korzystaniu z prawa do sprostowania danych na podstawie art. 16 rozporządzenia (UE) 2016/679 osoby fizyczne mogły z łatwością wystąpić o sprostowanie online za pośrednictwem usług dostępu do elektronicznych danych dotyczących zdrowia.

W art. 5 EHDS, wymieniono priorytetowe kategorie elektronicznych danych osobowych dotyczących zdrowia do celów ich pierwotnego wykorzystywania: skrócone karty zdrowia pacjenta, recepty elektroniczne, realizacja recept elektronicznych, obrazy medyczne i wyniki obrazowania medycznego, wyniki badań laboratoryjnych, wypisy. Ponadto, zgodnie z art. 5 ust. 2, Komisja Europejska może rozszerzyć ten katalog w drodze aktów wykonawczych.



#### Rekomendacje:

Projektując kolejne zmiany w obszarze e-zdrowia należy pamiętać o wymogach, które może wprowadzić EHDS. Wiązać się one mogą z koniecznością dostosowania IKP do nowych funkcjonalności oraz dostosowaniem katalogu EDM tak, by obejmował co najmniej wszystkie dane z kategorii „danych priorytetowych”, o których mowa w art. 5 ust. 1 EHDS. Nie należy przy tym zakładać, że podstawowym repozytorium danych medycznych będzie jakkolwiek system centralny. Dane stanowiące dokumentację medyczną są i powinny być gromadzone lokalnie przez podmioty medyczne, a możliwość ich udostępniania innym podmiotom medycznym i bezpośrednio pacjentowi powinna wynikać z poprawnego wdrożenia standardów i profili interoperacyjności.

### 3.6.2.3 Standard wtórnego wykorzystywania danych

Gromadzenie danych w celu ich wtórnego wykorzystania budzi wątpliwości z perspektywy zapewnienia prawa do prywatności osób, których dane dotyczą. W związku z tym, unijny prawodawca zdecydował się na wprowadzenie minimalnych standardów wtórnego wykorzystywania danych. Zgodnie z nimi, organ ds. dostępu do danych będzie musiał zapewnić, aby udzielony dostęp dotyczył wyłącznie elektronicznych danych dotyczących zdrowia związanych z celem przetwarzania, wskazanych we wniosku o udzielenie dostępu do danych i by był zgodny z udzielonym zezwoleniem na dostęp do danych. Ponadto, rozporządzenie przewiduje obowiązek: anonimizacji danych lub pseudonimizacji danych, w przypadku gdy zanonimizowane dane nie umożliwiają osiągnięcia celu przetwarzania.

Co ważne, na gruncie projektowanych regulacji EHDS państwa członkowskie będą musiały wyznaczyć krajowy punkt kontaktowy ds. wtórnego wykorzystywania elektronicznych danych dotyczących zdrowia, czyli organizacyjną i techniczną bramę umożliwiającą transgraniczne wtórne wykorzystywanie danych. Do zadań krajowego punktu kontaktowego należy m.in. podejmowanie decyzji w sprawie wniosków o udzielenie dostępu do danych na podstawie EHDS i wydawanie zezwolenia na dostęp do danych.

Pod kątem skuteczności nowego systemu ważną będzie szczegółowa architektura rozwiązań zapewniających dostęp do danych przeznaczonych do wtórnego wykorzystania. Krajowy punkt kontaktowy ds. wtórnego wykorzystywania elektronicznych danych dotyczących zdrowia będzie miał zadanie m.in. przetwarzać elektroniczne dane dotyczące zdrowia do celów realizacji wniosków o dostęp, czyli m.in. będzie gromadził, łączył, przygotowywał i ujawniał te dane do celów wtórnego wykorzystywania. Proces ten może zostać zaprojektowany w modelu centralnym, w którym dane udostępniane byłyby np. bezpośrednio z poziomu systemu P1, który przechowuje część danych oraz indeksuje dane przechowywane na poziomie lokalnym, lub w rozproszonym, z wykorzystaniem m.in. powstających regionalnych repozytoriów elektronicznej dokumentacji medycznej czy rejestrów medycznych. Kluczowa pozostaje przy tym wspomniana już wcześniej kwestia interoperacyjności.



### Rekomendacje:

Jednym z podstawowych problemów związanych z dostępem do danych medycznych jest brak jasnych i powszechnie uznanych standardów anonimizacji lub pseudonimizacji danych medycznych. Bez ich wypracowania stosowanie EHDS może być znacząco utrudnione. Kwestia ta została szerzej omówiona w punkcie 5.3.5.3 raportu, który wskazuje na pilną potrzebę wypracowania jasnych wytycznych dotyczących przeprowadzania operacji pseudonimizacji i anonimizacji o stanie zdrowia zgodnie z wymogami RODO.

Należy także rozpocząć szerszą dyskusję nad krajowym punktem kontaktowym, czyli podmiotem odpowiedzialnym za przyznawanie dostępu do danych medycznych m.in. w celach naukowych lub badawczo rozwojowych. Warto rozważyć powołanie w tym celu nowego, niezależnego podmiotu, który współpracowałby ściśle w szczególności z Centrum E-Zdrowia, Agencją Badań Medycznych oraz AOTMiT<sup>44</sup>. Podmiot ten powinien być odpowiedzialny za udostępnianie danych medycznych z sektora ochrony zdrowia w formule „jednego okienka”, co powinno zapewnić lepszą koordynację oraz większą przejrzystość i kontrolę nad dostępem. Alternatywnie, zamiast powoływać nowy podmiot możliwe jest wydzielenie nowego działu w strukturach już obecnie funkcjonującego podmiotu, np. ABM, pod warunkiem proceduralnego zapewnienia mu gwarancji niezależności. Tak samo, pod kątem organizacji systemu udostępniania danych ważną będzie docelowa architektura systemu.

44. Powołanie nowego podmiotu powinno zostać poprzedzone dokładną analizą zasadności takiego działania względem powierzenia wybranych zadań już funkcjonującym instytucjom

## 3.7 Jakie inne regulacje wpłyną na obszar danych medycznych?

### 3.7.1 AI Act - podstawowa charakterystyka

Jednym z celów wprowadzania rozwiązań gwarantujących lepszy przepływ i dostępność danych medycznych jest zapewnienie „paliwa” dla szybko rozwijanych algorytmów AI. Systemy AI mogą istotnie wpłynąć na ułatwienie pracy lekarzom. W procesie diagnostycznym, analiza dokumentacji medycznej pacjenta przez sztuczną inteligencję pomoże wykryć nieprawidłowości i nakierować personel medyczny na aspekty, które odchodzą od normy. Za pomocą analiz danych treningowych przez algorytmy AI, personel medyczny będzie w stanie lepiej dostosować rekomendacje dotyczące aktywności fizycznej do dobrostanu konkretnego pacjenta.

W związku z rosnącym potencjałem AI, Unia Europejska zdecydowała się na wprowadzenie przepisów, które mają na celu przede wszystkim ochronę prywatności przed algorytmami stwarzającymi wysokie ryzyko jej naruszenia. Z rozwojem sztucznej inteligencji wiąże się wzrost możliwości wykorzystywania danych, jednocześnie jednak – proces ten wiąże się z zagrożeniami, zwłaszcza w kontekście prawa do prywatności. Dlatego też 14 czerwca 2023 r. Parlament Europejski przyjął AI Act - rozporządzenie Parlamentu Europejskiego i rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji.

Głównym zagadnieniem wprowadzanym przez AI Act jest podział systemów wykorzystujących AI na trzy poziomy ryzyka: „niedopuszczalne ryzyko”, „wysokie ryzyko” oraz „niskie lub minimalne ryzyko”. Użyciem systemów, które prawodawca unijny zaliczy do pierwszej kategorii powyższej systematyki, będzie - co do zasady - zupełnie zakazane. Dotyczy to między innymi AI, które pozyskują dane biometryczne w czasie rzeczywistym w przestrzeni publicznej. Systemy zaliczone do grupy wysokiego ryzyka – mogące stanowić zagrożenie m.in. dla zdrowia - nie będą zakazane. Ich wprowadzenie na rynek zostanie jednak poddane ścisłej reglamentacji organów unijnych.

#### 3.7.1.1 Kategoryzacja danych pod kątem AI

Przepisy AI Act będą regulować również kwestię danych treningowych, walidacyjnych oraz testowych. Pojęcia te oznaczają:

- **Dane treningowe** – zestaw informacji, który służy do nauki algorytmu AI – na podstawie tych danych algorytm uczy się odpowiedniej klasyfikacji;
- **Dane walidacyjne** – zestaw informacji używanych do przeprowadzanie nieobciążonego testu modelu AI, który wcześniej został wyuczony na bazie danych treningowych, w celu dostosowania hiperparametrów;
- **Dane testowe** - zestaw danych, nieznanych wcześniej algorytmowi, stosowanych do sprawdzenia poprawności działania algorytmu i ostatecznej oceny jego wydajności.

Rozwój AI będzie wymagał odpowiedniej kategoryzacji danych, mając na względzie ich specyfikę oraz przydatność do konkretnych obszarów sztucznej inteligencji. Należy bowiem pamiętać, że dane medyczne mają znaczenie dla rozwoju i wykorzystania algorytmów sztucznej inteligencji w ochronie zdrowia w dwojakim aspekcie:

1. ilościowym – sztuczną inteligencję znajdującą zastosowanie w medycynie musi cechować odpowiedni poziom precyzji i rzetelności, gwarantujący odpowiedni poziom bezpieczeństwa dla ich wykorzystania w procesie diagnostyczno-terapeutycznym pacjenta. Kluczowym aspektem pozwalającym algorytmom na osiągnięcie wymaganego poziomu precyzji jest uzyskanie dostępu na etapie ich rozwoju do adekwatnej wielkości bazy danych wraz z znacznikami, które to znaczniki następnie mają być identyfikowane w dostarczanych algorytmom danych na etapie wykorzystywania algorytmów.
2. jakościowym – dane dostarczane algorytmom, zarówno na etapie ich rozwoju jak i wykorzystania – im bardziej kompletne, ustandaryzowane i rzetelne dane, tym precyzyjniejszy będzie rozwijany algorytm oraz tym precyzyjniejsze będzie wydane przez niego rozstrzygnięcie. Jakość danych determinuje ich przydatność do wykorzystania w rozwoju i korzystaniu z algorytmów AI<sup>45</sup>.

Zgodnie z AI Act, systemy AI zaliczane do kategorii wysokiego ryzyka, opracowuje się na bazie zbiorów danych treningowych, walidacyjnych i testowych, które podlegają odpowiednim praktykom w zakresie zarządzania danymi. Praktyki te dotyczą w szczególności:

- odpowiednich decyzji projektowych;
- gromadzenia danych;
- odpowiednich operacji przetwarzania na potrzeby przygotowania danych, takich jak anotowanie, etykietowanie, czyszczenie, wzbogacanie i agregacja;
- sformułowanie odpowiednich założeń, zwłaszcza w odniesieniu do informacji, do których pomiaru i reprezentowania mają służyć dane;
- uprzedniej oceny dostępności, ilości i przydatności zbiorów danych, które są potrzebne;
- badania pod kątem ewentualnej tendencyjności;
- określenia wszelkich możliwych luk w danych lub braków w danych oraz tego, w jaki sposób można zaradzić tym lukom i brakom.



### Rekomendacje:

Projektując procesy związane z przetwarzaniem danych medycznych należy brać pod uwagę powyższe kategorie danych i związane z nimi wymogi. Należy wypracować standard gromadzenia danych, który zapewniłby ich odpowiednią jakość pod kątem możliwości ich wykorzystania rozwijania systemów AI. Dzięki temu dane wprowadzane przez lekarza przełożą się na ułatwienie pracy dzięki efektywniejszym systemom AI. Zbieranie i kategoryzowanie danych powinno być przy tym możliwe zautomatyzowane, by nie wiązało się dla lekarza z dodatkowym obowiązkiem. W innym przypadku może się okazać, że inwestycje związane z tworzeniem nowych systemów szybko stracą na znaczeniu, bo zbierane dane będą niepełne albo nie będą spełniać kryteriów umożliwiających ich wykorzystanie w celu rozwijania AI.

45. Koalicja AI / DZP; 2020 r.; Wykorzystanie danych medycznych w celu rozwoju AI w Polsce i w celu prowadzenia badań naukowych. Prawne uwarunkowania dostępu do danych medycznych i ich jakości.

### 3.7.1.2 Piaskownice regulacyjne

Zbyt szerokie i restrykcyjne obciążenie innowatorów w dziedzinie AI regulacjami prawnymi, może spowodować zastój rozwoju tego sektora w Europie. W związku z tym, korzystne zdaje się być zastosowanie rozwiązań „piaskownic regulacyjnych”, stanowiących specjalną, bezpieczną przestrzeń prawną stworzoną na potrzeby testowania i wdrażania nowych technologii. Piaskownice regulacyjne mają na celu umożliwienie prywatnym innowatorom, w szczególności start-upom, prostszego i efektywniejszego wejścia na rynek z nowatorską usługą lub produktem. Z uwagi na czasochłonność prac legislacyjnych, może zdarzyć się sytuacja, gdy prawo nie nadąży za postępem technologicznym. W związku z tym, tworzy się specjalną przestrzeń prawną, które – z uwagi na znacznie mniejsze restrykcje regulacyjne – umożliwia przetestowanie danego rozwiązania. W krajach Unii Europejskiej stosuje się piaskownice regulacyjne m.in. w branży FinTech. Mając jednak na uwadze specyfikę sektora Life Sciences, w tym trudności przedsiębiorców związane z szeroką reglamentacją działalności leczniczej i farmaceutycznej, wprowadzanie piaskownic regulacyjnych w tym zakresie może nieść ze sobą korzystne skutki dla rozwoju medycyny.

Konieczność stworzenia środowisk prawnych umożliwiających start-upom prowadzenie działalności związanej z danymi medycznymi wynika m.in. z doniesień o spadającej popularności w rozwiązań w tym sektorze. Jak wynika z 4. edycji raportu Top Disruptors in Healthcare, „z pewnością w przyszłości będziemy mogli zobaczyć więcej rozwiązań opartych o samodzielną aplikację IT. W sektorze danych medycznych można zaobserwować spadającą popularność, mimo iż w ciągu dwóch lat nieznacznie wzrosła ilość startupów w nim działających. Może to wynikać z faktu, że sektor danych medycznych nie jest jeszcze wystarczająco uregulowany prawnie i stąd wynika trudność w pozyskaniu i wykorzystywaniu danych”<sup>46</sup>.



#### Rekomendacje:

W sektorze ochrony zdrowia należy rozpocząć wykorzystywać instytucje piaskownic regulacyjnych do wspierania rozwoju AI. Jest to stosunkowo innowacyjne rozwiązania pod kątem prawnym, dlatego warto jak najwcześniej rozpocząć prace koncepcyjne nad kształtem przyszłych uregulowań. Podobnie jak do testowania nowych rozwiązań medycznych lub systemowych w ochronie zdrowia wykorzystuje się pilotaże, tak też można tworzyć preferencyjne rozwiązania prawne, które pozwolą lepiej poznać i przetestować innowacje. W ramach tego rodzaju instrumentów prawnych należy pogodzić ewentualne ułatwienia wdrażania technologii z koniecznością zachowania poszanowanie praw pacjenta i bezpieczeństwa używania innowacyjnych wyrobów medycznych przez użytkowników, w tym pacjentów.

### 3.7.1 Regulacje krajowe – ustawa o jakości w opiece zdrowotnej i bezpieczeństwie pacjenta.

JakZdrU ma na celu promowanie jakości udzielanych świadczeń zdrowotnych, co zapewnić mają m.in. mechanizmy autoryzacji i akredytacji podmiotów leczniczych. Pojęcie „jakości” udzielanych świadczeń zdrowotnych jest bardzo szerokie – mieszczą się w nim potencjalnie również kwestie związane z systemami elektronicznej dokumentacji medycznej. Możliwa wysoka efektywność wspomnianych rozwiązań może przyczynić się do lepszego przepływu danych pomiędzy podmiotami leczniczymi, a w konsekwencji do bardziej kompleksowej obsługi pacjenta. Nowy model systemu jakości wprowadzony przez JakZdrU spotkał się jednak z szeroką krytyką. W szczególności w momencie przyjmowania przywołanej ustawy oraz powstawania niniejszego raportu nie były znane przepisy wykonawcze, od których w dużej mierze będzie zależał ostateczny kształt systemu jakości. Mając na uwadze jej kluczowe znaczenie dla całego systemu ochrony zdrowia, zasadne jest dokonanie oceny skutków regulacji ex post oraz na jej podstawie wprowadzenie ewentualnych zmian.

**Z perspektywy omawianego zagadnienia, najistotniejszą rolę będzie odgrywać kwestia rejestrów medycznych. Procedowana ustawa wprowadza:**

- Rozszerzenie katalogu podmiotów mogących prowadzić rejestry o towarzystwa naukowe;
- Wprowadzenie raportów generowanych przez rejestry

Brak jest jednak w omawianej ustawie systemowego podejścia do kwestii rejestrów medycznych. W poprzednich projektach aktu planowano m.in. powołanie rady ds. rejestrów medycznych, co jednak w finalnej wersji nie zostało wdrożone. Ponadto, wciąż brakuje odpowiednich narzędzi do tworzenia nowych rejestrów, co może spowodować, że dotychczas istniejące problemy nie zostaną rozwiązane.

JakZdrU wprowadza ponadto obowiązek obciążający dostawców usług informatycznych, aby ich systemy teleinformatyczne identyfikowały się wzajemnie oraz porozumiewały się między sobą w sposób bezpieczny, zgodnie z wymogami dotyczącymi wspólnych i bezpiecznych otwartych standardów komunikacji publikowanymi w Biuletynie Informacji Publicznej.



#### Rekomendacje:

Potrzebne jest poszerzenie regulacji związanych z systemem rejestrów medycznych oraz interoperacyjnością – por. punkty 5.3.4.2 i 5.3.4.3 raportu. Należy stworzyć dedykowane temu obszarowi eksperckie ciało, np. proponowaną w pierwszej wersji projektu JakZdrU Radę ds. Rejestrów lub centrum kompetencyjne ds. rejestrów jakości w jednostce dedykowanej monitorowaniu jakości w ochronie zdrowia. Proponujemy doprecyzowanie regulacji dotyczącej obowiązku sporządzania i publikowania raportów, tak by przedstawiały one informacje obejmujące: kompletność rekordów pacjentów i kompletność danych; produktywność poszczególnych podmiotów (rodzaj i zakres wykonywanych świadczeń); parametry skuteczności (outcomes) i bezpieczeństwa (powikłania, przeżycie, jakość życia), które mogą być przedstawiane bez publicznej identyfikacji konkretnych podmiotów. Alternatywnie, możliwe jest rozważenie budowy systemu opartego o łatwy dostęp do uporządkowanych danych z systemów podmiotów wykonujących działalność leczniczą (por. punkt 5.3.4.2).



## 4. Dane medyczne w pracy lekarza – jak być powinno?



Zbieranie i analizowanie danych medycznych jest nieodzownym elementem codziennej pracy lekarza. Chcąc lepiej poznać historię i sytuację zdrowotną pacjenta, jeszcze kilka lat temu lekarz – oprócz badania przedmiotowego – mógł polegać głównie na papierowej dokumentacji medycznej oraz pamięci pacjenta. Wraz z rozwojem e-zdrowia zmienia się forma gromadzenia i przetwarzania danych o stanie zdrowia. Lekarz może dużo łatwiej niż kiedyś uzyskać wiedzę na temat tego, co działo się z pacjentem. Co więcej, dzięki transmisji danych z wyrobów medycznych może monitorować wybrane parametry zdrowotne pacjenta w czasie rzeczywistym. Powstające przy tej okazji duże zbiory danych medycznych mogą być wykorzystywane przez lekarzy w celach naukowych i badawczo-rozwojowych.

Pod kątem odpowiedniego do rzeczywistych potrzeb lekarzy zaprojektowania przyszłych regulacji prawnych i innych interwencji strony publicznej należy spróbować przedstawić **kluczowe wartości oraz postulaty związane w tym, na jakich zasadach powinno odbywać się korzystanie przez lekarzy z danych medycznych.**

### 4.1 Świadomość

System e-zdrowia zapewnia różne możliwości – które dynamicznie się rozwijają wymagając stałej uwagi i zainteresowania – z których lekarz powinien mieć możliwość korzystania, jeżeli uzna to za przydatne. Jednocześnie też dostępne badania wskazują, że w realiach polskiego sektora ochrony zdrowia brakuje świadomości na temat potencjału wykorzystywania danych – wykorzystywanie zbiorów danych do wsparcia procesów leczniczych i zarządczych jest jeszcze bardzo rzadkim zjawiskiem<sup>47</sup>, co znajduje uzasadnienie w związku z faktem, że większość dostępnych danych jest obecnie bardzo mało wiarygodna, a zatem wykorzystywanie tych zbiorów mogłoby prowadzić do mylnych wniosków. Uzasadnia to promowanie wiedzy na temat możliwości wykorzystywania danych wśród kadry medycznej. Lekarz, który rozumie związane z tym korzyści, nie tylko będzie chciał je wykorzystywać, ale będzie też w stanie przekazać i wytłumaczyć to pacjentowi<sup>48</sup>.

Należy też podkreślić rolę państwa w podnoszeniu świadomości społeczeństwa. Możliwe jest prowadzenie kampanii informacyjnych i działań edukacyjnych w tym obszarze. Podnoszenie świadomości w temacie danych nie może bazować wyłącznie na zaufaniu pacjenta do lekarza.

47. I. Grabowska, K. Kuźma, Z. Polańska, J. Abramowicz, J. Kozera, Branża opieka zdrowotna i pomoc społeczna. Branżowy Bilans Kapitału Ludzkiego, Warszawa 2022, s. 31.

48. M. Libura, T. Imiela, D. Głód-Śliwińska (red.), Cyfryzacja zdrowia w interesie społecznym, Warszawa 2023, s. 104.

## 4.2 Dostępność

**Lekarz powinien mieć łatwy i szybki dostęp do danych pacjentów pochodzących z różnych źródeł.**

Jednym z podstawowych celów systemu e-zdrowia powinno być zapewnienie stanu rzeczy, w którym lekarz ma zagwarantowany jak najłatwiejszy i najszybszy dostęp do danych medycznych, które są mu niezbędne do zapewnienia opieki pacjentowi. Dane te mogą pochodzić potencjalnie z różnych źródeł, a kwestie techniczne lub uwarunkowania prawne nie powinny stanowić niepotrzebnych barier w dostępie do nich w uzasadnionych sytuacjach, w zależności od przyjętych rozwiązań – w szczególności w ramach ustawowego uprawnienia do określonych kategorii danych, pod warunkiem uzyskania zgody pacjenta lub przy braku jego sprzeciwu.

Lekarz jest już obecnie ustawowo umocowany do przetwarzania danych zawartych w dokumentacji medycznej (art. 24 ust. 2 PrPacjU). Wraz z szybkim rozwojem e-zdrowia, w ostatnich latach coraz większa część dokumentacji medycznej prowadzona jest w postaci elektronicznej. Dostęp do zawartych w niej jednostkowych danych medycznych dla lekarza jest zaś możliwy – z zastrzeżeniem wyjątków, np. lekarzy POZ – tylko na podstawie zgody pacjenta (art. 35 SystInfOchrZdrU, w zakresie dokumentacji prowadzonej w innych podmiotach wykonujących działalność leczniczą). Nawet jeżeli pacjent zgodę taką wyrazi, lekarz wciąż nie ma gwarancji dostępu do danych – część podmiotów wykonujących działalność leczniczą pomimo obowiązków nie prowadzi bowiem dokumentacji medycznej w postaci elektronicznej albo nie raportuje do systemu centralnego wymaganych danych, przez co zwyczajnie nie ma ich w systemie<sup>49</sup>. Dodatkowym problemem pozostaje interoperacyjność<sup>50</sup>, która warunkuje możliwość praktycznego wykorzystania danych.

## 4.3 Funkcjonalność

**Lekarz powinien móc sprawnie korzystać z różnych danych, a także aplikacji i programów, które pomogą mu zebrać, przeanalizować oraz wykorzystać dane w procesie opieki nad pacjentem.**

Dzięki dostępowi do danych możliwe jest tworzenie rozwiązań, które usprawniają codzienną pracę lekarza, np. automatycznie wypełniając za niego część dokumentacji medycznej lub podpowiadając możliwą diagnozę. Zapewniając dostęp do danych dla firm rozwijających podobne produkty i usługi wspieramy rozwój tego rodzaju technologii. Pod tym kątem ważne jest także odróżnianie różnych kategorii danych – np. autoryzowanych przez personel medyczny w formie dokumentacji medycznej, danych z wyrobów medycznych lub innych źródeł. Dane te mogą cechować się inną jakością i wiarygodnością, co ma kluczowe znaczenie dla lekarza, ale także dla podmiotów, które wykorzystują te dane w innych celach.

49. Por. media branżowe: <https://www.rynekzdrowia.pl/E-zdrowie/Obowiazkowa-EDM-to-fikcja-Tylko-15-proc-podmiotow-zaraportowalo-dane.232153.7.html>, <https://praca.gazetaprawna.pl/artykuly/8520027,ochrona-zdrowia-nfz-elektroniczna-dokumentacja-medyczna-rozliczenie.html> (dostęp: 19 lipca 2023).

50. Pojęcie interoperacyjności w systemach IT na gruncie prawnym rozumiane może być jako szereg wymogów na poziomie organizacyjnym, semantycznym i technologicznym. Dokładniejsze wymogi dla każdego z tych poziomów określa § 5 rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

Na polskim rynku dostępne są różnego rodzaju produkty i usługi, których zadaniem jest ułatwienie i usprawnienie pracy lekarza. Tworzone są i doskonalone właśnie dzięki dostępowi do danych medycznych. Pozwalają m.in. oszczędzić czas pracy lekarza automatycznie uzupełniając za niego część dokumentacji, szybciej zestawiać ze sobą pewne informacje np. dotyczące interakcji pomiędzy lekami, czy też wreszcie zapewniać merytoryczne wsparcie dzięki analizie danych. Rozwiązania oparte o sztuczną inteligencję – odpowiedzialnie wykorzystywane – mogą znacząco podnieść jakość opieki, dając lekarzowi więcej czasu na badanie i rozmowę z pacjentem. Tworzenie i udostępnienie narzędzi predykcji stanu zdrowia pacjenta zostało już przewidziane w strategicznych planach dalszego rozwoju e-zdrowia w Polsce. Jak wynika z raportu Future Health Index Polska 2022 – przemodelowanie opieki zdrowotnej; 2022 r., „Polscy liderzy ochrony zdrowia dostrzegają potencjał analityki predykcyjnej, która może pomóc im w realizacji kluczowych priorytetów. Na poziomie klinicznym, analityka predykcyjna może ułatwić świadczeniodawcom zapewnianie właściwej opieki właściwym pacjentom we właściwym czasie. Na poziomie operacyjnym, daje systemom opieki zdrowotnej możliwość identyfikowania trendów, poprawiając jakość opieki i redukując koszty. Jednak polscy liderzy ochrony zdrowia wdrażają technologie analityczne wolniej, niż ma to miejsce w innych krajach”<sup>51</sup>. Lekarze powinni mieć zapewniony łatwy dostęp do różnego rodzaju tego typu narzędzi, których jakość i bezpieczeństwo stosowania nie mogą budzić wątpliwości.

## 4.4 Bezpieczeństwo

**Lekarz powinien mieć dostęp do narzędzi, które zapewniają bezpieczeństwo korzystania z danych.**

Praca na danych o stanie zdrowia wymaga korzystania z narzędzi i rozwiązań umożliwiających bezpieczne zbieranie danych oraz zapisywanie ich w chronionej przestrzeni cyfrowej. Dostęp do nich oraz ich wykorzystanie powinno zawsze następować z poszanowaniem zasad cyberbezpieczeństwa.

Dane o stanie zdrowia pacjenta stanowią dane niezwykle wrażliwe, tzw. dane sensytywne (por. art. 9 RODO)<sup>52</sup>. Dlatego też regulacje prawne, w tym m.in. przepisy PrPacjU oraz RODO, przewidują szereg wymogów związanych z ich zabezpieczeniem. Systemy do prowadzenia dokumentacji medycznej w postaci elektronicznej oraz narzędzia stosowane do gromadzenia i wykorzystywania cyfrowych danych medycznych muszą gwarantować wysoki poziom ochrony danych, w tym w szczególności w przypadku przetwarzania danych w ramach technologii tzw. chmury obliczeniowej, a lekarz powinien móc w łatwy sposób zweryfikować, czy warunki z tym związane są spełniane przez narzędzia, które wykorzystuje. Wykorzystywanie danych medycznych zawsze musi następować odpowiedzialnie, w sposób zapewniający ich należyłą ochronę, co w świetle dostępnych badań z różnych przyczyn wciąż jest dużym wyzwaniem w wielu placówkach ochrony zdrowia<sup>53</sup>.

51. Future Health Index Polska 2022 – przemodelowanie opieki zdrowotnej; 2022 r.

52. „W ramach tego założenia dane medyczne jednostki zyskują dodatkowo na znaczeniu, gdyż są zbiorem najwrażliwszych i najbardziej personalnych danych. Zgodnie z podejściem Floridiego informacje określają nas jako ludzi, a informacje medyczne stają się w takim wypadku pewnego rodzaju metainformacjami. Umożliwiają one jeszcze dokładniejsze poznanie graniczące z naruszeniem wartości jednostki (intymności, godności). Takie podejście pozwala na sprecyzowanie wolności człowieka i jej granicy”. – K. Ruciński; P. Lewandowski – Etyczne uzasadnienie zarządzania danymi medycznymi w perspektywie działań rozwojowych Unii Europejskiej; Studia Humanistyczne AGH 2022;21(4): s. 79–90.

53. Por. raport NIK o ochronie danych osobowych w szpitalach: <https://www.nik.gov.pl/aktualnosci/rodo-w-szpitalu.html> (dostęp: 20 lipca 2023)

Zasadniczy ciężar związany z zapewnieniem wysokiego poziomu ochrony danych powinien spoczywać na dostawcach sprzętu i oprogramowania, którzy są podmiotami wyspecjalizowanymi, znającymi bieżący stan wiedzy technicznej. Odpowiedzialność lekarza powinna ograniczać się do wyboru sprzętu i oprogramowania, którego dostawca zapewnia spełnianie takiego standardu. Lekarz powinien mieć w związku z tym dostęp do dokumentów, które pozwolą mu zweryfikować i łatwo ocenić dostawców oraz zakres ich odpowiedzialności.

## 4.5 Rozwój

### **Lekarz powinien móc wykorzystać dane medyczne w celach naukowych i badawczych.**

Wykorzystanie dużych zbiorów danych medycznych jest niezbędne dla rozwoju innowacji w różnych jej wymiarach, obecnie jest to szczególnie istotne zagadnienie pod kątem zwiększania jakości systemów sztucznej inteligencji. Zbiory danych medycznych powinny być w związku z tym w interesie publicznym możliwie szeroko dostępne dla innowatorów, w szczególności dla wszystkich podmiotów wchodzących w skład systemu szkolnictwa wyższego i nauki, oczywiście przy zachowaniu ich poufnego charakteru.

Lekarz może przetwarzać dane medyczne nie tylko w celu zapewnienia opieki zdrowotnej. Występuje też m.in. w roli naukowca, który analizując duże zbiory danych może poszerzać wiedzę medyczną, badacza, który podczas badań klinicznych weryfikuje skuteczność i bezpieczeństwo produktów leczniczych i wyrobów medycznych, a także startupowca, który rozwija własne produkty i usługi mające na celu usprawnienie opieki medycznej. Jak wskazano w motywie 41. preambuły do EHDS, za sprawą wtórnego wykorzystywania danych dotyczących zdrowia w ramach europejskiej przestrzeni danych dotyczących zdrowia podmioty publiczne, prywatne, niedochodowe, a także poszczególni badacze powinni zyskać dostęp do danych dotyczących zdrowia na potrzeby badań naukowych, innowacji, kształtowania polityki, działań edukacyjnych, bezpieczeństwa pacjenta, działań regulacyjnych lub medycyny personalizowanej. Dostęp ten powinni mieć także lekarze, którzy mogą wykorzystywać je we wszystkich przywołanych celach.

## 5. Kluczowe wyzwania i kierunki potencjalnych zmian

### 5.1 Wprowadzenie

Dotychczasowa część raportu prezentowała obecne uwarunkowania prawne i pozaprawne związane z obszarem przetwarzania danych medycznych, przyszłe lub dopiero projektowane zmiany, zarówno na poziomie krajowym, jak i unijnym, jak również rekomendacje co do tworzonych w przyszłości przepisów prawa. W następnych punktach raportu zaprezentowano konkretne problemy i wyzwania występujące w tym obszarze, możliwy wpływ reform na ich rozwiązanie, a także rekomendowane zmiany, które służą pełniejszej realizacji postulatów dotyczących zasad korzystania przez lekarzy z danych przedstawionych w poprzednim punkcie raportu.

Analiza w tym obszarze została podzielona na cztery części dotyczące:

1. **dostępu do danych**, od którego na poziomie systemu e-zdrowia zależy to, czy dane w ogóle będą gromadzone i czy będą mogły zostać wykorzystane przez lekarza w jakikolwiek sposób,
2. **postępowania z danymi**, czyli zasad zgodnego z prawem, w tym m.in. obowiązkami wynikającymi z regulacji wykonywania zawodu lekarza, wykorzystywania danych w ramach różnych narzędzi i w różnych celach,
3. **udostępniania danych**, a więc warunków, które muszą być spełnione, by lekarz mógł zgodnie z prawem podzielić się z innymi osobami, firmami i instytucjami danymi, które posiada, lub uzyskać takie dane od innego podmiotu,
4. **wykorzystywania danych w celach naukowych**, a więc możliwości przetwarzania danych o stanie zdrowia w celach niezwiązanych bezpośrednio z udzielaniem świadczeń zdrowotnych, np. w ramach prowadzonych przez lekarza badań nieinterwencyjnych.

W ramach każdej z wyżej wymienionych części wyodrębniono jeszcze bardziej szczegółowe obszary, pod kątem których zidentyfikowano i przedstawiono konkretne zagadnienia.

### 5.2 Dostęp do danych

Pierwsza część dotyczy najszerzej rozumianego dostępu do danych. Dane o stanie zdrowia gromadzone są przez bardzo różne podmioty, które mają odmienne obowiązki związane z ich udostępnianiem. Brak danych lub niemożność ich wykorzystania stanowi pierwszą i zarazem podstawową barierę dla realizacji wskazanych w punkcie 4. raportu postulatów.

#### 5.2.1 Zakres danych medycznych dostępnych dla lekarza

Pierwszy obszar związany z dostępem do danych dotyczy zakresu danych, które może uzyskać lekarz. W świetle obecnych uwarunkowań prawnych i pozaprawnych występują bowiem sytuacje, w których lekarz może być np. pozbawiony dostępu do potrzebnych mu danych, podczas gdy są one gromadzone w systemie centralnym lub na poziomie podmiotów wykonujących działalność leczniczą.

### 5.2.1.1 Ograniczenia związane z zasadami dostępu do danych

**Stan obecny.** W pierwszej kolejności należy zauważyć, że przepisy prawa wyraźnie odróżniają zasady dostępu lekarza do dokumentacji medycznej od dostępu do jednostkowych danych medycznych.

W pierwszym przypadku dostęp lekarza do dokumentacji medycznej określonego pacjenta nie jest wcale bliżej regulowany. Zgodnie bowiem z art. 24 ust. 2 PrPacjU lekarz, jako osoba wykonująca zawód medyczny, jest uprawniony w sposób ogólny do przetwarzania danych zawartych w dokumentacji medycznej. Przywołana regulacja nie zawiera dodatkowych ograniczeń takiego dostępu. W zakresie wglądu do już wcześniej wytworzonej dokumentacji medycznej, przepisy prawa określają warunki jej przekazywania na poziomie podmiotów wykonujących działalność leczniczą – bez upoważnienia pacjenta dokumentację medyczną udostępnia się podmiotom udzielającym świadczeń zdrowotnych, jeżeli dokumentacja ta jest niezbędna do zapewnienia ciągłości świadczeń zdrowotnych (art. 26 ust. 3 pkt 1 PrPacjU). Tym samym, jeżeli podmiot wykonujący działalność leczniczą uzyska dokumentację (niezależnie od formy dokumentacji), może skorzystać z niej lekarz. Drugi ze wskazanych przypadków odnosi się do pojęcia jednostkowych danych medycznych, a nie dokumentacji medycznej. Zgodnie z art. 35 SystInfOchrZdrU dostęp „do danych osobowych lub jednostkowych danych medycznych”<sup>54</sup>, które są przetwarzane w systemie teleinformatycznym usługodawcy (czyli m.in. podmiotu leczniczego) lub w Systemie Informacji Medycznej, mają:

1. pracownik medyczny, który wytworzył elektroniczną dokumentację medyczną zawierającą dane osobowe lub jednostkowe dane medyczne usługobiorcy;
2. pracownik medyczny wykonujący zawód u usługodawcy, u którego została wytworzona elektroniczna dokumentacja medyczna zawierająca dane osobowe lub jednostkowe dane medyczne usługobiorcy, w związku z wykonywaniem przez niego zawodu u tego usługodawcy, jeżeli jest to niezbędne do prowadzenia diagnostyki lub zapewnienia ciągłości leczenia;
3. lekarz, pielęgniarka lub położna udzielający usługobiorcy świadczeń opieki zdrowotnej w ramach umowy o udzielanie świadczeń opieki zdrowotnej z zakresu podstawowej opieki zdrowotnej;
4. każdy pracownik medyczny w sytuacji zagrożenia życia usługobiorcy.

W przypadkach innych niż określone powyżej udostępnienie danych osobowych lub jednostkowych danych medycznych z systemu teleinformatycznego usługodawcy lub z Systemu Informacji Medycznej następuje za zgodą usługobiorcy lub jego przedstawiciela ustawowego. Wyrażając zgodę, wskazuje się zakres czasowy i przedmiotowy dostępu do tych danych.

Zgodnie z art. 35 ust. 5 SystInfOchrZdrU przepisy ustanawiające powyższe zasady dostępu do jednostkowych danych medycznych nie naruszają przy tym przepisów o dostępie do danych zawartych w dokumentacji medycznej w sposób określony w przepisach PrPacjU, a więc m.in. dostępu na podstawie art. 26 ust. 3 pkt 1 PrPacjU, czyli przestanki kontynuacji leczenia.

54. Różnice pomiędzy tymi pojęciami zostały scharakteryzowane w punkcie 3.2.2 raportu.

Powyższe regulacje prowadzą do sytuacji, w której nie jest jasne i czytelne, na jakich dokładnie zasadach następuje dostęp do danych medycznych pacjenta np. lekarza specjalisty przyjmującego pacjenta w ramach ambulatoryjnej opieki zdrowotnej. Choć przepisy SystInfOchrZdrU nie naruszają przepisów PrPacjU, uznanie, że każdy lekarz ma dostęp do jednostkowych danych medycznych w ramach ich niezbędności do zapewnienia ciągłości świadczeń zdrowotnych prowadzi do sytuacji, w której art. 35 ust. 1 SystInfOchrZdrU traciłby sens, bowiem w zasadzie każdy lekarz miałby dostęp do danych. Treść przywołanego przepisu literalnie nie zawęża jego zastosowania jedynie do EDM, lecz odnosi się do wszelkich danych osobowych lub jednostkowych danych medycznych pacjenta dostępnych w systemie teleinformatycznym placówki medycznej.

Tym samym należy uznać, że dostęp do danych medycznych dla przywołanego lekarza specjalisty pod kątem systemowym uzależniony został co do zasady od uzyskania zgody pacjenta (lub przedstawiciela ustawowego) – jest to tzw. model opt-in<sup>55</sup>. Brak aktywności pacjenta – wyrażenia zgody – pozbawia więc lekarza możliwości poznania historii choroby pacjenta (z zastrzeżeniem wcześniejszych uwag co do innych przestąnek i stanów nagłych). W sytuacji, w której część przepisów odnosi się do możliwości wykorzystania jednostkowych danych medycznych pacjenta dostępnych za pośrednictwem systemu P1 (np. recepta na preparat zawierający środek odurzający grupy I-N lub II-N, substancję psychotropową grupy II-P, III-P lub IV-P lub prekursor kategorii 1 może być wystawiana po uprzednim dokonaniu przez osobę wystawiającą receptę weryfikacji za pośrednictwem systemu centralnego, że ilość i rodzaj produktów leczniczych przepisanych pacjentowi na receptach wystawionych i zrealizowanych nie jest wystarczająca dla prawidłowego prowadzenia farmakoterapii<sup>56</sup>), może dochodzić do problematycznych sytuacji, w których lekarz nie uzyska dostępu do tych danych z powodu braku zgody pacjenta, a jednocześnie dane te będą mu potrzebne do udzielenia świadczenia zdrowotnego.

Obecnie przyjęte rozwiązania prawne prowadzą do sytuacji, w której część lekarzy (np. lekarze specjaliści) na podstawie art. 35 SystInfOchrZdrU może uzyskać dostęp do jednostkowych danych medycznych w tzw. modelu opt-in, tj. za uprzednią zgodą pacjenta. Lekarze POZ mają zapewniony pełny dostęp do danych pacjenta, który nie ma możliwości wyrażenia względem tego sprzeciwu. Jest to więc rozwiązanie bardziej restrykcyjne niż tzw. model opt-out, który przewiduje możliwość wyrażenia sprzeciwu w stosunku do dostępu do danych.

55. Przy zastrzeżeniu możliwości dostępu do dokumentacji w trybie wynikającym z PrPacjU.

56. § 7 ust. 2a rozporządzenia Ministra Zdrowia w sprawie środków odurzających, substancji psychotropowych, prekursorów kategorii 1 i preparatów zawierających te środki lub substancje.



## Perspektywa zmian

Program rozwoju e-zdrowia w Polsce do 2027 r. zakłada powstanie spójnej polityki prywatności danych pacjenta stosowanej na wszystkich poziomach systemu ochrony zdrowia. Polityka ma zostać umocowana w ustawie o danych medycznych. Bliższe założenia i szczegóły tych zmian nie zostały jednak przedstawione.

EHDS opiera się na zasadzie, że w przypadku przetwarzania danych w formacie elektronicznym pracownicy ochrony zdrowia mają dostęp do elektronicznych danych dotyczących zdrowia osób, które leczą, niezależnie od państwa członkowskiego ubezpieczenia i państwa członkowskiego leczenia (por. art. 4 ust. 1 EHDS). Co więcej, państwa członkowskie mają zapewnić pracownikom ochrony zdrowia dostęp co najmniej do priorytetowych kategorii elektronicznych danych dotyczących zdrowia, za pośrednictwem usług dostępu dla pracowników ochrony zdrowia (por. art. 4 ust. 3 EHDS).

Zgodnie z 3 ust. 9 EHDS, niezależnie od art. 6 ust. 1 lit. d RODO<sup>57</sup> osoby fizyczne mają prawo ograniczyć dostęp pracowników ochrony zdrowia do całości lub części ich elektronicznych danych dotyczących zdrowia. W tym celu państwa członkowskie mogą ustanawiać przepisy i określone zabezpieczenia dotyczące takich mechanizmów ograniczania. Tym samym możliwe jest przyjęcie tzw. modelu opt-out, w którym zasadą jest dostęp lekarza do potrzebnych mu danych pacjenta. Pacjent może przy tym wyrazić sprzeciw względem takiego dostępu – sprzeciw taki równoznaczny jest z niedopuszczalnością uzyskania danych przez lekarza (z wyjątkiem sytuacji wyjątkowych, np. stanów nagłych, lub dostępu w wybranym zakresie wynikającego wprost z przepisów prawa).



## Możliwe działania

Polityki prywatności danych pacjenta umocowane w przepisach prawa powinny po pierwsze ustanawiać jasne i czytelne zasady dostępu do danych medycznych, w tym danych zawartych w dokumentacji medycznej, jak i samej dokumentacji, z uwzględnieniem obecnych uwarunkowań i możliwości systemu e-zdrowia. Zagadnienie to zostało szerzej opisane w punkcie 5.3.5.1 raportu.

Po drugie, konieczne jest rozpoczęcie dyskusji publicznej na temat docelowego modelu dostępu lekarzy do danych medycznych pacjentów, tak by znaleźć optymalne rozwiązanie zapewniające z jednej strony łatwy dostęp lekarza do kompletu informacji potrzebnych mu do opieki nad pacjentem, z drugiej zaś poszanowanie autonomii informacyjnej pacjenta. W tym zakresie możliwe jest przyjęcie w różnych zakresach różnych rozwiązań, w szczególności jednego z podstawowych modeli<sup>58</sup>:

57. Podstawa prawna przetwarzania danych osobowych niezbędnych do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej.

58. Niezależnie bezwzględny dostęp do danych na zasadzie wyjątku może obejmować stany nagłe. W takim przypadku ważny jest jednak mechanizm przejrzystości, który umożliwić będzie weryfikacją, czy dostęp rzeczywiście był uzasadniony. Dalszy opis odnosić się będzie do standardowych zasad dostępu.



- 1. model regulowany**, w którym dostęp określonych kategorii lekarzy do danych pacjenta wynika wprost z przepisów prawa i nie wymaga uzyskania jego zgody, pacjent nie ma też możliwości wniesienia sprzeciwu. Obecnie taki dostęp do danych przysługuje na mocy art. 35 SystInfOchrZdrU lekarzom POZ. Podstawowym plusem tego rozwiązania jest zapewnienie dostępu do pełnych danych pacjenta lekarzom odpowiedzialnym systemowo za koordynację opieki medycznej nad nim. Zapobiega to sytuacji, w której lekarz nie mógłby uzyskać dostępu do potrzebnych mu informacji. Z drugiej strony ograniczona zostaje autonomia informacyjna pacjenta.
- 2. model opt-in**, który zakłada dostęp lekarza do danych na podstawie uprzedniej zgody pacjenta. W modelu tym pacjent zachowuje pełną kontrolę nad dotyczącymi go danymi medycznymi, od jego aktywnego działania (wyrażenia zgody) uzależniony jest dostęp lekarza. Podstawową zaletą tego modelu jest pełna kontrola dostępu do danych medycznych przez pacjenta. Zaleta ta pod kątem systemowym rodzi jednak szereg wyzwań. Po pierwsze, mniej świadomi pacjenci mogą nie wiedzieć o konieczności wyrażania zgody lub nie potrafić jej wyrazić (np. za pośrednictwem IKP), co dodatkowo wydłuża proces obsługi pacjenta. Brak wyrażenia zgody oznacza też mniej danych dostępnych dla lekarza, co utrudnia rozeznanie się w sytuacji zdrowotnej pacjenta i może prowadzić np. do powtarzania części badań diagnostycznych, wydłużać proces diagnostyki i leczenia i generować dodatkowe koszty.
- 3. model opt-out**, który z góry zakłada dostęp lekarza i personelu zaangażowanego w udzielanie świadczeń zdrowotnych do danych medycznych pacjenta. Tym samym nie występują dodatkowe organizacyjne ograniczenie związane z koniecznością uzyskania uprzedniej zgody pacjenta. Jednocześnie, aby zapewnić pacjentowi możliwość decydowania o dostępie do danych, może on wyrazić sprzeciw względem takiego dostępu. Podstawowym plusem tego modelu jest domyślny dostęp do danych, co pod kątem organizacyjnym stanowi znaczące usprawnienie procesu opieki. Model ten zapewnia jednocześnie poszanowanie autonomii informacyjnej pacjenta przez prawo do wyrażenia sprzeciwu. Dodatkowo, sam dostęp do danych może podlegać mechanizmom kontrolnym, np. być rejestrowany, co umożliwi zapobieganie i wychwytywanie ewentualnych nadużyć. Minusem tego rozwiązania jest to, że wspomnianych nadużyć może jednak dochodzić. Dodatkowo mniej świadomi pacjenci mogą nie wiedzieć o przysługującym im prawie sprzeciwu. Dodatkowo, w przypadku zgłaszania sprzeciwów zachodzi ryzyko komplikacji analogicznych jak przy braku wyrażonej zgody na dostęp.
- 4. model mieszany**, który zakłada wykorzystanie powyższych rozwiązań w różnych zakresach w celu wykorzystania ich podstawowych zalet. Przykładowo, lekarz POZ, który potrzebuje możliwie wszechstronnej i aktualnej wiedzy o pacjencie, mógłby mieć dostęp do danych w modelu opt-out, podczas gdy lekarz specjalista, który potrzebuje zazwyczaj tylko określonego zakresu danych, w modelu opt-in. Modele te mogą nie znaleźć w ogóle zastosowania w przypadkach uregulowanych przez prawo, np. dostęp wszystkich lekarzy opierać się będzie o model opt-out, ale możliwość wniesienia sprzeciwu nie obejmować będzie lekarzy POZ.

Dodatkowym zagadnieniem pozostaje przy tym zakres zastosowania potencjalnej zgody lub sprzeciwu, tj. oświadczenie pacjenta o zgodzie lub sprzeciwie może mieć charakter generalny i dotyczyć wszystkich kontaktów z systemem ochrony zdrowia, znajdować zastosowanie tylko względem określonych podmiotów leczniczych lub tylko względem konkretnych lekarzy.

Pod kątem jakości opieki zdrowotnej oraz ergonomii pracy lekarza należy rozważyć oparcie nowego systemu w jak największym zakresie na modelu opt-out, który stwarza szansę na pełne wykorzystanie potencjału stwarzanego przez cyfryzację ochrony zdrowia oraz obieg elektronicznych danych medycznych. W związku z potrzebą koordynacji opieki nad pacjentem model opt-out może być ograniczony, tj. gwarantować części lekarzy bezwzględny dostęp do danych. Jednocześnie jest to zagadnienie wymagające dalszej dyskusji i konsensusu, w tym w szczególności ze środowiskiem pacjenckim. Należy przedyskutować możliwe korzyści i ryzyka poszczególnych rozwiązań dla systemu ochrony zdrowia, praktyki wykonywania zawodu lekarza oraz praw pacjenta.

W celu zapobieżenia możliwym nadużyciom, niezależnie do przyjętego modelu, każdy dostęp do danych medycznych powinien być rejestrowany w systemie i widoczny dla pacjenta. Zapewni to możliwość kontrolowania tego, kto faktycznie sięgał do danych oraz czy były to działania uprawnione, tj. uzasadnione opieką nad pacjentem lub innym dopuszczalnym celem dostępu. Ponadto, potrzebny jest mechanizm kontroli takiego dostępu. Należy rozważyć np. powołanie funkcji niezależnego pełnomocnika do spraw kontroli przetwarzania danych, który otrzymałaby uprawnienia kontrolne w tym zakresie.



### Uzasadnienie

Proponowana zmiana na poziomie systemowym powinna zmierzać do zwiększenia możliwości dostępu do danych medycznych dla lekarzy. Obecnie obowiązujące rozwiązania z jednej strony i tak ograniczają autonomię informacyjną pacjenta (pełen dostęp do danych lekarza POZ), z drugiej strony mogą okazać się nieefektywne przy dalszym wprowadzaniu opieki koordynowanej, w której dostęp specjalistów uzależniony byłby od zgody pacjenta. Mając na uwadze rosnącą skalę danych gromadzonych w postaci cyfrowej konieczne jest rozpoczęcie szerokiej dyskusji na temat zasad dostępu do danych medycznych dla lekarzy i personelu medycznego.

Warto przy tym zwracać uwagę na przykłady z innych państw Unii Europejskiej. Model opt-out stosowany jest z powodzeniem m.in. w Danii oraz w Estonii<sup>59</sup>, a więc w krajach, które wskazywane są często jako dobre przykłady pod kątem budowania systemów e-zdrowia. Dla równowagi warto wspomnieć, iż model opt-in znajduje zastosowanie m.in. w Republice Federalnej Niemiec, która – podobnie jak Polska – przechodzi intensywną transformację cyfrową w sektorze ochrony zdrowia<sup>60</sup>.

Propozycja wpisuje się w postulat dotyczący dostępności danych – lekarz powinien mieć łatwy i szybki dostęp do danych pacjentów z różnych źródeł. W największym stopniu może to zapewnić system dostępu do danych oparty o model opt-out, ale z uwagi na wrażliwy charakter danych konieczne jest wypracowanie w tym zakresie szerszego konsensusu społecznego.

59. [https://health.ec.europa.eu/system/files/2016-11/laws\\_estonia\\_en\\_o.pdf](https://health.ec.europa.eu/system/files/2016-11/laws_estonia_en_o.pdf), <https://d-nb.info/1138409464/34>

60. <https://www.netdokter.de/diagnostik/elektronische-patientenakte/>

### 5.2.1.2 Niekompletność danych gromadzonych w tzw. systemie P1

**Stan obecny.** Jedną z podstaw dalszego rozwoju i funkcjonowania systemu informacji w ochronie zdrowia mają być dane medyczne przesyłane obowiązkowo przez podmioty wykonujące działalność leczniczą w ramach raportowania zdarzeń medycznych i przetwarzane dalej w ramach centralnej Elektronicznej Platformy Gromadzenia, Analizy i Udostępnienia Zasobów Cyfrowych o Zdarzeniach Medycznych (czyli tzw. systemu P1).

Zgodnie z art. 11 ust. 3 SystInfOchrZdrU, każdy usługodawca, czy m.in. podmiot wykonujący działalność leczniczą oraz apteka, ma obowiązek przekazywać do SIM dane zdarzenia medycznego w celu umożliwienia innemu podmiotowi pobrania danych osobowych lub jednostkowych danych medycznych zawartych w elektronicznej dokumentacji medycznej lub dokumentacji medycznej, o której mowa w PrPacjU, niezbędnych do prowadzenia diagnostyki lub zapewnienia ciągłości leczenia. Zgodnie z przywołanym przepisem dane te są ponadto udostępniane Narodowemu Funduszowi Zdrowia w celu rozliczania świadczeń opieki zdrowotnej.

Szczegółowy zakres danych zdarzenia medycznego oraz sposób i terminy przekazywania tych danych do SIM określa rozporządzenie Ministra Zdrowia w sprawie szczegółowego zakresu danych zdarzenia medycznego przetwarzanego w systemie informacji oraz sposobu i terminów przekazywania tych danych do Systemu Informacji Medycznej. Zakres przekazywanych danych obejmuje m.in. dane kliniczne, w tym np. kod przyczyny głównej i kody przyczyn współistniejących według Międzynarodowej Statystycznej Klasyfikacji Chorób i Problemów Zdrowotnych Rewizja Dziesiąta, kody zrealizowanych istotnych procedur medycznych według polskiej wersji Międzynarodowej Klasyfikacji Procedur Medycznych Rewizja Dziewiąta CM, informacje o zaimplantowanych wyrobach medycznych, alergiach, ciąży, wyniku grupy krwi. Informacjom tym towarzyszą dane dotyczące dokumentacji medycznej prowadzonej w postaci elektronicznej, w tym adres repozytorium, w którym jest przechowywana dokumentacja medyczna, oraz tryb jej udostępniania.

Jak wynika z badania przeprowadzonego przez Centrum e-Zdrowia, przesyłanie danych – pomimo ustawowego obowiązku – nie jest jeszcze powszechną praktyką. W świetle dostępnych danych zaledwie 57,2% placówek wdrożyło raportowanie zdarzeń medycznych. Ponad 14% podmiotów nie stosuje tego rozwiązania ze względu na brak systemu gabinetowego lub szpitalnego posiadającego odpowiedni moduł raportowania zdarzeń medycznych, a kolejne ponad 10% borykało się z problemami organizacyjnymi<sup>61</sup>. Dodatkowo należy zauważyć, że do SIM nie trafiają dane związane z leczeniem poza granicami Polski. Tym samym zbiór danych dostępnych w systemie P1 nie daje gwarancji kompletności, tj. nie mamy np. pewności, czy dane dotyczące konkretnego pacjenta są rzeczywiście pełne.

61. VI Edycja „Badania stopnia informatyzacji podmiotów wykonujących działalność leczniczą”, Centrum e-Zdrowia, wrzesień 2022, s. 17. Dostęp: [https://cez.gov.pl/sites/default/files/2022-09/Raport%20CeZ\\_2022.pdf](https://cez.gov.pl/sites/default/files/2022-09/Raport%20CeZ_2022.pdf)



Program rozwoju e-zdrowia w Polsce do 2027 r. opiera się na założeniu, że dane medyczne gromadzone w ramach systemu raportowania zdarzeń medycznych będą podstawą dla nowych funkcjonalności systemu, np. system obsługujący opiekę koordynowaną ma definiować plany leczenia oraz monitorować jego realizację na podstawie m.in. zdarzeń medycznych<sup>62</sup>. Co więcej, dane pochodzące z raportowania zdarzeń medycznych – obok innych kategorii danych - mają być podstawą do analiz i mają być używane m.in. do predykcji stanu zdrowia pacjenta, w tym rozwoju rozwiązań opartych o sztuczną inteligencję.

Inne akty prawne wykorzystują dostęp do danych z systemu P1 jako narzędzie pracy lekarza. Przywołać należy np. wspomniane w poprzednim punkcie rozporządzenie w sprawie środków odurzających, substancji psychotropowych, prekursorów kategorii 1 i preparatów zawierających te środki lub substancje, które wskazuje, że część recept będzie mogła być wystawiana po uprzednim dokonaniu przez osobę wystawiającą receptę weryfikacji danych pacjenta za pośrednictwem systemu P1. Opiera się to na założeniu, że w systemie rzeczywiście znajdują się wszystkie wymagane dane, co w świetle obecnej praktyki nie jest wcale pewne.

W kontekście planowanych zmian należy też zaznaczyć, że program rozwoju e-zdrowia w Polsce do 2027 r. wskazuje na konieczność „poszerzenia zakresu danych medycznych dostępnych elektronicznie zarówno dla pacjenta, jak i pracowników medycznych, w sposób adekwatny do potrzeb”. Tym samym „zasoby ZM należy rozszerzać wraz z pojawianiem się kolejnych potrzeb”, tak by część danych była łatwo dostępna z poziomu „rozszerzonego zdarzenia medycznego”<sup>63</sup>. Tym samym należy się spodziewać, że zakres raportowanych danych zostanie poszerzony o dane o charakterze klinicznym, dostępne obecnie na poziomie dokumentacji medycznej.

Skuteczność już stosowanych rozwiązań oraz planowanych zmian może być ograniczona z uwagi na fakt, że w świetle dostępnych informacji system P1 nie daje jeszcze gwarancji kompletności danych. Tym samym wszelkie analizy i predykcje zagrożone są ryzykiem błędu związanego z nieuwzględnieniem części istotnych danych.

Kwestie dostępu do danych z innych krajów leczenia częściowo rozwiąże EHDS, który zakłada dostęp lekarza do danych medycznych pacjenta z jego leczenia w innych krajach Unii Europejskiej.

62. Por. Program rozwoju e-zdrowia w Polsce do 2027 r., s. 27.

63. Por. Program rozwoju e-zdrowia w Polsce do 2027 r., s. 30.



W pierwszej kolejności warto wskazać, że wprowadzenie obowiązku raportowania zdarzeń medycznych nie było poprzedzone szerszą dyskusją publiczną nad celem i zakresem tego rozwiązania. Jak się wydaje, nie wszyscy pacjenci mogą być świadomi faktu, że dane o ich stanie zdrowia są przesyłane z poziomu placówki medycznej do systemu centralnego. Podobnie w przypadku lekarzy oraz personelu medycznego – wielu profesjonalistów medycznych jest błędnie przekonanych, że obowiązek raportowania zdarzeń medycznych obejmuje tylko świadczenia zdrowotne finansowane przez NFZ. Szerszą dyskusję w tym zakresie wywołało dopiero wprowadzenie obowiązku raportowania danych obejmujących informacje o ciąży. Dlatego tak ważne jest, by wszelkie ewentualne zmiany związane z systemem raportowania zdarzeń medycznych były uprzednio odpowiednio komunikowane i dobrze uzasadniane, szerzej niż w przypadku standardowych konsultacji publicznych. Konieczne jest wypracowanie w tej materii szeroko akceptowanego konsensusu, który może potencjalnie obejmować np. możliwość sprzeciwu względem raportowania części danych.

Przed projektowaniem dalszych zmian rekomendujemy przeprowadzenie audytu systemu P1 w celu weryfikacji i walidacji jakości, spójności i kompletności danych przechowywanych w systemie. Wyniki audytu mogą przyczynić się do ulepszenia systemu, zwiększania waloru naukowego i klinicznego danych tam przechowywanych, a także wypracowania dalszych potrzebnych zmian i usprawnień.

Przyjmując jako punkt odniesienia obecne rozwiązania oraz przedstawione wcześniej plany rozwoju systemu e-zdrowia, na obecnym etapie kluczowe jest zapewnienie przestrzegania już obowiązujących wymogów w zakresie raportowania zdarzeń medycznych. Podstawowym warunkiem skuteczności większości rozwiązań opartych o system P1 jest kompletność zgromadzonych w nim danych. W związku z tym należy dążyć do egzekwowania obecnych regulacji prawnych.

Rozważyć można wprowadzenie mechanizmu promowania placówek, które rzetelnie wywiązują się z obowiązku raportowania. Tym samym poniesienie ciężaru związanego z raportowaniem danych będzie dodatkowo nagradzane w wymiarze finansowym. Okazją do zastosowania takiego mechanizmu jest JakZdrU, która wprowadza system akredytacji. Włączenie obszaru sprawozdawania wysokiej jakości danych do standardów akredytacyjnych spowoduje, że rzetelna sprawozdawczość służąca realizacji obowiązków w wyższym standardzie będzie „nagradzana” przez możliwość otrzymania większych środków od NFZ.

Cennym wsparciem w tym zakresie będzie też wyposażenie podmiotów wykonujących działalność leczniczą w dedykowane systemy, w tym oparte o chmurę obliczeniową oraz rozwiązania AI, które wspierać będą automatyzację procesu zbierania i przesyłania danych, bo możliwie odciążąc z realizacji tych czynności personel placówek ochrony zdrowia.

Mając na uwadze plany rozwoju systemu e-zdrowia, należy się spodziewać, że zakres raportowanych danych będzie ulegał poszerzeniu. Należy zawczasu przedstawić i skierować do konsultacji projekt przyszłych funkcji systemu i zakresu danych, które będą w związku z nimi potrzebne. Placówki medyczne (oraz dostawcy systemów IT) powinny mieć czas, by odpowiednio przygotować się do poszerzonego zakresu przesyłanych danych. Podobnie w przypadku dostępności danych medycznych z innych krajów Unii Europejskiej, którą przewiduje EHDS.

Projektując dalszą architekturę systemu e-zdrowia należy zwrócić szczególną uwagę na stale rosnącą liczbę danych zapisywanych w platformie P1, co wiąże się z koniecznością zapewnienia adekwatnej przestrzeni obliczeniowej dla poprawnego funkcjonowania całego systemu. Szczególnym wyzwaniem jest przy tym zapewnienie możliwości zapisywania i transferu dokumentów obrazowych, które są zazwyczaj plikami o stosunkowo dużych rozmiarach. Uzasadnione jest priorytetowe podejście do tworzenia repozytoriów tej kategorii dokumentów oraz zapewnienie narzędzi umożliwiających ich sprawny i niezakłócony transfer.



### Uzasadnienie

Przedstawione wyzwanie jest charakterystyczne dla wszystkich prowadzonych na dużą skalę projektów z zakresu informatyzacji w ochronie zdrowia. W tym przypadku, warunkiem koniecznym nie tylko dla dalszego budowania systemu e-zdrowia, ale także zapewnienia lekarzowi łatwego dostępu do kompletnych i rzetelnych danych medycznych pacjenta, jest zapewnienie pełnej sprawozdawczości zdarzeń medycznych w uzgodnionym w ramach szerszej dyskusji społecznej zakresie. System powinien dawać lekarzowi gwarancję, że rzetelnie odzwierciedla dotychczasowe postępowanie z pacjentem (czy to w zakresie objętym zgodą pacjenta, czy w modelu opt-out). Co ważne, powinny zostać wdrożone narzędzia dokonujące chociażby podstawowej analityki danych w celu przedstawienia lekarzowi kluczowych dla niego informacji – lekarz nie powinien zostać przeciążony nadmiarem danych, lecz móc uzyskać szybki dostęp do kluczowych dla niego informacji.

Aby zwiększyć poziom sprawozdawczanych obecnie zgodnie z przepisami prawa danych, w pierwszej kolejności warto rozważyć bodziec stymulujący – powiązanie sprawozdawczości z akredytacją oraz związaną z nią korzyścią finansową.

Propozycja wpisuje się w postulat dotyczący dostępności danych – lekarz powinien mieć łatwy i szybki dostęp do danych pacjenta z różnych źródeł. Nie będzie możliwe, jeżeli system nie będzie gwarantował kompletności danych o stanie zdrowia pacjenta.

### 5.2.1.3 Utrzymująca się papierowa postać dokumentacji medycznej

**Stan obecny.** Dokumentacja medyczna powinna być obecnie – co do zasady – prowadzona w postaci elektronicznej, w tym jako elektroniczna dokumentacja medyczna. Zgodnie z § 1 ust. 1 DokMedR, dokumentacja medyczna jest prowadzona przez podmiot udzielający świadczeń zdrowotnych w postaci elektronicznej. Dokumentacja może być prowadzona w postaci papierowej tylko, jeżeli przepis prawa tak stanowi względem określonego typu dokumentu (np. karta przebiegu ciąży) lub warunki organizacyjno-techniczne uniemożliwiają prowadzenie dokumentacji w postaci elektronicznej.

Choć zgodnie z przytoczonymi przepisami niemal całość dokumentacji medycznej powinna mieć postać elektroniczną, w praktyce obowiązek zachowania tej formy nie jest powszechnie przestrzegany. O ile w świetle dostępnych danych zdecydowana większość podmiotów leczniczych (89,% ankietowanych) deklaruje posiadanie rozwiązań IT umożliwiających prowadzenie dokumentacji medycznej w postaci elektronicznej oraz elektroniczne przetwarzanie danych medycznych istotnych z punktu widzenia procesu leczenia, to 34,2% podmiotów robi to tylko częściowo. Wynika z tego, że dane z co dziesiątej placówki nie są dostępne cyfrowo, a w przypadku 30% pozostałych podmiotów jedynie część dokumentacji może być prowadzona cyfrowo. Tym samym, pomimo wielu lat informatyzacji ochrony zdrowia, dalej istotna część danych medycznych dostępna jest tylko w postaci papierowej. Dość ogólna przesłanka warunków organizacyjno-technicznych, które uniemożliwiają prowadzenie dokumentacji w postaci elektronicznej, może być nadużywana w celu unikania niezbędnych zmian i kosztów procesu digitalizacji dokumentacji medycznej.

Szczególnym rodzajem dokumentacji medycznej prowadzonej w postaci elektronicznej jest elektroniczna dokumentacja medyczna (EDM), która obejmuje dokumenty wskazane w art. 2 pkt 6 SystlnyOchZdrU, w tym m.in. dokumenty określone w DokMedR. Choć w tym przypadku nie znajduje zastosowania przywołana w poprzednim akapicie przesłanka warunków organizacyjno-technicznych, tylko niecała połowa zbadanych przez Centrum e-Zdrowia podmiotów leczniczych (45,7%) zadeklarowała, że prowadzi EDM w zakresie informacji dla lekarza kierującego świadczeniobiorcę do poradni specjalistycznej lub leczenia szpitalnego o rozpoznaniu, sposobie leczenia, rokowaniu, ordynowanych lekach, środkach spożywczych specjalnego przeznaczenia żywieniowego i wyrobach medycznych, w tym okresie ich stosowania i sposobie dawkowania oraz wyznaczonych wizytach kontrolnych<sup>64</sup>. Jedynie 28,4% badanych placówek prowadzi EDM w zakresie wyników badań laboratoryjnych wraz z opisem, a co trzeci ankietowany podmiot (33,2%) w zakresie opisu badań diagnostycznych innych niż laboratoryjne. Także w tym przypadku obowiązek prowadzenia elektronicznej dokumentacji nie jest więc w pełni egzekwowany<sup>65</sup>. Co więcej, tylko niewiele ponad połowa ankietowanych podmiotów (57,5%) wdrożyła indeksowanie EDM w systemie P1<sup>66</sup>, co tym samym oznacza, że ponad 40% wytwarzanej przez placówki medyczne EDM jest „niewidoczne” z poziomu systemu centralnego.

64. VI Edycja „Badania stopnia informatyzacji podmiotów wykonujących działalność leczniczą”, Centrum e-Zdrowia, wrzesień 2022; s. 14.

65. Tamże; str. 77.

66. Tamże str. 17.

Dodatkowo warto zauważyć, że podmioty lecznicze mają możliwość digitalizacji papierowej dokumentacji medycznej. Zgodnie z art. 13b SystInfOchrZdrU, można dokonać zmiany postaci dokumentacji medycznej prowadzonej i przechowywanej w postaci papierowej na postać elektroniczną przez sporządzenie jej odwzorowania cyfrowego i opatrzenie go kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym przez osobę upoważnioną przez usługodawcę do potwierdzenia zgodności odwzorowania cyfrowego z dokumentem w postaci papierowej. Dokument powstały w wyniku digitalizacji dokumentacji medycznej jest równoważny oryginałowi tego dokumentu. Mimo takiej możliwości, blisko 74% placówek medycznych nie poddaje digitalizacji dokumentacji prowadzonej w postaci papierowej<sup>67</sup>.



### Perspektywa zmian

Wynikający z przepisów prawa obowiązek prowadzenia elektronicznej dokumentacji medycznej na przestrzeni ostatniej dekady był już kilkakrotnie przesuwany w czasie w drodze kolejnych nowelizacji SystInfOchrZdrU (pierwotnie był zaplanowany na 2014 r.). Choć od 1 stycznia 2019 r. część dokumentów ma już obowiązkowo postać cyfrową jako elektroniczna dokumentacja medyczna, to wciąż w dużej mierze wymóg ten nie jest w praktyce spełniany.

Program rozwoju e-zdrowia w Polsce do 2027 r. wyraźnie dostrzega ten problem, słusznie wskazując, że „dotychczasowe doświadczenie w obszarze przechowywania dokumentacji medycznej na poziomie usługodawców, a także udostępniania elektronicznej dokumentacji medycznej w ramach budowy Systemu P1, wskazuje na potrzebę wsparcia usługodawców. Część z nich nie ma wystarczających środków finansowych na utrzymanie lub budowę własnych rozwiązań w obszarze repozytoriów EDM”. Nie zawiera przy tym jednak jasnych wskazań, jak problem ma zostać rozwiązany (w programie jest mowa w stosunkowo ogólny sposób o tworzeniu HUBów wymiany zleceń i wyników, którym towarzyszyć mają repozytoria EDM).

Na przestrzeni ostatnich kilkudziesięciu miesięcy strona publiczna zorganizowała dedykowane programy dofinansowania zakupu systemów do prowadzenia EDM, co niewątpliwie przyczyniło się do poprawy sytuacji. W ramach projektów skierowanych do POZ zawarto prawie dwa tysiące umów z podmiotami udzielającymi świadczeń zdrowotnych, a wartość dofinansowania wyniosła niecałe 200 mln zł. Kolejne wsparcie dla podmiotów w zakresie wdrażania elektronicznej dokumentacji medycznej przewidziane jest w Programie FENIKS (Fundusze Europejskie na Infrastrukturę, Klimat, Środowisko) na lata 2021-2027. Nabory w ramach ww. programu będą ogłaszane przez właściwe komórki organizacyjne Ministerstwa Zdrowia w 2024 r.

67. Tamże; str. 27.

68. Np. projekty wdrożenia e-usług w placówkach POZ i ich integracja z systemem e-zdrowia (akronim „e-usługi POZ”) nr POIS.11.03.00-00-0074/22 oraz „Wdrożenie e-usług w placówkach POZ i ich integracja z systemem e-zdrowia z wykorzystaniem narzędzia centralnego (akronim „Centralne e-usługi POZ” lub „e-Gabinet\*”) nr POIS.11.03.00-00-0073/22.



Pomimo braku pełnego wdrożenia w postaci cyfrowej obecnego katalogu dokumentów, Program rozwoju e-zdrowia w Polsce do 2027 r. zakłada jego dalsze poszerzenie, w szczególności wskazuje, że zostanie przygotowane narzędzie do prowadzenia karty ciąży w postaci elektronicznej, tak aby kobieta miała stały dostęp do aktualnych danych o swoim stanie zdrowia. Informacje o zdrowiu dziecka wynikające z książeczki zdrowia dziecka, karty szczepień oraz przeprowadzonych badaniach profilaktycznych będą dostępne dla rodziców w postaci elektronicznej. Katalog dokumentów, które obowiązkowo mają być prowadzone w postaci elektronicznej zawiera też EHDS, w tym m.in. skrócone karty zdrowia pacjenta czy obrazy medyczne i wyniki obrazowania medycznego (por. art. 5 EHDS).



### Możliwe działania

Podobnie jak w przypadku poprzedniego podpunktu, na obecnym etapie kluczowe jest zapewnienie przestrzegania już obowiązujących wymogów w zakresie prowadzenia dokumentacji medycznej w postaci elektronicznej. Podstawowym warunkiem dostępu do danych pacjenta jest utrwalanie ich w postaci cyfrowej oraz działanie systemu indeksującego przechowywaną w postaci elektronicznej dokumentację medyczną.

Analogicznie jak w poprzednim punkcie, aby zmienić taki stan rzeczy, można wprowadzić mechanizm promowania placówek, które rzetelnie wywiązują się z obowiązku prowadzenia dokumentacji medycznej w wymaganej postaci. Podobne mogą być narzędzia promocji, tj. włączenie obszaru prowadzenia wysokiej jakości dokumentacji medycznej w postaci elektronicznej (w tym potencjalnie także digitalizacji części dokumentacji papierowej) do standardów akredytacyjnych spowoduje, że realizacja obowiązków w tym zakresie determinować będzie możliwość otrzymania większych środków od NFZ.



### Uzasadnienie

O ile system raportowania zdarzeń medycznych będzie zapewniał podstawowe dane, zasadniczym źródłem informacji o pacjencie pozostaje dokumentacja medyczna. Dlatego też niezwykle ważne jest, by była powszechnie prowadzona i dostępna w postaci elektronicznej i dlatego właśnie potrzebne jest zwiększenie stopnia dokumentacji medycznej prowadzonej w postaci cyfrowej. Inaczej z systemowego punktu widzenia nie będziemy w stanie wykorzystać potencjału danych medycznych, które dostępne są tylko na papierze. Podobnie też lekarz ma przez to dodatkową trudność w dostępie do potrzebnych mu danych – uzyskanie przez niego dokumentów pacjenta będzie oczywiście możliwe, ale proces z tym związany będzie dużo wolniejszy – odpowiednie dokumenty papierowe będą musiały być dopiero odszukane w archiwum, zeskanowane i przesłane. Taka forma utrudni też automatyczną analizę danych, jako że skany mogą nie mieć formy nadającej się do odczytu maszynowego.

Propozycja wpisuje się w postulat dotyczący dostępności danych – lekarz powinien mieć łatwy i szybki dostęp do danych pacjenta z różnych źródeł. Wymaga to przejścia na postać elektroniczną dokumentacji medycznej oraz stworzenie mechanizmów jej sprawnego przesyłania.

## 5.2.2 Zasady dostępu lekarzy do danych przetwarzanych w podmiotach leczniczych

Zaprezentowane do tej pory zagadnienia związane z dostępnością danych medycznych miały charakter bardziej systemowy, tj. dotyczyły zasad dostępu lekarza do danych, w tym danych zawartych w dokumentacji medycznej, z poziomu systemu P1. Niezależnie od tej problematyki, w tej części raportu prezentujemy tematy dotyczące dostępności danych dla lekarza na poziomie podmiotu wykonującego działalność leczniczą.

### 5.2.2.1 Nieostra przesłanka „kontynuacji leczenia” w kontekście zasad dostępu

**Stan obecny.** Z uwagi na fakt, że zdecydowana większość dokumentacji medycznej nie stanowi elektronicznej dokumentacji medycznej, dla możliwości uzyskania dostępu do niej wciąż kluczowe są przepisy PrPacjU. Pod kątem zapewnienia pacjentowi opieki medycznej najważniejsza jest regulacja art. 26 ust. 3 pkt 1 PrPacjU, zgodnie z którym podmiot udzielający świadczeń zdrowotnych udostępnia dokumentację medyczną m.in. innym podmiotom udzielającym świadczeń zdrowotnych, jeżeli dokumentacja ta jest niezbędna do zapewnienia ciągłości świadczeń zdrowotnych. Przywołany przepis przez wiele lat był jedyną stosowaną w praktyce podstawą przekazywania dokumentacji medycznej pacjentów pomiędzy różnymi świadczeniodawcami, do dziś ogrywa w tym zakresie fundamentalną rolę. Jednocześnie jest to rozwiązanie przyjęte jeszcze w 2009 r., jak można zakładać, głównie z myślą o przekazywaniu dokumentacji medycznej w postaci papierowej.

W obecnych uwarunkowaniach faktycznych i prawnych wynikająca z przywołanego przepisu norma jest już mniej oczywista. Zasady dostępu do danych osobowych pacjentów i ich jednostkowych danych medycznych, które są podstawową treścią dokumentacji medycznej, reguluje na odmiennych zasadach art. 35 SystInfOchrZdrU. Pojawia się więc np. pytanie o podstawy prawne automatycznego transferu dokumentacji medycznej do zewnętrznych repozytoriów, np. tzw. platform regionalnych (które mogą działać w różnych modelach, np. jako niezależny administrator danych), które mogłyby przechowywać kopię dokumentacji na wypadek potrzeby jej szybkiego udostępnienia w celu leczniczym w przyszłości. Wreszcie też nieprecyzyjna jest przesłanka „niezbędności” dokumentacji do zapewnienia ciągłości świadczeń zdrowotnych – kto i wedle jakich kryteriów miałby to oceniać, jaki zakres dokumentacji jest faktycznie niezbędny pod kątem określonego zabiegu itd. Choć w praktyce przesłanka ta jest interpretowana dość szeroko i nie jest przedmiotem zasadniczych sporów, pod kątem pewności prawa warto rozważyć jej nowelizację z uwzględnieniem zasad transferu dokumentów w postaci cyfrowej.



### Perspektywa zmian

Program rozwoju e-zdrowia w Polsce do 2027 r. zapowiada przygotowanie ustawy o danych medycznych regulującej cały obszar danych medycznych i dokumentacji medycznej w jednym akcie prawnym. Choć nie przedstawiono dokładniejszych założeń czy zakresu tego aktu, jak należy przyjąć, powinien on uwzględniać m.in. uchylene lub zmianę omawianego art. 26 ust. 3 pkt 1 PrPacjU.



## Możliwe działania

Przyjęcie osobnej ustawy o danych medycznych jest uzasadnione i potrzebne. W ten sposób możliwe będzie doprowadzenie do uchylecia lub zmiany dotychczasowych przepisów regulujących dostęp do danych i dokumentacji pacjenta, które przyjmowane były w różnych okresach czasu i rozsięte są po różnych aktach prawnych, oraz przyjęcie w tej materii jednej, kompleksowej, spójnej i jasnej regulacji. Podobnie jak w przypadku art. 26 ust. 3 pkt 1 PrPacjU, lekarz powinien mieć zapewniony dostęp do niezbędnych mu informacji o stanie zdrowia pacjenta (por. pkt 5.2.1.1 raportu).



## Uzasadnienie

Mając na uwadze dalsze wyzwania, w tym zapewnienie łatwego dostępu do danych medycznych niezbędnych do kontynuacji leczenia zgodnie z zasadami EHDS, warto dokonać pełnego przeglądu obecnie obowiązujących regulacji w tym zakresie oraz uporządkować je w ramach dedykowanej ustawy o danych medycznych. Przyjęcie jasnych i czytelnych dla odbiorców zasad w jednym akcie prawnych powinno pozytywnie wpłynąć na praktykę ich stosowania. Dotychczasowe doświadczenia wskazują, że wszelkie wątpliwości interpretacyjne i związane z nimi ryzyko działa niekorzystnie na proces dostępu do danych.

Propozycja wpisuje się w postulat dotyczący dostępności danych – lekarz powinien mieć łatwy i szybki dostęp do danych pacjentów z różnych źródeł.

### 5.2.2.2 Upoważnienia do przetwarzania danych i kontrola dostępu

**Stan obecny.** Zgodnie z art. 24 ust. 2 PrPacjU, lekarz, jako osoba wykonująca zawód medyczny, jest ustawowo uprawniony do przetwarzania danych zawartych w dokumentacji medycznej. Przepis ten należy odczytywać w świetle art. 29 RODO, zgodnie z którym każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego. Pomimo ustawowego upoważnienia, administrator danych może zdecydować o nadawaniu upoważnień do przetwarzania danych osobowych lekarzom i innym osobom wykonującym zawód medyczny przetwarzającym dane pacjentów w ramach wykonywania zawodu jako jednym ze środków organizacyjnych, którego celem jest zapewnienie odpowiedniej ochrony danych i kontroli nad procesem ich przetwarzania<sup>69</sup>.

O ile samo upoważnienie lekarzy do przetwarzania danych zawartych w dokumentacji medycznej nie budzi wątpliwości, należy pamiętać o dokonywaniu tego zgodnie z wewnętrznymi procedurami lub zasadami postępowania. Zakres upoważnienia powinien być dostosowany do zadań zawodowych, co ma szczególne uzasadnienie w szczególności w szpitalach i większych placówkach – gdzie nie występuje potrzeba, by lekarz miał co do zasady dostęp do dokumentacji medycznej pacjentów z innego oddziału (z zastrzeżeniem np. stanów nagłych). Na zbyt szerokie uprawnienia dostępowe pracowników podmiotów leczniczych zwracała uwagę m.in. NIK<sup>70</sup>. Podobne naruszenia

69. Por. [www.uodo.gov.pl/pl/225/1578](http://www.uodo.gov.pl/pl/225/1578)

70. Informacje o wynikach kontroli „Wdrożenie przez podmioty lecznicze regulacji dotyczących ochrony danych osobowych”, NIK, Warszawa 2019; str. 37

związane z brakiem kontroli nad zakresem dokumentacji, która jest dostępna dla pracowników podmiotów leczniczych, były też stwierdzane w szpitalach w innych państwach Unii Europejskiej.



### Perspektywa zmian

Zgodnie z art. 4 EHDS, w przypadku przetwarzania danych w formacie elektronicznym pracownicy służby zdrowia mają mieć dostęp do elektronicznych danych dotyczących zdrowia osób fizycznych, które leczą, niezależnie od państwa członkowskiego ubezpieczenia i państwa członkowskiego leczenia. Zgodnie z zasadą minimalizacji danych przewidzianą w RODO państwa członkowskie mogą ustanowić przepisy określające kategorie elektronicznych danych osobowych dotyczących zdrowia wymaganych przez różne zawody związane ze służbą zdrowia (przepisy te nie mogą opierać się na źródle elektronicznych danych dotyczących zdrowia), przy czym państwa członkowskie zapewniają pracownikom służby zdrowia dostęp co najmniej do priorytetowych kategorii elektronicznych danych dotyczących zdrowia. Regulacja daje więc możliwość określenia na poziomie krajowym zasad dostępu lekarzy do określonych danych medycznych (co już obecnie poniekąd ma miejsce, m.in. art. 24 ust. 2 PrPacjU, art. 35 SystInfOchrZdrU).



### Możliwe działania

Mając na uwadze dotychczasową praktykę oraz okoliczność zmian, które może wprowadzić EHDS, można na poziomie krajowym wyraźnie doprecyzować zasady wydawania lekarzom upoważnień do przetwarzania elektronicznych danych medycznych. EHDS nakłada m.in. na lekarzy obowiązek zapewnienia, aby elektroniczne dane osobowe dotyczące zdrowia osób fizycznych, których leczą, były aktualizowane o informacje dotyczące udzielonych świadczeń zdrowotnych. Nowy system upoważnień powinien więc być bardziej precyzyjny, dostosowany do miejsca pracy, zakresu obowiązków lekarza i związanej z tym grupy pacjentów, którymi się rzeczywiście opiekuje (np. dostosowany do struktury jednostek organizacyjnych, w których działa lekarz). Wdrożenie podobnego rozwiązania pozwoli m.in. lepiej zaadresować nowy obowiązek aktualizowania danych.

Uzupełniająco lub alternatywnie, jako że obowiązująca regulacja ustawowa jest elastyczna i daje duże możliwości działania w tym zakresie na poziomie podmiotu leczniczego, wystarczające może być przygotowanie i opublikowanie wytycznych dotyczących nadawania upoważnień lekarzom oraz innym osobom wykonującym czynności pomocnicze przy udzielaniu świadczeń zdrowotnych. Zasadniczym problemem nie jest bowiem brak regulacji, lecz praktyka ich stosowania, która jest różna w różnych podmiotach wykonujących działalność leczniczą.



## Uzasadnienie

Z uwagi na ustawowe uprawnienie lekarzy do przetwarzania danych zawartych w dokumentacji medycznej, które ma generalny charakter, część podmiotów wykonujących działalność leczniczą nie przykłada należytej wagi do kontroli zasad dostępu do danych i dokumentacji, w której są zawarte. Oczywiście nie budzi wątpliwości konieczność dostępu lekarza do danych pacjentów, którym udziela świadczeń zdrowotnych. Jednocześnie też nie ma uzasadnienia dla swobodnego dostępu lekarza do danych zupełnie dowolnego pacjenta. Bardziej precyzyjny sposób wydawania upoważnień będzie wymaganym przez RODO środkiem ochrony przed naruszeniami zasady poufności i rozliczalności.

Propozycja wpisuje się w postulat dotyczący dostępności danych – lekarz powinien mieć łatwy i szybki dostęp do danych pacjentów z różnych źródeł. Ważne jest przy tym zachowanie kontroli nad dostępem i zapewnienie jego odpowiedniego zakresu względem obowiązków.

### 5.2.2.3 Upoważnienia do przetwarzania danych i kontrola dostępu

**Stan obecny.** Przepisy prawa medycznego opierają się na zasadzie neutralności technologicznej. Podmioty wykonujące działalność leczniczą mogą stosować dowolną liczbę systemów IT tak długo, jak spełniają one wymagane przepisami prawa funkcjonalności oraz standardy bezpieczeństwa. W praktyce, w szczególności w przypadku większych placówek medycznych, równolegle działają obok siebie co najmniej kilka różnych wewnętrznych systemów informatycznych, które nie zawsze są ze sobą w pełni kompatybilne. Skutkiem takiego stanu rzeczy jest sytuacja, w której lekarz potrzebuje kilku loginów i haseł, by uzyskać dostęp do potrzebnych mu informacji. W sytuacjach, w którym dostęp do danych jest pilny, ryzyko związane np. z zapomnieniem hasła jest tym bardziej istotne. Dodatkową trudnością są obowiązki raportowania określonych danych do różnych systemów, np. raportowanie zdarzeń medycznych, rozliczenia z płatnikiem publicznym, statystyka itp.



## Perspektywa zmian

Wskazany problem nie jest w wyraźny sposób zaadresowany przez projektowane zmiany. Kwestia interoperacyjności dokumentacji medycznej w postaci elektronicznej regulowana będzie przez EHDS, które zakłada, że każdy system elektronicznej dokumentacji medycznej umożliwi wymianę elektronicznych danych osobowych dotyczących zdrowia między pracownikami służby zdrowia lub innymi podmiotami systemu opieki zdrowotnej oraz między pracownikami służby zdrowia i portalami dla pacjentów lub pracowników służby zdrowia w powszechnie stosowanym interoperacyjnym formacie elektronicznym, który obejmuje m.in. zawartość zbiorów danych, struktury danych, formaty danych, słowniki, taksonomie, formaty wymiany, normy, specyfikacje, profile wymiany i wykazy kodów, umożliwiając w ten sposób komunikację międzysystemową. System elektronicznej dokumentacji medycznej zaprojektowany do użytku przez pracowników systemu ochrony zdrowia ma także zapewniać wiarygodne mechanizmy służące identyfikacji i uwierzytelnianiu pracowników, w tym kontrole w zakresie praw i kwalifikacji zawodowych<sup>71</sup>. Tym samym stworzone będą musiały zostać „mechanizmy służące identyfikacji i uwierzytelnianiu pracowników”, które potencjalnie można ustandaryzować.

71. Por. załącznik nr 2 do EHDS.



## Możliwe działania

Z perspektywy lekarza ważne jest doprowadzenie do sytuacji, w której w ramach jednego konta lub korzystając z jednego sposobu uwierzytelniania mógłby korzystać z wielu różnych systemów IT wykorzystywanych przez dany podmiot leczniczy (zasada jednego konta). Kwestia interoperacyjności oraz przenaszalności przetwarzanych danych regulowana będzie na poziomie unijnym w celu zapewnienia łatwej transgranicznej wymiany danych. Na poziomie krajowym pożądanym jest zaś wypracowanie standardu uniwersalnego uwierzytelniania lekarza w różnych systemach IT (np. wykorzystanie weryfikacji biometrycznej), by miał możliwość łatwego korzystania z szeregu różnych narzędzi cyfrowych bez potrzeby oddzielnego logowania się z wykorzystaniem innych danych. Zmiana o takim charakterze może mieć charakter prawny, tj. umocowany w przepisach ustawy lub rozporządzenia wymóg zapewnienia integracji z innymi systemami do prowadzenia dokumentacji pacjentów w zakresie nadawania dostępu użytkownikom na wspólnych zasadach, lub pozaprawny – wypracowanie branżowego standardu. Zmiany prawne powinny też zapewnić urzeczywistnienie zasady tzw. jednej klawiatury, tj. dane raz wpisane powinny służyć różnym celom sprawozdawczym, bez konieczności ponownego ręcznego wprowadzania tych samych danych do różnych systemów<sup>72</sup>.

Należy dalej rozwijać systemy informatyczne ułatwiające pracę lekarza, które będą pozwalać na zasilanie danymi różnych systemów dedykowanych (np. historia choroby, rejestr jakości, inny rejestr medyczny).



## Uzasadnienie

Wyniki dotychczasowych kontroli wskazują, że dużym problemem w kontekście dostępu do danych jest zarządzanie systemem uwierzytelniania w systemach IT<sup>73</sup>. W celu jego ułatwienia – czy wręcz obchodzenia procesu logowania – stosowane są np. krótkie i proste hasła, które nie spełniają standardów bezpieczeństwa, lub następuje przyznawanie loginów i haseł wspólnych dla kilku lub kilkudziesięciu osób<sup>64</sup>. Tym samym, oprócz możliwości łatwej migracji danych pacjenta pomiędzy różnymi systemami, lekarz powinien mieć także zapewniony prosty sposób uwierzytelniania, który umożliwi mu logowanie się do różnych systemów z poziomu jednego konta lub przy użyciu jednej spójnej metody potwierdzania uprawnień. Na analogicznych zasadach dane raz wprowadzone do jednego systemu powinny móc nadawać się do zaimportowania do innego systemu w celu realizacji obowiązków sprawozdawczych.

Propozycja wpisuje się w postulat dotyczący dostępności danych – lekarz powinien mieć łatwy i szybki dostęp do danych pacjentów z różnych źródeł. Lekarz nie powinien tracić czasu związanego z różnymi sposobami logowania się do poszczególnych systemów.

73. Informacje o wynikach kontroli „Wdrożenie przez podmioty lecznicze regulacji dotyczących ochrony danych osobowych”, NIK, Warszawa 2019.; str. 14

## 5.3 Postępowanie z danymi medycznymi

Po uzyskaniu dostępu do danych medycznych lekarz powinien móc je skutecznie wykorzystać – w tym przy wsparciu dedukowanych narzędzi, np. systemów predykcji opartych o AI - zachowując ich bezpieczeństwo i poufność. Jednym z kluczowych wyzwań związanych z rosnącą ilością dostępnych dla lekarza danych dotyczących bezpośrednio lub pośrednio stanu zdrowia pacjenta jest ich kategoryzacja pod kątem jakości i wartości terapeutycznej. W środowisku cyfrowym szybko zaciera się granica pomiędzy tradycyjnie rozumianą dokumentacją a zbiorem danych, które mogą pochodzić z różnych mniej lub bardziej zaufanych źródeł, takich jak elektroniczna dokumentacja medyczna, rejestry medyczne, wyroby medyczne czy też inne urządzenia i systemy mierzące określone parametry organizmu pacjenta. Wreszcie część danych może być wpisywana samodzielnie przez pacjenta. Także pod kątem wartości naukowej oraz potencjału związanego z możliwością wykorzystania danych do trenowania algorytmów AI szczególnego znaczenia nabiera klasyfikowanie gromadzonych i wykorzystywanych przez lekarza danych.

### 5.3.1 Podejście oparte o dane

System obiegu informacji o pacjencie opiera się na tradycyjnym pojęciu dokumentacji medycznej, która stosowana jest w podmiotach leczniczych od XVIII wieku. Zmiany technologiczne przemawiają na rzecz skupienia się na danych, a nie sformalizowanych dokumentach. Taka systemowa zmiana podejścia jest w stanie zapewnić szereg korzyści. Dane są o wiele bardziej funkcjonalne niż dokumenty, tzn. dużo łatwiej zestawiać je ze sobą i wykonywać na nich operacje. Przykładowo, analiza kosztów określonego świadczenia w skali całego szpitala w przypadku dokumentacji medycznej wymagała weryfikacji pełnej treści poszczególnych dokumentów pod kątem pożądaných kryteriów i zestawienia tak uzyskanych, zbiorczych informacji z danymi fiskalnymi. Bazując na bazach danych możliwa jest automatyczna selekcja wyników pod kątem wskazanych kryteriów, co zapewnia istotną oszczędność czasu. Bazy danych mogą być także bezpośrednio wykorzystywane przez oprogramowanie analityczne lub systemy oparte o AI, co ułatwia ich wtórne wykorzystanie np. w celach naukowych. Ważna jest przy tym odpowiednia kategoryzacja różnych danych, z których może korzystać lekarz. Ustrukturyzowane zbiory danych autoryzowane przez lekarza podpisem dalej mogą pełnić tę samą funkcję, co dokumentacja medyczna. Odróżnienie od siebie różnych zbiorów może być podstawą do odmiennego uregulowania np. dopuszczalnego zastosowania, okresu przechowania czy zasad podziału odpowiedzialności za ich gromadzenie i przetwarzanie.

#### 5.3.1.1 Dokumentacja medyczna a jednostkowe dane medyczne

**Stan obecny.** Regulacje prawne dotyczące obszaru przetwarzania danych medycznych przyjmowane były na przestrzeni ostatnich kilkunastu lat, na kolejnych etapach budowy systemu e-zdrowia w Polsce. W efekcie tego procesu funkcjonuje obecnie nieintuicyjny i niespójny system pojęć prawnych, który może wywoływać niepotrzebne wątpliwości interpretacyjne i utrudniać postępowanie z danymi.

Na gruncie art. 2 pkt 4 SystInfOchrZdrU, dane oznaczają litery, wyrazy, cyfry, teksty, liczby, znaki, symbole, obrazy, kombinacje liter, cyfr, liczb, symboli i znaków, zebrane w zbiory o określonej strukturze, dostępne według określonych kryteriów, w tym dane osobowe. Tak rozumiane dane

mogą stanowić jednostkowe dane medyczne, czyli zgodnie z art. 2 pkt 7 SystInfOchrZdrU, dane osoby fizycznej o udzielonych, udzielanych i planowanych świadczeniach opieki zdrowotnej oraz dotyczące jej stanu zdrowia, w tym profilaktyki zdrowotnej i realizacji programów zdrowotnych. Co ważne, art. 35 SystInfOchrZdrU pod kątem zasad dostępu do danych odróżnia od siebie pojęcia danych osobowych oraz jednostkowych danych medycznych usługobiorców, co rodzi dodatkowe wątpliwości o status jednostkowych danych medycznych na gruncie RODO.

Zgodnie z art. 4 pkt 1 RODO dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, przy czym możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Tym samym pojawia się wątpliwość, jak rozumieć pod tym kątem jednostkowe dane medyczne, które stanowią „dane osoby fizycznej”, a które jednocześnie w świetle art. 35 SystInfOchrZdrU wcale nie muszą stanowić danych osobowych. Takie ujęcie sugeruje, że jednostkowe dane medyczne obejmują też dane nieosobowe, czyli np. dane z dokumentacji medycznej poddane anonimizacji. Tym samym udostępnienie jakichkolwiek danych z systemu IT podmiotu leczniczego wymagałoby zgody pacjenta, nawet w sytuacji, w której nie da się już zidentyfikować, którego pacjenta dane dotyczą.

Co więcej, dane osobowe, jak i jednostkowe dane medyczne, utrwalane są w ustrukturyzowany sposób w dokumentacji medycznej. Pojęcie dokumentacji medycznej nie zostało zdefiniowane. Zgodnie z art. 25 PrPacjU, dokumentacja medyczna zawiera co najmniej oznaczenie pacjenta, pozwalające na ustalenie jego tożsamości, oznaczenie podmiotu udzielającego świadczeń zdrowotnych ze wskazaniem komórki organizacyjnej, w której udzielono świadczeń zdrowotnych opis stanu zdrowia pacjenta lub udzielonych mu świadczeń zdrowotnych oraz datę sporządzenia. Dokumenty zawierające wskazany zakres danych powinny być uznawane za dokumentację medyczną (konkretne typy wybranych dokumentów regulowane są dodatkowo przez przepisy odrębne, w szczególności regulację DokMedR).

Zgodnie z par. 1 ust. 1 DokMedR dokumentacja medyczna jest prowadzona przez podmiot udzielający świadczeń zdrowotnych w postaci elektronicznej. Szczególnym typem dokumentacji medycznej jest elektroniczna dokumentacja medyczna, która zgodnie z art. 2 pkt 6 SystInfOchrZdrU oznacza dokumenty wytworzone w postaci elektronicznej opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym, podpisem osobistym albo z wykorzystaniem sposobu potwierdzania pochodzenia oraz integralności danych dostępnego w systemie teleinformatycznym udostępnionym bezpłatnie przez Zakład Ubezpieczeń Społecznych: recepty, dokumenty określone w przepisach wydanych na podstawie art. 13a SystInfOchrZdrU, skierowania określone w przepisach wydanych na podstawie art. 59aa ust. 2 ŚOZŚrPubU, zlecenia na zaopatrzenie i zlecenia naprawy wyrobów medycznych, Karty Szczepień oraz wyniki badania histopatologicznego.



Powyższe rozróżnienie jest istotne i zarazem problematyczne głównie pod kątem zasad dostępu do danych – inne są bowiem zasady dostępu do jednostkowych danych medycznych (które mogą – ale wcale nie muszą – być częścią elektronicznej dokumentacji medycznej lub innej dokumentacji prowadzonej w postaci elektronicznej), inne zaś do dokumentacji medycznej. Inne są podstawy i zasady udostępniania danych osobowych, a inne danych nieosobowych (danych anonimowych).



### Perspektywa zmian

Program rozwoju e-zdrowia w Polsce do 2027 r. przewiduje przygotowanie ustawy o danych medycznych regulującej cały obszar danych medycznych i dokumentacji medycznej w jednym akcie prawnym. Przyjęcie tej regulacji jest doskonałą okazją do dokonania weryfikacji oraz uporządkowania siatki pojęciowej z tego obszaru.

Jest to tym bardziej zasadne, jako że EHDS operuje jeszcze innymi pojęciami, takimi jak m.in. „elektroniczne dane osobowe dotyczące zdrowia”, które oznaczają dane dotyczące zdrowia i dane genetyczne w rozumieniu RODO, a także dane odnoszące się do czynników warunkujących zdrowie lub dane przetwarzane w związku z udzielaniem świadczeń zdrowotnych, przetwarzane w formie elektronicznej, a także „elektroniczne dane nieosobowe dotyczące zdrowia” oznaczają dane dotyczące zdrowia i dane genetyczne w formacie elektronicznym, które nie wchodzą w zakres definicji danych osobowych zawartej w art. 4 pkt 1 RODO, czy wreszcie „elektroniczne dane dotyczące zdrowia”, które oznaczają elektroniczne dane osobowe lub nieosobowe dotyczące zdrowia. Co więcej, EHDS wyraźnie odróżnia dane od dokumentu, definiując „elektroniczną dokumentację medyczną” jako zbiór elektronicznych danych dotyczących zdrowia odnoszących się do osoby fizycznej i zgromadzonych w systemie opieki zdrowotnej, przetwarzanych do celów opieki zdrowotnej. Zaproponowana definicja jest bardzo pojemna, obejmuje potencjalnie szeroki zakres danych odnoszących się do pacjenta. Warto jednak zauważyć, że EHDS postuluje się tym pojęciem w poszczególnych przepisach głównie pod kątem wymogów dla systemów do prowadzenia elektronicznej dokumentacji medycznej lub formatów jej wymiany. Wskazuje to, że pojęciem tym posłużono się pod kątem dookreślenia wymogów dla przetwarzania elektronicznych danych dotyczących zdrowia, a nie dookreślenia zakresu dokumentacji medycznej w dotychczasowym rozumieniu krajowej regulacji.



### Możliwe działania

Mając na uwadze, że zmienia się system gromadzenia danych na temat pacjenta – miejsce dotychczasowych papierowych teczek stopniowo zajmują elektroniczne bazy danych, zasadne jest rozważenie odejścia od podejścia opartego o pojęcie dokumentu na rzecz, wzorem EHDS, podejścia opartego o pojęcie danych. Dane na temat pacjenta mogą pochodzić z różnych źródeł (por. następny podpunkt raportu) i być przetwarzane równolegle w różnych bazach danych (.in.. systemach gabinetowych, rejestrach medycznych, platformach e-zdrowia). Zbiory cyfrowych danych pacjenta autoryzowane cyfrowym podpisem lekarza lub innej osoby wykonującej zawód medyczny mogą przy tym dalej stanowić dokumentację medyczną w postaci elektronicznej.

Pożądanym jest dostosowanie nowego modelu do podejścia prezentowanego w EHDS, czyli rozróżnienia zbiorów danych osobowych i nieosobowych – jest to kluczowe pod kątem zasad dostępu i wykorzystywania tych danych, które w przypadku danych nieosobowych powinny być znacznie bardziej otwarte i dostępne. Należy przy tym opracować zasady wykorzystywania danych medycznych, które będą ograniczały możliwość przekazywania i wykorzystywania danych wyłącznie w postaci dobrze zdefiniowanych modułów o jednoznacznie określonym znaczeniu klinicznym zawartej w nich informacji i o kontekście ich wytworzenia. Zasadna jest więc kategoryzacja danych, z których znaczna część może stanowić dokumentację medyczną, o czym szerzej w kolejnym punkcie raportu.

Należy przy tym wyraźnie podkreślić, że niezależnie od przyjętej nomenklatury, odpowiedzialność za przetwarzanie danych zgromadzonych w systemach podmiotów wykonujących działalność leczniczą, dalej powinny ponosić te podmioty (analogicznie jak obecnie w kontekście dokumentacji medycznej). Nie wyklucza to możliwości uregulowania zasad postępowania z danymi medycznymi poza podmiotami wykonującymi działalność leczniczą, np. przez wytwórców wyrobów medycznych, ubezpieczycieli, itp.



### Uzasadnienie

Obowiązujące regulacje z jednej strony posługują się pojęciem dokumentacji medycznej (z którym związane jest m.in. prawo pacjenta do dokumentacji medycznej), z drugiej zaś operują pojęciem jednostkowych danych medycznych, które mogą stanowić dane zawarte w takiej dokumentacji. Co więcej, przewidują dla nich inne zasady dostępu, niż dla samej dokumentacji. Sytuacja taka może być mało czytelna dla pacjentów i lekarzy oraz rodzi zupełnie niepotrzebne ryzyka związane z interpretacją prawa. Uporządkowanie obecnej siatki pojęciowej jest więc potrzebne i powinno być dokonane z perspektywy wykorzystania jednostkowych danych medycznych jako bazowego pojęcia dla uregulowania praw i obowiązków związanych z tym obszarem. Dostosowanie terminologii do terminów, którymi posługuje się EHDS, przyczyni się do wyeliminowania niepotrzebnych wątpliwości interpretacyjnych dotyczących zasad postępowania z określonymi zbiorami danych lub dokumentów, w szczególności w zakresie ich udostępniania. Jasność i przejrzystość w tym zakresie jest podstawą skutecznego obiegu danych, których wykorzystywanie, w tym transferowanie do innych podmiotów, powinno następować bez obaw o ewentualne naruszenie prawa z uwagi na jego nieprecyzyjność czy niedostosowanie do obecnych realiów. Nie wyklucza to też w żaden sposób kategoryzacji danych, z których większość tak jak dotychczas może być zbierana w ustrukturyzowany sposób i autoryzowana podpisem przez personel medyczny, z powodzeniem pełniąc funkcję dokumentacji medycznej.

Odejście od obecnego rozumienia dokumentacji medycznej (danych zbieranych i przetwarzanych w celu wsparcia procesu leczenia) jako zbioru dokumentów medycznych niesie ze sobą ryzyko wybiórczego korzystania z jednostkowych danych medycznych bez zachowania kontekstu, w których informacja medyczna została zapisana i przekazana.

Propozycja wpisuje się w postulat dotyczący zapewnienia funkcjonalnego wykorzystywania danych - lekarz powinien móc sprawnie korzystać z różnych danych, a także aplikacji i programów, które pomogą mu zebrać, przeanalizować oraz wykorzystać dane w procesie opieki nad pacjentem. Aby było to możliwe, ważne jest uporządkowanie siatki pojęciowej w przepisach prawa.

### 5.3.1.2 Dane pochodzące z wyrobów medycznych i innych źródeł

**Stan obecny.** Jak wynika z poprzedniego podpunktu raportu, centralnym pojęciem dla obiegu danych na temat pacjenta pozostaje ciągle dokumentacja medyczna, w której zawarte mogą być jednostkowe dane medyczne. Tymczasem lekarz ma dostęp do coraz większej ilości danych na temat pacjenta pochodzących z różnych źródeł, w szczególności wyrobów medycznych, które mogą być stosowane bezpośrednio przez lekarza lub pacjenta, stacjonarnie lub w sposób telemedyczny, czy też różnego rodzaju narzędzi o podobnym charakterze nie stanowiących jednak wyrobów medycznych. Wreszcie sam pacjent decyduje o udostępnianiu pewnych danych, m.in. samodzielnie dokonywanych pomiarów, np. w ramach elektronicznych dzienniczków. Część danych na podstawie innych danych mogą generować systemy oparte o AI. Tym samym lekarz będzie miał coraz częściej dostęp do różnego rodzaju danych, które mogą znacząco różnić się jakością i poziomem wiarygodności.

Obecnie obowiązujące regulacje prawne nie uwzględniają jeszcze powyższej specyfiki. Lekarz może mieć do czynienia z danymi pacjenta o różnym charakterze, które będą załączane do dokumentacji medycznej lub przechowywane na innych zasadach (regulacje prawne nie przesądzają jednoznacznie statusu np. zapisów z kamery laparoskopowej lub podobnych rozwiązań).

Taka sytuacja jest problematyczna z dwóch podstawowych względów. Po pierwsze, nie jest jasne, jak należy kwalifikować podobne dane pod kątem prawnym – jako dokumentację medyczną lub dane, w tym np. dane „surowe” przetwarzane obok dokumentacji medycznej, a zatem jakie wymogi należy spełniać w związku z ich przetwarzaniem i udostępnianiem (z uwagi na ich wrażliwy charakter oraz wartość dowodową dane takie włączane są zazwyczaj do dokumentacji medycznej, co m.in. może generować dodatkowe koszty związane z jej przechowywaniem). Po drugie, lekarz może nie wiedzieć, którym danym należy ufać, a względem których powinno się zachować większą ostrożność. Potrzebny byłby w tym zakresie rodzaj drogowaskazu, który ułatwi orientację w charakterze poszczególnych zbiorów danych.



### Perspektywa zmian

Program rozwoju e-zdrowia w Polsce do 2027 r. przewiduje przygotowanie ustawy o danych medycznych regulującej cały obszar danych medycznych i dokumentacji medycznej w jednym akcie prawnym. Przyjęcie tej regulacji jest doskonałą okazją również do wprowadzenia jasnych zasad przetwarzania danych medycznych pochodzących potencjalnie z różnych źródeł.

Podstawowym punktem odniesienia może być EHDS, które wskazuje na potrzebę dostarczenia wszystkim zainteresowanym stronom informacji na temat zbiorów danych umieszczanych w europejskiej przestrzeni danych dotyczących zdrowia w postaci m.in. znaków jakości

i użyteczności, arkuszy informacyjnych dotyczących zbioru danych, a także dostarczania użytkownikom danych aktualnych informacji na temat jakości i użyteczności danych znajdujących się w zbiorach danych. Znak jakości i użyteczności danych, którym byłyby opatrywane zbiory, informowałby użytkowników danych o jakości i cechach użytkowych zbioru danych oraz umożliwiałby im wybór zbiorów, które najlepiej odpowiadają ich potrzebom.

Co więcej, EHDS wprowadza pojęcie aplikacji wspierającej dobrostan, która oznacza każde urządzenie lub oprogramowanie przewidziane przez producenta do używania przez osobę fizyczną do przetwarzania elektronicznych danych dotyczących zdrowia do celów innych niż opieka zdrowotna, takich jak dobrostan i prowadzenie zdrowego stylu życia. EHDS jasno wskazuje, że jeżeli dane generowane przez aplikacje wspierające dobrostan są przydatne w kontekście opieki zdrowotnej, użytkowników tego typu aplikacji wspierających dobrostan, w tym aplikacji mobilnych, należy informować, czy takie aplikacje można połączyć z systemami elektronicznej dokumentacji medycznej lub krajowymi elektronicznymi rozwiązaniami w zakresie zdrowia i wykorzystywać do przesyłania danych do takich systemów lub rozwiązań. Tym samym wprowadzona zostanie nowa kategoria źródła danych w postaci aplikacji wspierających dobrostan.

Poza tym, jak można zakładać, wciąż będą inne źródła danych mogących mieć znaczenie kliniczne. Pod tym kątem należy zwrócić uwagę, że AI w oparciu o dane jest w stanie generować zupełnie nowe zestawy danych, których także nie należy ignorować.



### Możliwe działania

Uzasadnione jest przyjęcie podejścia prezentowanego w EHDS, a więc znakowania zbiorów danych pod kątem ich jakości, wiarygodności i użyteczności. Przyjęty system znaków powinien uwzględniać w szczególności wykorzystywanie danych przez lekarza – dostarczać działającemu z należytą starannością profesjonalście bardzo szybkiej i jasnej wskazówki, z jakim poziomem zaufania może traktować określone zbiory danych i wynikające z nich informacje. Przykładowo, zbiory danych o niskiej jakości pochodzące ze źródeł, które nie stanowią wyrobów medycznych, mogłyby być podstawą do kontaktu z pacjentem i zasugerowania mu badań potrzebnych do ich potwierdzenia. Kluczowe będzie odpowiednie zaprojektowanie systemu klasyfikacji – najwyższym poziomem zaufania powinny cieszyć się dane autoryzowane przez personel medyczny, czyli odpowiednik dokumentacji medycznej. Im większej kontroli podlega źródło danych np. wyrób medyczny lub niecertyfikowane rozwiązanie, zastosowanie pod nadzorem profesjonalisty lub samodzielnie przez pacjenta, tym wyższy powinien być poziom zaufania do tych danych (a tym samym niższa odpowiedzialność lekarza za ewentualne szkody związane z tym, że dane były jednak błędne, niekatulane lub niekompletne). Dodatkowo, z taką klasyfikacją danych mogą iść w parze odmienne obowiązki, np. krótszy okres przechowywania części danych jedynie o pomocniczym charakterze.

Alternatywnie lub uzupełniająco, bez dokonywania interwencji prawnej (w szczególności przed przyjęciem rozwiązań wymaganych przez EHDS), możliwe jest także wypracowanie przez środowisko, we współpracy ze stroną publiczną, wytycznych i rekomendacji w tym zakresie.

Jedynie sygnalizacyjnie warto zwrócić też uwagę, że w przypadku wyrobów medycznych dane medyczne uzyskiwane przez te wyroby mogą być gromadzone i administrowane przez przedsiębiorców. Zbiory takie mogą zostać objęte szczególną regulacją: być prawnie chronione, łatwo dostępne, nie tylko dla pacjenta, ale też upoważnionego przez niego lekarza, a prawo powinno gwarantować możliwość ich udostępniania dla dobra publicznego<sup>74</sup>.



### Uzasadnienie

Zaproponowane rozwiązanie w pierwszej kolejności uporządkuje zasady postępowania z określonymi rodzajami danych. Będzie jasno wskazywać, jakie wymogi regulacyjne należy spełniać w związku z ich przetwarzaniem i udostępnianiem. Po drugie, dzięki systemowi oznaczeń lekarz zostanie wyposażony w wiedzę, którym danym może ufać, a względem których powinien zachować dużo większą ostrożność. Zapewni to lepszą orientację w charakterze poszczególnych zbiorów danych, co pozwoli zaoszczędzić czas pracy profesjonalisty medycznego potrzebny na ich analizę i rozróżnienie. Wpływać będzie także na odpowiedzialność lekarza, który działając z należytą starannością powinien móc bazować na systemie znakowania zbiorów danych pod kątem ich jakości, wiarygodności i użyteczności, bez konieczności każdorazowej samodzielnej ich weryfikacji pod tym kątem.

Propozycja wpisuje się w postulat dotyczący zapewnienia funkcjonalnego wykorzystywania danych - lekarz powinien móc sprawnie korzystać z różnych danych, a także aplikacji i programów, które pomogą mu zebrać, przeanalizować oraz wykorzystać dane w procesie opieki nad pacjentem. W tym celu lekarz powinien mieć jasne informacje o statusie poszczególnych danych oraz ich jakości i wiarygodności.

## 5.3.2 Bezpieczeństwo przetwarzania

Jednym z głównych wyzwań związanych z przejściem na cyfrową postać dokumentacji medycznej jest zapewnienie wysokiego poziomu jej bezpieczeństwa. Wymaga to zrozumienia przez lekarzy różnych zagrożeń związanych z przetwarzaniem danych pacjentów w środowisku cyfrowym oraz dostępu do produktów i usług zapewniających ochronę danych.

### 5.3.2.1 Stosowanie środków ochrony danych medycznych

**Stan obecny.** Regulacje prawne przewidują objęcie danych medycznych szczególną ochroną. Dane te, jako dane osobowe, podlegają pod przepisy RODO. Dane o stanie zdrowia, które w świetle art. 4 pkt 15 RODO oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia, zaliczane są do grupy tzw. danych wrażliwych, sensytywnych, wskazanych w art. 9 RODO. Przetwarzające je podmioty muszą zapewnić wyższy standard w zakresie ich ochrony (np. w przypadku przetwarzania na większą skalę, obowiązkowo powołać inspektora ochrony danych).

74. W drugą stronę, dokumentacja medyczna może zawierać informacje o faktycznym działaniu wyrobów medycznych, których to udostępnianie dostawcom technologii medycznych (w postaci anonimowej) mogłoby służyć ulepszeniom wyrobów medycznych z korzyścią dla pacjenta.

Dodatkowe wymogi regulacyjne związane z ochroną danych medycznych wynikają m.in. z zasad prowadzenia dokumentacji medycznej oraz przetwarzania jednostkowych danych medycznych. Tylko tytułem przykładu, sam § 1 ust. 5 DokMedR wskazuje, że zabezpieczenie dokumentacji wymaga w szczególności:

- a) systematycznego szacowania ryzyka zagrożeń oraz zarządzania tym ryzykiem;
- b) opracowania i stosowania udokumentowanych procedur zabezpieczania dokumentacji i systemów ich przetwarzania, w tym procedur dostępu oraz przechowywania;
- c) stosowania środków bezpieczeństwa adekwatnych do zagrożeń, uwzględniających najnowszy stan wiedzy;
- d) dbałości o aktualizację oprogramowania;
- e) bieżącego kontrolowania funkcjonowania organizacyjnych i techniczno-informatycznych sposobów zabezpieczenia, a także okresowego dokonywania oceny skuteczności tych sposobów;
- f) przygotowania i realizacji planów przechowywania dokumentacji w długim czasie, w tym jej przenoszenia na informatyczne nośniki danych i do nowych formatów danych, jeżeli tego wymaga zapewnienie ciągłości dostępu do dokumentacji.

Co więcej, część podmiotów leczniczych - jako operatorzy usług kluczowych - musi dodatkowo spełniać wymogi przewidziane przez KrSystCyberU, a więc m.in. wdrożyć system zarządzania bezpieczeństwem w systemie IT.

Pomimo szeregu wymogów związanych z ochroną danych medycznych, dostępne badania wskazują, że nie są one egzekwowane w zadawalającym stopniu. Opublikowane w 2019 r. przez NIK wyniki kontroli wykazały, że w ponad połowie skontrolowanych szpitali doszło do naruszeń ochrony danych osobowych, z czego w sześciu sytuacja była na tyle poważna, że konieczne było powiadomienie Prezesa Urzędu Ochrony Danych Osobowych<sup>75</sup>. Także bardziej aktualne dane wskazują na duże potrzeby w tym zakresie – jak wynika z analizy Centrum e-Zdrowia, w ponad połowie podmiotów zidentyfikowano potrzeby w zakresie cyberbezpieczeństwa (55,9%), przy czym najczęściej zgłaszały je szpitale (86,1%). Wskazywane potrzeby badanych placówek w zakresie cyberbezpieczeństwa to przede wszystkim odporność na cyberataki (68,9%), zwiększenie ochrony danych osobowych (65,9%) oraz poprawa stanu wiedzy o zagrożeniach informatycznych wśród pracowników/kierownictwa jednostki (59,4%)<sup>76</sup>.

75. <https://www.nik.gov.pl/aktualnosci/rodo-w-szpitalu.html>

76. [https://cez.gov.pl/sites/default/files/2022-09/Raport%20CeZ\\_2022.pdf](https://cez.gov.pl/sites/default/files/2022-09/Raport%20CeZ_2022.pdf)



Jak wynika z Programu rozwoju e-zdrowia w Polsce do 2027 r., obszar bezpieczeństwa ma być jednym z pięciu głównych obszarów zmian. Głównym działaniem w tym zakresie w perspektywie krótkoterminowej ma być powołanie w ramach Centrum e-Zdrowia Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT). Jego głównym zadaniem będzie zapobieganie wystąpieniu incydentów, a w przypadku ich wystąpienia – reakcja i obsługa. Kolejnym działaniem będzie rozbudowa systemu bezpieczeństwa dwóch kluczowych pod względem teleinformatycznym instytucji systemu ochrony zdrowia: CeZ i NFZ. Przywołany dokument przewiduje także wsparcie organizacyjne operatorów usług kluczowych sektora ochrony zdrowia powoływanych zgodnie z KrSystCyberU, a także podnoszenie świadomości cyfrowej osób zarządzających w jednostkach ochrony zdrowia.

W kontekście pracy lekarzy kluczowe jest to, że zapewniony ma być dostęp do regularnych szkoleń w zakresie pożądanых zachowań i polityk cyberbezpieczeństwa oraz ochrony danych osobowych. Obowiązkowe szkolenia mają się odbywać minimum raz w roku, w formie e-learningu lub prezentacji. Mają być przy tym udokumentowane i prowadzone w formule podobnej do szkoleń BHP (coroczny test).

W temacie bezpieczeństwa należy zwrócić uwagę, że dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) wyznaczać będzie nowy standard w zakresie cyberbezpieczeństwa. Polska, podobnie jak inne kraje członkowskie, ma czas do dnia 17 października 2024 r. by dostosować do niej krajowe regulacje.

Warto też zauważyć, że Prezes UODO w 11 grudnia 2023 r. zatwierdził „Kodeksu postępowania dla sektora ochrony zdrowia”. Jest to drugi kodeks postępowania wydany na podstawie art. 40 RODO dla sektora ochrony zdrowia, pierwszy, do którego mogą przystępować także podmioty publiczne<sup>77</sup>.

77. <https://uodo.gov.pl/pl/138/2929>



## Możliwe działania

Systematyczne podnoszenie lub stałe, bieżące utrzymywanie odpowiednio wysokiego poziomu ochrony danych medycznych wymaga szeregu działań o różnym charakterze. Zasadnicza część z nich została już zaadresowana w Programie rozwoju e-zdrowia w Polsce do 2027 r. i wymaga skutecznego wdrożenia. Pod kątem systemowym niezmiernie ważne jest także wypracowanie krajowej implementacji dyrektywy NIS 2 w konsultacji ze środowiskiem medycznym, by nowe wymogi mogły być skutecznie wdrożone przez podmioty wykonujące działalność leczniczą zobowiązane do jej stosowania.

Wsparciem dla wielu podmiotów wykonujących działalność leczniczą będzie też określenie możliwie jasnych wymogów związanych z cyberbezpieczeństwem. W tym celu możliwe jest dalsze rozwinięcie oraz doprecyzowanie przepisów wykonawczych o minimalne, techniczne standardy ochrony jednostkowych danych medycznych oraz dokumentacji medycznej. Uzupelniająco lub alternatywnie można też przyjąć opracowane przez ekspertów i autoryzowane przez stronę publiczną wytyczne i rekomendacje w tym zakresie, które ustanawiać będą podobne wymogi w formie tzw. miękkiego prawa. Przykładem mogą być rekomendacje w zakresie cyberbezpieczeństwa w ochronie zdrowia opublikowane przez Centrum e-Zdrowia<sup>78</sup>. Dokumenty o takim charakterze powinny być cyklicznie przeglądane i aktualizowane, jako że dynamika zmian w tym obszarze jest bardzo duża.

Niezależnie od tych działań, zasadne jest także kontynuowanie programów wsparcia finansowego dla podmiotów wykonujących działalność leczniczą, które byłyby dedykowane zakupom towarów i usług związanych z ochroną danych medycznych. Niski poziom ochrony danych wynika czasem z – wynikających z przyczyn finansowych – braków w sprzęcie i oprogramowaniu, które spełniałoby aktualne standardy cyberbezpieczeństwa.



## Uzasadnienie

Działający z należytą starannością lekarz powinien być świadomy roli bezpieczeństwa danych medycznych. Powinien znać podstawowe wymogi z tym związane, kluczowe ryzyka i zagrożenia oraz potrafić postępować zgodnie z przyjętymi w placówce medycznej zasadami działania. Lekarz musi znać w szczególności dane kontaktowe do inspektora ochrony danych zatrudnionego w podmiocie leczniczym i wiedzieć, jakie sprawy powinien do niego zgłaszać. Choć w przypadku podmiotów leczniczych główny ciężar zapewnienia bezpieczeństwa danych nałożony został właśnie na nie, a nie na zatrudniany przez nie personel medyczny, lekarz powinien mieć na uwadze kwestie bezpieczeństwa i umieć reagować, jeżeli w jego ocenie dochodzi do nieprawidłowości. Dla bezpieczeństwa danych istotne jest również poszerzanie świadomości społecznej na temat technologii AI, w szczególności rozwiązań ocenianych przez Komisję Europejską jako systemy „wysokiego ryzyka”.

Propozycja wpisuje się w postulat dotyczący bezpieczeństwa - lekarz powinien mieć dostęp do narzędzi, które zapewniają bezpieczeństwo korzystania z danych. Jest to podstawowy i niezbędny warunek przetwarzania tak wrażliwych danych, jak dane o stanie zdrowia.



### 5.3.2.2 Budowanie świadomości po stronie pacjentów

**Stan obecny.** Wymogi regulacyjne związane z ochroną danych medycznych adresowane są jedynie do podmiotów wykonujących działalność leczniczą i personelu medycznego. Tymczasem bezpieczeństwo danych zależy także od zapewnienia odpowiednich zabezpieczeń po stronie pacjenta. Część ataków hakerskich bazuje na kradzieży tożsamości w celu podszycia się pod pacjenta i uzyskaniu jego danych lub ataku na dane, które już zostały przesłane do systemu pacjenta. Nawet najlepsze zabezpieczenia po stronie podmiotów wykonujących działalność leczniczą mogą nie być wystarczające, jeżeli celem ataku będzie pacjent i wykorzystywane przez niego narzędzia cyfrowe.



#### Perspektywa zmian

Programu rozwoju e-zdrowia w Polsce do 2027 r. zakłada, że zostanie przygotowany przewodnik pacjenta po świecie e-zdrowia i inne materiały edukacyjne, a także organizowane będą dedykowane szkolenia, które pomogą pacjentowi bezpiecznie korzystać z rozwiązań z zakresu e-zdrowia. Charakter i dokładniejszy zakres zapowiadanych materiałów i szkoleń nie jest jednak znany.



#### Możliwe działania

Aktywności edukacyjne skierowane do pacjenta i przewidziane w Programie rozwoju e-zdrowia w Polsce do 2027 r. powinny zawierać komponent dotyczący podstawowych zasad z zakresu cyberbezpieczeństwa. Warto także uzupełnić je o kampanię informacyjną, która promować będzie korzystanie z bezpiecznych narzędzi przy korzystaniu z teleporad, logowaniu się na IKP lub inne serwisy, w tym konta pocztowe, w których dostępne są dane o stanie zdrowia. Także lekarze powinni mieć świadomość tych zagrożeń i zwracać na nie uwagę pacjentów.



#### Uzasadnienie

Wysoki poziom ochrony danych medycznych zależy od wszystkich uczestników systemu e-zdrowia, w tym pacjentów. O ile przepisy prawa nie nakładają na nich określonych obowiązków w tym zakresie, warto edukować i promować wśród pacjentów wiedzę z zakresu cyberbezpieczeństwa. Warto, by także lekarze zwracali na to pacjentom uwagę i potrafili udzielić podstawowych wskazówek. Ewentualne naruszenia występujące z winy pacjenta lub wskutek ataku na system pacjenta podważać mogą zaufanie pacjenta do całego systemu e-zdrowia, zniechęcając do korzystania z wielu co bardziej innowacyjnych rozwiązań.

Propozycja wpisuje się w postulat dotyczący bezpieczeństwa - lekarz powinien mieć dostęp do narzędzi, które zapewniają bezpieczeństwo korzystania z danych. W środowisku cyfrowym ochrona danych zależy od działania wszystkich użytkowników, w tym pacjentów.

### 5.3.3 Narzędzia wykorzystywane do przetwarzania danych medycznych

Jednym z czynników bezpieczeństwa danych jest wykorzystywanie do ich przetwarzania narzędzi, które spełniają podstawowe standardy. Ich dobór wpływa także na różne możliwości wykorzystania danych.

#### 5.3.3.1 Chmura obliczeniowa

**Stan obecny.** Zgodnie z art. 23 ust. 5 PrPacjU, podmiot udzielający świadczeń zdrowotnych może zawierać umowy o powierzeniu przetwarzania danych osobowych, o których mowa w art. 28 ust. 3 RODO. Realizacja tej umowy nie może jednak powodować zakłócenia udzielania świadczeń zdrowotnych, w szczególności w zakresie zapewnienia, bez zbędnej zwłoki, dostępu do danych zawartych w dokumentacji medycznej. Regulacja ta (pierwotnie w nieco innym brzmieniu) została przyjęta w 2015 r. w celu doprecyzowania zasad tzw. outsourcingu przetwarzania danych medycznych. Jednym z celów dokonanej wówczas nowelizacji było wyraźne dopuszczenie możliwości korzystania z zewnętrznych serwerów do przetwarzania dokumentacji medycznej przez podmioty udzielające świadczeń zdrowotnych, w tym wykorzystywania narzędzi i rozwiązań opartych o technologię tzw. chmury obliczeniowej.

Zasadnicza wątpliwość co do takiej możliwości obejmuje podmioty lecznicze dla osób pozbawionych wolności, podmioty lecznicze utworzone przez ministra właściwego do spraw wewnętrznych lub Ministra Obrony Narodowej. W ich przypadku przepisy wykonawcze wydane przez poszczególnych ministrów<sup>79</sup> zawierają wymóg, by dokumentację indywidualną wewnętrzną oraz dokumentację zbiorczą wewnętrzną przechowywać „w podmiocie”, w którym została sporządzona (w przypadku pozostałych placówek ten wymóg został sformułowany inaczej – dokumentacja wewnętrzna ma być przechowywana „przez podmiot”, który ją sporządził).



#### Perspektywa zmian

Mając na uwadze dynamiczny wzrost ilości dokumentacji medycznej prowadzonej w postaci elektronicznej, a także dość ograniczoną skalowalność własnych serwerowni podmiotów leczniczych, dużego znaczenia w ochronie zdrowia nabrało wykorzystywanie chmury obliczeniowej. Program rozwoju e-zdrowia w Polsce do 2027 r. co prawda nie odnosi się wprost do chmury, ale przewiduje np., że powstanie HUB pośredniczący w wymianie zleceń na usługi, wyników oraz komunikacji pomiędzy interesariuszami, który zapewni przepływ informacji. Wraz z HUBem powstać ma repozytorium danych medycznych i EDM. Niewykluczone, że rozwiązania te oparte będą o chmurę.

79. Rozporządzenie Ministra Sprawiedliwości z dnia 12 lipca 2022 r. w sprawie dokumentacji medycznej prowadzonej w podmiotach leczniczych dla osób pozbawionych wolności (Dz. U. poz. 1659).; Rozporządzenie Ministra Obrony Narodowej z dnia 6 sierpnia 2021 r. w sprawie rodzajów, zakresu i wzorów oraz sposobu przetwarzania dokumentacji medycznej w podmiotach leczniczych utworzonych przez Ministra Obrony Narodowej (Dz. U. poz. 1825 z późn. zm.); Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów oraz sposobu przetwarzania dokumentacji medycznej w podmiotach leczniczych utworzonych przez ministra właściwego do spraw wewnętrznych (t.j. Dz. U. z 2022 r. poz. 1957).



## Możliwe działania

Mając na uwadze obecne regulacje, zasadne jest doprecyzowanie wymogów związanych z zawieraniem umów o powierzenie przetwarzania danych osobowych, które zawierają jedynie dość ogólnie sformułowane przesłanki (konieczność zapewnienia, bez zbędnej zwłoki, dostępu do danych zawartych w dokumentacji medycznej). Jednocześnie też dotychczasowa praktyka wskazuje, że może to nastąpić w formie rekomendacji lub wytycznych (wydanych np. przez Centrum e-Zdrowia), a nie zmian prawnych. Dzięki temu stanie się jasne, jaki jest pożądanym, aktualny standard w tym zakresie.

Ponadto, warto ujednoczyć regulacje dotyczące zasad przechowywania dokumentacji medycznej przez różne podmioty lecznicze, niezależnie od podmiotu, który je utworzył. Nie wyklucza to możliwości wprowadzenia wyższych standardów co do bezpieczeństwa usługi np. dla placówek wojskowych.



## Uzasadnienie

Chmura obliczeniowa jest rozwiązaniem umożliwiającym – w zależności od warunków konkretnej usługi – tańsze i bezpieczniejsze przetwarzanie dużych zbiorów danych niż prowadzenie w tym celu jedynie własnej serwerowni. Tym samym dostęp do niej powinna mieć jak najszersza grupa podmiotów leczniczych. Popularyzacji chmury sprzyjać będą też zmiany wprowadzane przez EHDS, które zakładają większą interoperacyjność danych, a więc jeszcze łatwiejsze przenoszenie danych do i pomiędzy chmurami. To zaś przekłada się na większą dostępność tych danych dla lekarza.

Propozycja wpisuje się w postulat dotyczący zapewnienia funkcjonalnego wykorzystywania danych – lekarz powinien móc sprawnie korzystać z różnych danych, a także aplikacji i programów, które pomogą mu zebrać, przeanalizować oraz wykorzystać dane w procesie opieki nad pacjentem. Taki stan rzeczy może zapewnić wykorzystanie środowiska chmury obliczeniowej.

### 5.3.3.2 Aplikacje, komunikatory i inne podobne rozwiązania

**Stan obecny.** W codziennej praktyce lekarze wykorzystują różne narzędzia, w których mogą być przetwarzane dane medyczne. Mają one różne postacie i funkcje, mogą służyć do komunikacji z pacjentem, zapisywania jego danych, dzielenia się wynikami badań z innymi lekarzami itp. Z tego typu rozwiązań można korzystać tak długo, jak długo spełniają one wymagania regulacyjne niezbędne do przetwarzania danych medycznych. Jak zostało to zauważone w poprzednim podpunkcie, podstawowym warunkiem outsourcingu danych medycznych jest zawarcie umowy o powierzeniu przetwarzania danych osobowych, o której mowa w art. 28 ust. 3 RODO. Należy przy tym pamiętać, że dane medyczne podlegają szczególnej ochronie na mocy PrPacjU. Nie mogą być wykorzystywane przez dostawców różnego rodzaju aplikacji i komunikatorów – bez zgody pacjenta – w jakimkolwiek innym celu, np. prowadzenia działań marketingowych. Oznacza to, że część dostępnych i bardzo popularnych narzędzi, np. media społecznościowe czy bezpłatne komunikatory internetowe, może nie spełniać tych wymogów, a zatem nie powinna być wykorzystywana w celach sprawowania opieki nad pacjentem lub wysyłania jego dokumentacji medycznej.



## Perspektywa zmian

Jak można się spodziewać, podobnych rozwiązań, które potencjalnie będą mogły być stosowane w ochronie zdrowia, będzie coraz więcej. EHDS wprowadza nowe zasady i pojęcia, np. pojęcie aplikacji wspierających dobrostan, która oznacza każde urządzenie lub oprogramowanie przewidziane przez producenta do używania przez osobę fizyczną do przetwarzania elektronicznych danych dotyczących zdrowia do celów innych niż opieka zdrowotna, takich jak dobrostan i prowadzenie zdrowego stylu życia. Może więc rosnąć niepewność po stronie lekarzy i innych profesjonalistów medycznych, których z nich można bezpiecznie używać, a których unikać.



## Możliwe działania

Dane medyczne mogą być przetwarzane w aplikacjach, komunikatorach i innych podobnych rozwiązaniach, nawet tych, które nie są adresowane do wykorzystania klinicznego. Dobór właściwego narzędzia należy do lekarza. Aby mu to ułatwić, zasadne jest przyjęcie wytycznych dotyczących dopuszczalności stosowania różnych narzędzi przetwarzania danych i warunków, jakie muszą być przez nie spełniane, by lekarz mógł je wykorzystać w opiece nad pacjentem. Wytyczne powinny umożliwić mu łatwe sprawdzenie, czy dane rozwiązanie spełnia wymagany standard.

W związku z powyższym warto też wprowadzić system walidacji podobnych rozwiązań przez stronę publiczną pod kątem zastosowania w ochronie zdrowia opierający się o badania naukowe, w tym w szczególności badania kliniczne. Narzędzia, które przejdą pozytywnie weryfikację powinny być wyróżnione np. przez dedykowane certyfikaty, co będzie stanowić dla lekarza jasną wskazówkę w zakresie możliwości wykorzystania konkretnego rozwiązania przy postępowaniu z pacjentem. Kierunkowym przykładem podobnego systemu może być już funkcjonujący w Polsce Portfel Aplikacji Zdrowotnych (PAZ). Warto przy tym zweryfikować dotychczasowe doświadczenia z działania PAZ i na ich podstawie zaprojektować nowy system.



## Uzasadnienie

Przyjęcie podobnych wytycznych byłoby dodatkowym ułatwieniem dla lekarza przy wyborze cyfrowych narzędzi wykorzystywanych do przetwarzania danych pacjenta. Dzięki temu dodatkowo wzrośnie poziom bezpieczeństwa przetwarzanych danych.

Propozycja wpisuje się w postulat dotyczący zapewnienia funkcjonalnego wykorzystywania danych - lekarz powinien móc sprawnie korzystać z różnych danych, a także aplikacji i programów, które pomogą mu zebrać, przeanalizować oraz wykorzystać dane w procesie opieki nad pacjentem. Należy przy tym pamiętać o korzystaniu jedynie z rozwiązań spełniających wymagane standardy.

### 5.3.3.3 Sztuczna inteligencja

**Stan obecny.** W praktyce funkcjonowania wielu podmiotów leczniczych w Polsce i na świecie rośnie skala wykorzystywania oraz rola narzędzi opartych o sztuczną inteligencję. Badania przeprowadzone przez Centrum e-Zdrowia wskazują, że stosowanie rozwiązań AI zadeklarowało 2,5% ankietowanych placówek medycznych, tj. o 1,4 punktu procentowego więcej biorąc pod uwagę wyniki poprzedniego badania z 2021 r. Najczęściej wykorzystywane są rozwiązania mające zastosowanie w diagnostyce obrazowej typu CT (tomografia komputerowa) – 39,4% oraz w procesie wyszukiwania, gromadzenia, przechowywania i standaryzacji danych medycznych – 22,6%. Jednocześnie 5,4% zbadanych podmiotów zadeklarowało plan rozpoczęcia wykorzystywania narzędzi opartych o AI w najbliższym roku<sup>80</sup>. Jak można zakładać, tendencja ta będzie utrzymywać się w kolejnych latach.

W obecnym stanie prawnym wciąż brakuje dedykowanych regulacji dotyczących stosowania AI w ochronie zdrowia, w tym jasnych zasad jej stosowania w opiece nad pacjentem oraz podziału odpowiedzialności. Podstawowe pytania i wątpliwości w tym zakresie, a także sugerowane rozwiązania zawiera opublikowana w 2022 r. Biła księga AI w praktyce klinicznej<sup>81</sup>.



#### Perspektywa zmian

Prace nad uregulowaniem AI prowadzone są przede wszystkim na poziomie UE. Procedowane są obecnie dwa podstawowe akty prawne w tym zakresie: rozporządzenie ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze unii oraz dyrektywa w sprawie dostosowania przepisów dotyczących pozaumownej odpowiedzialności cywilnej do sztucznej inteligencji (dyrektywa w sprawie odpowiedzialności za sztuczną inteligencję).

Program rozwoju e-zdrowia w Polsce do 2027 r. wskazuje, że będą prowadzone prace nad budową modeli sztucznej inteligencji, możliwych do zastosowania oraz polityką udostępniania danych dla sektora badań i rozwoju. Na poziomie centralnym mają być tworzone i trenowane modele do predykcji zdrowia pacjenta. Powstaną też zasady oceny skuteczności i bezpieczeństwa rozwiązań m-Zdrowia i AI badające skuteczność, bezpieczeństwo i efektywność<sup>82</sup>.

Warto też zwrócić uwagę na Krajowy Plan Odbudowy i Rozwoju (KPO), który przewiduje, że już w pierwszym kwartale 2026 r. 30% podmiotów leczniczych o znaczeniu ogólnokrajowym lub regionalnym podłączonych do centralnego elektronicznego repozytorium danych medycznych, będzie wyposażonych w narzędzie wspomaganie podejmowania decyzji oparte na sztucznej inteligencji<sup>83</sup>.

80. VI Edycja „Badania stopnia informatyzacji podmiotów wykonujących działalność leczniczą”, Centrum e-Zdrowia, wrzesień 2022; s. 40-42, 77

81. Biła Księga AI w praktyce klinicznej - Stosowanie sztucznej inteligencji przy udzielaniu świadczeń zdrowotnych; Warszawa 2022 r.

82. Program rozwoju e-zdrowia w Polsce do 2027 r.; str. 34

83. Krajowy Plan Odbudowy i Zwiększania Odporności; str. 287



## Możliwe działania

Podstawowe regulacje dotyczące AI przyjmowane będą na poziomie unijnym. Nie stoi to jednak na przeszkodzie, aby już dziś zaadresować podstawowe pytania i wątpliwości związane ze stosowaniem AI w ochronie zdrowia w formie wytycznych i rekomendacji. Dotyczy to także kwestii wykorzystywania danych medycznych na potrzeby rozwoju AI, bez których technologia ta nie będzie mogła dalej szybko i skutecznie się rozwijać. Obok działań o takim charakterze postulować należy akcje podnoszenia świadomości wśród lekarzy i pacjentów o korzyściach wynikających z wykorzystywania AI w ochronie zdrowia oraz związanych z tym szansach, wyzwaniach i zagrożeniach.

Możliwym do wprowadzenia działaniem jest także oznaczanie w dedykowany sposób zbiorów danych i rekomendacji generowanych przez systemy AI. Po pierwsze, będzie to cenna wskazówka dla lekarza dotycząca charakteru danych (wynik interpretacji algorytmów). Po drugie, dzięki temu łatwiejsze stanie się prowadzenie badań nad skutecznością systemów AI w ochronie zdrowia. Dzięki temu może stać się możliwe wdrożenie systemu, w którym wyniki generowane przez AI miałyby pod kątem prawnym szczególny status wpływający na odpowiedzialność lekarza, który bazowałby na nich przy dalszym postępowaniu z pacjentem.



## Uzasadnienie

Sztuczna inteligencja jest w stanie znacząco ułatwić pracę lekarzy. Narzędzia oparte o AI już dziś świetnie sprawdzają się np. przy analizach ustrukturyzowanych zbiorów danych, pozwalając na oszczędność czasu profesjonalisty medycznego. Nie zastępują lekarza, ale - jak każde inne narzędzie odpowiednio zastosowane - podnoszą jakość jego pracy. Z uwagi na ich innowacyjny charakter oraz brak dedykowanych regulacji lekarze powinni mieć jasne wytyczne, jak powinni z nimi postępować, a także nie obawiać się ich wykorzystywania z obawy o zarzut naruszenia prawa lub irracjonalnego lęku przed bliżej nieokreślonym zagrożeniem ze strony AI. Tym samym za jasnymi zasadami powinny iść w parze działania edukacyjne.

Systemy AI są wciąż rozwijane i doskonalone. Mogą stanowić wsparcie dla lekarza, który dalej ponosi odpowiedzialność za postępowanie z pacjentem. Jeżeli w najbliższej przyszłości badania kliniczne wykażą bardzo wysoką jakość i skuteczność poszczególnych systemów AI w ochronie zdrowia, zasadne może być rozważenie uregulowania zasad odpowiedzialności związanej z ich stosowaniem, tak by lekarz miał jasność co do tego, w jakim zakresie może bazować na generowanych przez AI wynikach, bez konieczności ich dodatkowej, nadmiernej weryfikacji, tak jak obecnie bazuje na wynikach generowanych przez zaawansowane wyroby medyczne, które nie stanowią AI.

Propozycja wpisuje się w postulat dotyczący zapewnienia funkcjonalnego wykorzystywania danych - lekarz powinien móc sprawnie korzystać z różnych danych, a także aplikacji i programów, które pomogą mu zebrać, przeanalizować oraz wykorzystać dane w procesie opieki nad pacjentem. W tym zakresie bardzo duże możliwości stwarza już teraz wykorzystanie sztucznej inteligencji, a jak można się spodziewać, jej możliwości na przestrzeni najbliższych lat będą stale rosnąć.

### 5.3.4 Jakość danych - jakość leczenia

Pod kątem wykorzystywania danych w codziennej praktyce należy zwrócić uwagę na ich jakość. Nawet łatwy i pełny dostęp do danych w bezpiecznych warunkach może okazać się niepotrzebny, jeżeli dane nie będą przedstawiać wartości klinicznej i lekarz nie będzie widział korzyści z ich wykorzystania. Od jakości danych zależy też jakość bazujących na nich badań naukowych i prac badawczo-rozwojowych.

#### 5.3.4.1 Premiowanie wysokiej jakości danych

**Stan obecny.** W pierwszej kolejności należy zaznaczyć, że pojęcie „jakości danych” może być różnie rozumiane. W literaturze sformułowano szereg definicji tego pojęcia, które różnią się w zależności od kontekstu wykorzystania danych i dyscypliny naukowej. Na potrzeby raportu przyjmujemy uproszone podejście, w świetle którego dane medyczne zapewniają jakość, jeżeli są one wartościowe dla potencjalnych celów ich pierwotnego i wtórnego przetwarzania, tj. są łatwo dostępne i stanowią wsparcie dla lekarza, który opiekuje się pacjentem, lub mogą być z powodzeniem wykorzystane w pracach naukowych lub badawczo-rozwojowych. Tym samym jakościowe dane medyczne powinny być wiarygodne, aktualne i kompletne, a także dostępne i porównywalne, a więc prowadzone w formie nadającej się do ich łatwego odszukania, transferu i wykorzystania.

W świetle obecnie obowiązujących przepisów prawa podmioty wykonujące działalność leczniczą zasadniczo nie są w żaden sposób premiowane za prowadzenie dokumentacji medycznej w sposób zapewniający – rozumianą w powyższy sposób - wysoką jakość gromadzonych danych oraz ich terminowe raportowanie. Wskazać można tylko szątkowe rozwiązania, które premiowałyby działania na rzecz wysokiej jakości przetwarzanych danych medycznych, np. ustanowiony w obwieszczeniu w sprawie standardów akredytacyjnych w zakresie udzielania świadczeń zdrowotnych oraz funkcjonowania podmiotów leczniczych wykonujących inwazyjne procedury zabiegowe i operacyjne mechanizm, polegający na punktowaniu w procesie akredytacji zapewnienia interoperacyjności systemów informatycznych podmiotu leczniczego jako kryterium podlegające ocenie w procedurze akredytacyjnej<sup>84</sup>.

Jednym z aspektów jakości danych jest ich interoperacyjność. Zagadnienie to z uwagi na jego szczególne znaczenie zostanie szerzej przedstawione w dalszym podpunkcie raportu.

84. System informatyczny powinien zapewniać interoperacyjność – umożliwić współpracę z: wieloma systemami medycznymi, innymi bazami danych, zapewnić przekazywanie komunikatów medycznych do zewnętrznych systemów informatycznych. System powinien pozwalać na analizy przekrojowe, z wykorzystaniem danych z innych systemów informatycznych podmiotu.



## Perspektywa zmian

Na poziomie JakZdrU, jak wskazuje już sam tytuł tego aktu, promować ma jakość. Przepisy tej ustawy nie wskazują jednak na ten moment dokładnie, jakie będą kryteria owej jakości – stosunkowo duża część szczegółowych regulacji pozostała do dookreślenia na poziomie przepisów wykonawczych. Potencjalnie mogą one obejmować więc także jakość prowadzonej dokumentacji medycznej i przetwarzanych danych medycznych.

No poziomie unijnym kluczowe w tym zakresie będą regulacje EHDS. Jak wskazano w motywie 20. preambuły tego aktu, aby przyczynić się do wysokiej jakości i ciągłości opieki zdrowotnej, niektóre kategorie danych dotyczących zdrowia należy rejestrować w formacie elektronicznym systematycznie i zgodnie z określonymi wymogami dotyczącymi jakości danych. Europejski format wymiany elektronicznej dokumentacji medycznej powinien stanowić podstawę specyfikacji związanych z rejestracją i wymianą elektronicznych danych dotyczących zdrowia. Komisja powinna posiadać uprawnienia do przyjęcia aktów wykonawczych w celu określenia dodatkowych aspektów związanych z rejestracją elektronicznych danych dotyczących zdrowia, takich jak kategorie świadczeniodawców, którzy mają rejestrować dane dotyczące zdrowia drogą elektroniczną, kategorie danych, które mają być rejestrowane drogą elektroniczną, lub wymogi dotyczące jakości danych. Podstawowym rozwiązaniem w tym zakresie ma być znak jakości i użyteczności danych, którym byłyby opatrywane zbiory danych, informowałby użytkowników danych o jakości i cechach użytkowych zbioru danych oraz umożliwiałby im wybór zbiorów danych, które najlepiej odpowiadają ich potrzebom.



## Możliwe działania

W pierwszej kolejności uzasadnione jest wypracowanie kryteriów jakości danych medycznych uwzględniających ich kluczowe cechy takie jak wiarygodność, aktualność, kompletność i interoperacyjność oraz włączenie ich do systemu jakości wynikającego z JakZdrU, np. jako element fakultatywnego systemu akredytacji. Dzięki temu rozwiązaniu podmioty wykonujące działalność leczniczą będą miały motywację finansową do starannego utrwalania danych w pożądanym formatach oraz ich terminowego sprawozdawania.

Rozwiązaniem sprzyjającym jakości i bezpieczeństwu danych będzie także wypracowanie w gronie ekspertów co najmniej ramowego standardu zarządzania danymi, który powinien być stosowany we wszystkich podmiotach wykonujących działalność leczniczą (adekwatnie do zakresu udzielanych świadczeń i struktury organizacyjnej). Podstawowe elementy standardu mogą zostać wyznaczone na poziomie regulacji prawnych, np. w formie rozporządzenia wydanego do postulowanej ustawy o danych medycznych. Standard powinien być punktem odniesienia i wsparciem w procesie opracowywania procedur wewnętrznych i polityki ochrony danych na poziomie poszczególnych podmiotów. Ważne jest bowiem systemowe podejście do obszaru gromadzenia i postępowania z danymi medycznych pod kątem pierwotnych i wtórnych celów ich przetwarzania, które będzie co najmniej w podstawowym zakresie spójne dla wszystkich podmiotów leczniczych. Ważne jest



przy tym budowanie świadomości osób zarządzających podmiotami leczniczymi w tym obszarze oraz dzielenie dobrymi przykładami. Podobne rozwiązania są już wymagane przez prawodawcę, np. § 1 ust. 5 pkt 6 DokMedR obliguje do przygotowania i realizacji planów przechowywania dokumentacji w długim czasie, w tym jej przenoszenia na informatyczne nośniki danych i do nowych formatów danych, jeżeli tego wymaga zapewnienie ciągłości dostępu do dokumentacji.

Działanie takie wpisuje się w postulowane w Programie rozwoju e-zdrowia w Polsce do 2027 r. stworzenie ram dla zarządzania danymi zdrowotnymi<sup>85</sup>. Obecnie każda placówka w pełni samodzielnie przyjmuje tego rodzaju dokumenty, przez co ich jakość i zakres różnią się między sobą, co dodatkowo komplikuje współpracę przy wymianie danych pomiędzy placówkami. Wspólny standard zapewniający spójność kluczowych elementów systemu obiegu danych oraz dający jasne wytyczne jak powinno się opracowywać tego rodzaju procedury powinien przetożyć się na rewizję dotychczasowej praktyki i większą staranność przy jej dostosowywaniu do nowych wymogów wynikających m.in. z EHDS.

W dalszej perspektywie czasowej szczegółowe wymogi dotyczące jakości danych i nowy system znakowania jakości i użyteczności danych wynikać będą z regulacji unijnych. Już obecnie można jednak dookreślić takie wymogi na poziomie krajowym oraz wprowadzić podobny system znakowania np. w ramach programu pilotażowego, by zawczasu przygotować się do wdrożenia nowych rozwiązań, które dzięki temu będą mogły być potencjalnie szybciej i sprawniej zaadaptowane.

Przy opracowywaniu ram jakości i użyteczności danych należy wziąć pod uwagę oczekiwania zawarte w akcie w sprawie sztucznej inteligencji i jego odpowiedniej dokumentacji określonej w załącznikach. AI Act wyodrębnia bowiem różne zbiory danych – zbiory danych treningowych, walidacyjnych i testowych, które muszą spełniać określone wymogi, by mogły być wykorzystywane na potrzeby rozwoju AI. Brak spełnienia tych wymogów oznacza, że określone zbiory danych mogą okazać się niedopuszczalne pod kątem wykorzystania przez AI.



### Uzasadnienie

Od jakości gromadzonych danych zależy jakość opieki sprawowanej nad pacjentem – czy to bezpośrednio przez lekarza, który na podstawie m.in. tych danych podejmuje decyzje, czy pośrednio, przez rozwiązania oparte np. o AI, które uczą się na danych i wykorzystują je do realizacji powierzonych im zadań. Jak trafnie wskazuje motyw 59. EHDS, poprawa jakości i użyteczności zbiorów danych dzięki umożliwieniu klientom świadomego wyboru oraz poprzez harmonizację powiązanych wymogów na szczeblu unijnym, z uwzględnieniem istniejących norm unijnych i międzynarodowych, wytycznych, zaleceń dotyczących gromadzenia i wymiany danych (tj. zasad FAIR: możliwe do znalezienia (Findable), dostępne (Accessible), interoperacyjne (Interoperable), nadające się do ponownego wykorzystania (Re-usable), przynosi korzyści również posiadaczom danych, lekarzom i innym pracownikom systemu zdrowia, osobom fizycznym i całej gospodarce Unii Europejskiej.

85. Program rozwoju e-zdrowia w Polsce do 2027 r.; str. 33.

Propozycja wpisuje się w postulat dotyczący zapewnienia funkcjonalnego wykorzystywania danych - lekarz powinien móc sprawnie korzystać z różnych danych, a także aplikacji i programów, które pomogą mu zebrać, przeanalizować oraz wykorzystać dane w procesie opieki nad pacjentem. Dane będą nadawać się wykorzystania tylko pod warunkiem zapewnienia ich jakości.

#### 5.3.4.2 Rozwój systemu rejestrów medycznych

**Stan obecny.** Systemowe zbieranie danych medycznych, których struktura i dostępność może być ustalona na transparentnych, konsultowanych publicznie zasadach, była dotąd możliwa głównie dzięki wykorzystaniu rejestrów medycznych. Rejestry te mogą być tworzone bezpośrednio na podstawie ustawy lub poprzez rozporządzenia ministra zdrowia.

Rejestry „ustawowe” mają przede wszystkim charakter ewidencyjny, są to m.in. Centralny Wykaz Usługobiorców czy Centralny Wykaz Usługodawców. Pod kątem pracy lekarza kluczowe są rejestry tworzone w drodze rozporządzeń, które gromadzą dane kliniczne. Utworzenie takiego rejestru może nastąpić na wniosek podmiotów wykonujących działalność leczniczą, Narodowego Funduszu Zdrowia albo innych jednostek podległych lub nadzorowanych przez ministra właściwego do spraw zdrowia. Celem tworzenia rejestrów jest monitorowanie zapotrzebowania na świadczenia opieki zdrowotnej oraz stanu zdrowia usługobiorców, prowadzenie profilaktyki zdrowotnej lub realizacja programów zdrowotnych albo programów polityki zdrowotnej, oraz monitorowanie i ocena bezpieczeństwa, skuteczności, jakości i efektywności kosztowej badań diagnostycznych lub procedur medycznych.

Warto przy tym zauważyć, że problem z obecnie funkcjonującymi rejestrami polega m. in. na tym, że dane przesyłane do rejestru są przekazywane niezależnie od prowadzonej przez lekarza dokumentacji medycznej. Tym samym dochodzi do dublowania zbiorów danych kosztem dodatkowej pracy po stronie raportującej placówki.

Jak można zauważyć, rejestrów medycznych funkcjonuje stosunkowo niewiele. Ponadto kontrola NIK stwierdziła m.in. ograniczoną wymianę danych pomiędzy poszczególnymi rejestrami medycznymi lub nieporównywalność zawartych w nich danych, brak przepływu informacji o procesie leczenia i jego efektach oraz nierzetelność danych zawartych w niektórych rejestrach medycznych<sup>86</sup>. Generalnie więc system rejestrów nie pełni dobrze swej funkcji – nie zapewnia łatwo dostępnych, wysokiej jakości danych medycznych.

Obecny system rejestrów medycznych należy ocenić krytycznie. Brakuje jakichkolwiek danych świadczących o pozytywnym wpływie dotychczas prowadzonych rejestrów na jakość lub dostępność udzielanych świadczeń. Z reguły brak publicznie dostępnych raportów z obecnie działających rejestrów uniemożliwia ich pełną ocenę, co w świetle wyników kontroli NIK wskazuje, że system rejestrów nie działa prawidłowo.

86. <https://www.nik.gov.pl/aktualnosci/quo-vadis-sluzbo-zdrowia.html>

Warto też zauważyć, że zmiany technologiczne oraz postępy w budowanie systemu e-zdrowia mogą rodzić pytania o zasadność dalszego zbierania danych w formie rejestrów medycznych. Dzięki zapewnieniu możliwości dostępu oraz wspólnych standardów interoperacyjności odpowiednie dane mogą być sprawnie gromadzone bezpośrednio z podmiotów wykonujących działalność leczniczą. W pewnym uproszczeniu, wszystkie połączone w ten sposób systemy informatyczne w ochronie zdrowia tworzyć będą jeden wielki rozproszony rejestr.



### Perspektywa zmian

JakZdrU wprowadziła zmiany w zakresie systemu rejestrów medycznych, w szczególności poszerzyła zakres podmiotów, które mogą wystąpić z wnioskiem o utworzenie rejestru o towarzystwa naukowe oraz wprowadziła obowiązek publikowania określonych danych (o rozpoznaniu zgodnie z aktualnie obowiązującą Międzynarodową Klasyfikacją Chorób i Problemów Zdrowotnych, dotyczących przeprowadzonych badań diagnostycznych, dotyczących pacjenta: wykształcenie, wiek, płeć oraz przyczyna zgonu, a także na temat powikłań i wyników odległych, związanych z pogorszeniem jakości życia, bezpośrednio zagrażających życiu lub mogących prowadzić do zgonu pacjenta) oraz raportów zawierających analizę zapotrzebowania na świadczenia opieki zdrowotnej, stanu zdrowia usługobiorców, bezpieczeństwa, skuteczności, jakości i efektywności kosztowej badań diagnostycznych lub procedur medycznych, kompletności i jakości danych, które są przetwarzane w rejestrze medycznym, w podziale na usługodawców przekazujących dane do rejestru medycznego, a także ocenę efektów wynikających z wdrożenia rejestru medycznego, w tym wskazanie korzyści i zagrożeń związanych z prowadzeniem tego rejestru oraz ocenę funkcjonalności i spójności prowadzonego rejestru medycznego z innymi rejestrami publicznymi. O ile zmiana ta może okazać się korzystna, o tyle trudno się spodziewać, by istotnie wpłynęła na funkcjonowanie obecnego systemu rejestrów, w szczególności na powstawanie nowych rejestrów lub jakość i dostępność zawartych w nich danych.



### Możliwe działania

Wątpliwe jest, zakładane zmiany przetożą się na powstawanie nowych rejestrów oraz poprawę działania tych dotychczasowych. Zasadne jest powołanie specjalnej rady ds. rejestrów<sup>87</sup>, która wyznaczy strategiczny plan rozwoju systemu rejestrów medycznych (powołanie podobnej rady zawierała pierwotna wersja projektu ustawy o jakości w opiece zdrowotnej i bezpieczeństwie pacjenta). Tworzenie kolejnych rejestrów powinno się odbywać w uporządkowany sposób, zgodny z priorytetami polityki zdrowotnej.

W ramach dalszego rozwoju rejestrów medycznych należy dokonać zmian prawnych wprowadzających pojęcie "rejestru jakości" jako specyficznej kategorii rejestru medycznego. Głównym celem rejestru jakości jest pozytywne oddziaływanie na jakość opieki i uzyskiwane wyniki. Rejestry takie pozwalają ocenić kwalifikację do udzielania świadczeń, wyniki bezpośrednio udzielanych świadczeń i wyniki odległe poprzez powiązane ze świadczeniem wizyt kontrolnych w ustalonym schemacie czasowym (tzw. wizyty follow-up). Należy w Centrum Monitorowania

87. Opublikowany w 2017 r. projekt założeń do JakZdrU zakładał utworzenie kilkudziesięciu nowych rejestrów.

Jakości utworzyć krajowy ośrodek kompetencyjny rejestrów jakości na wzór rozwiązań skandynawskich. Ośrodek ten powinien mieć za zadanie ocenę istniejących rejestrów medycznych oraz tworzenia nowych rejestrów jakości zgodnych z zasadami dobrej praktyki rejestrowej w bezpośredniej współpracy z towarzystwami naukowymi, prowadzenia rejestrów jakości, dostarczania towarzystwom specjalistycznym informacji zwrotnej o jakości udzielanych świadczeń i wynikach medycznych oraz publikowanie ogólnodostępnych raportów z prowadzonych rejestrów. Wyniki rejestrów jakości winny być przekuwane w plany poprawy jakości (Quality Improvement).

Dla zasilenia rejestrów w dane zasadne jest wprowadzenie mechanizmów dodatkowego premiowania świadczeniodawców za przekazywanie danych medycznych oraz wprowadzenie środków technicznych i organizacyjnych służących ułatwieniu i automatyzacji przekazania danych do rejestrów medycznych. Inwestować należy w nowatorskie rozwiązania informatyczne ułatwiające gromadzenie danych w rejestrach jakości. Tylko bowiem rozwiązania ułatwiające i przyspieszające pracę lekarza spowodują powszechny udział i kompletność rejestrów jakości.

Pod kątem organizacyjnym wprowadzanie obowiązku przekazywania określonych danych do rejestru powinno być domyślnie realizowane poprzez zmianę wymagań (zakresu danych), które mają być zawarte w dokumencie medycznym powstającym w określonej sytuacji klinicznej. Standaryzacja dokumentacji medycznej prowadzonej w postaci elektronicznej pozwala na bezpieczne pobieranie jej części i przekazywanie do właściwego rejestru bez konieczności dublowania pracy lekarza.

Pożądaną jest też zagwarantowanie dodatkowych środków publicznych na stworzenie i prowadzenie rejestrów medycznych, a także zliberalizowanie zasad ich tworzenia (w tym nawet odstępianie od prawodawczego trybu ich tworzenia), prowadzenia i finansowania, w szczególności popularyzacja formuły partnerstwa publiczno-prywatnego, jednakże przy zachowaniu wysokich standardów w zakresie zabezpieczenia danych znajdujących się w rejestrach. Pacjent powinien mieć zagwarantowaną możliwość opt-out z rejestru.

Mając na uwadze możliwość wnioskowania o utworzenie rejestru medycznego przez medyczne towarzystwa naukowe, warto przy tej okazji dookreślić kryteria uznawania określonego podmiotu za medyczne towarzystwo naukowe. Nie jest to termin zdefiniowany prawnie, w związku z tym mogą zachodzić wątpliwości, czy określona organizacja kwalifikuje się jako medyczne towarzystwo naukowe w rozumieniu przywołanej ustawy.

Jak zostało to zasygnalizowane, możliwe jest także rozważenie innego systemu pełniącego podobną funkcję, lecz nie opierającego się na dotychczasowym systemie rejestrów jako osobnych bazach danych zasilanych przez dane raportowane z poziomu podmiotów wykonujących działalność leczniczą. Każdy nowy rejestr nakłada dodatkowy obowiązek sprawozdawczy na lekarzy i placówki ochrony zdrowia. Tymczasem możliwe jest stworzenie systemu, w którym dane medyczne mogą być możliwe do pobrania ze źródła, czyli wprost z systemów informacyjnych każdego podmiotu leczniczego, w zakresie określonym przepisami prawa. Stworzenie systemu umożliwiającego zebranie aktualnych danych (tzw. z ang. real world data) z wielu źródeł może dać efekt lepszy niż sieć silosowych rejestrów.



Sprawnie działający system rejestrów jakości zawierających rzetelne dane jest bezcenną informacją zwrotną dla lekarzy wykonujących świadczenia, stymulującą ich do poprawy własnych wyników. Zapewni zasoby umożliwiające m.in. prowadzenie badań naukowych i prac badawczo-rozwojowych oraz projektowanie polityki publicznej w ochronie zdrowia w oparciu o dane. Rejestry medyczne są już elementem systemu e-zdrowia w Polsce, postulowane zmiany wpisują się więc w dotychczasową politykę publiczną – zwracamy uwagę na potrzebę nadania bardziej priorytetowego charakteru działaniom w tym zakresie. Ich efektem powinien być sprawnie funkcjonujący system dostępu do jakościowych danych medycznych – czy to w modelu rejestrów, czy w modelu zapewniającym równie łatwy dostęp do danych bezpośrednio u źródła, czyli na poziomie systemu IT podmiotu wykonującego działalność leczniczą.

### 5.3.4.3 Zapewnienie interoperacyjności dokumentacji medycznej

**Stan obecny.** Podobnie jak w przypadku pojęcia jakości, także interoperacyjność może być różnie rozumiana, występować na poziomie organizacyjnym, semantycznym i technologicznym. Na potrzeby raportu interoperacyjność rozumiana będzie zgodnie z normami rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

Interoperacyjność w ochronie zdrowia regulowana jest przede wszystkim przez standardy prowadzenia dokumentacji medycznej oraz jej udostępniania. Zgodnie z § 1 ust. 6 pkt 6 i 8 DokMedR, system teleinformatyczny, w którym jest prowadzona dokumentacja medyczna, zapewnia możliwość prowadzenia i udostępniania dokumentacji w formatach i standardach wydanych na podstawie art. 11 ust. 1a i 1b SystInfOchZdr, a w przypadku ich braku - możliwość prowadzenia i udostępniania dokumentacji w standardach HL7 oraz DICOM lub innych standardach i formatach, a także możliwość eksportu całości danych w tych standardach i formatach, w sposób umożliwiający odtworzenie ich w innym systemie teleinformatycznym.

Zgodnie z przywołanym art. 11 ust. 1a i 1b SystInfOchZdr, elektroniczna dokumentacja medyczna jest prowadzona przez usługodawców w formatach zamieszczonych w Biuletynie Informacji Publicznej ministra właściwego do spraw zdrowia, a jej wymiana (w zakresie dokumentacji medycznej określonej w przepisach wydanych na podstawie art. 13a przywołanej ustawy) musi następować zgodnie ze standardami wymiany elektronicznej dokumentacji medycznej, zamieszczonymi w Biuletynie Informacji Publicznej ministra właściwego do spraw zdrowia.

Zgodnie z art. 8b SystInfOchZdr usługodawcy i podmioty prowadzące rejestry medyczne są obowiązane zapewniać zgodność swoich systemów teleinformatycznych z minimalnymi wymaganiami technicznymi i funkcjonalnymi zamieszczanymi w Biuletynie Informacji Publicznej ministra właściwego do spraw zdrowia, w terminie 9 miesięcy od dnia ich zamieszczenia.

Standardy przyjęte przez Centrum e-Zdrowia opublikowane zostały w „Portalu Interoperacyjności i Architektury” na stronie internetowej:

<https://www.gov.pl/web/ia/standardy-e-zdrowia>

W zakresie standardów gromadzenia i wymiany danych wskazano, za wytycznymi IHE, jako zasadne użycie standardu HL7 i DICOM. Podobnie też Komisja Europejska wskazała w decyzji 2015/1302 z dnia 28 lipca 2015 r. profile IHE jako rekomendowane do wykorzystania w zamówieniach publicznych w obszarze ochrony zdrowia. Minimalne wymagania dla systemów usługodawców zgodne z art. 8b SystInfOchZdr dostępne są pod adresem:

<https://www.gov.pl/web/zdrowie/minimalne-wymagania-dla-systemow-uslugodawcow>

Pomimo powyższych wymogów, standardy interoperacyjności nie są powszechnie przestrzegane. Jak wynika z badania przeprowadzonego przez Centrum e-Zdrowia, problemy z interoperacyjnością i jej standardami wciąż sygnalizuje 15% placówek<sup>88</sup>.

Problemy występują także na poziomie semantyki, tj. niespójnej terminologii stosowanej do opisu udzielanych świadczeń zdrowotnych. Obecnie trwają prace, zainicjowane w Polskim Towarzystwie Diagnostyki Laboratoryjnej pod koniec 2020 r., mające na celu opracowanie aktualnego, standaryzowanego nazewnictwa badań laboratoryjnych w Polsce<sup>89</sup>. Projekt dotyczy jednak tylko obszaru medycyny laboratoryjnej, podczas gdy podobne działania są potrzebne także w innym zakresie, np. w badaniach obrazowych. Jest to szczególnie ważne, bowiem proces zastępowania tradycyjnej dokumentacji medycznej dokumentacją elektroniczną wymaga pilnego zajęcia się zagadnieniem standaryzacji gromadzonych i przetwarzanych informacji, zarówno w zakresie nazewnictwa (semantycznym), jak i składni (syntaktycznym).



### Perspektywa zmian

Program rozwoju e-zdrowia w Polsce do 2027 r. przewiduje powołanie centrum kompetencyjnego ds. danych medycznych, które zajmie się interoperacyjnością semantyczną oraz modelem danych medycznych. Jako bazowa terminologia zostanie wdrożona SNOMED CT, wokół której będą tworzone zbiory wartości budowane spośród innych terminologii i klasyfikacji (w tym rodzinę międzynarodowych klasyfikacji medycznych WHO-FIC i inne dziedzinowe). Zostanie opracowany logiczny model danych, struktury danych w postaci zasobów HL7 FHIR oraz specyfikacja MedAPI oparta na zasobach HL7 FHIR<sup>90</sup>.

W świetle EHDS interoperacyjność oznacza zdolność organizacji, jak również aplikacji lub wyrobów tego samego producenta lub różnych producentów do współdziałania na rzecz osiągnięcia celów korzystnych dla wszystkich stron, w tym wymiany informacji i wiedzy między tymi organizacjami, aplikacjami lub wyrobami bez zmiany treści danych, za pomocą obsługiwanych przez nie procesów.

88. VI Edycja „Badania stopnia informatyzacji podmiotów wykonujących działalność leczniczą”, Centrum e-Zdrowia, wrzesień 2022; s. 66

89. <https://www.termedia.pl/mz/Standaryzacja-informacji-w-diagnostyce-laboratoryjnej,51341.html>

90. Program rozwoju e-zdrowia w Polsce do 2027 r.; str. 33.

Na poziomie EHDS zasadnicze wymagania dotyczące systemów elektronicznej dokumentacji medycznej i produktów, w odniesieniu do których deklaruje się interoperacyjność z systemami elektronicznej dokumentacji medycznej określone zostały w załączniku II. Komisja ma dodatkowo przyjmować, w drodze aktów wykonawczych, wspólne specyfikacje w odniesieniu do zasadniczych wymagań dotyczących systemów elektronicznej dokumentacji medycznej i przywołanych produktów.



## Możliwe działania

Obecne regulacje zobowiązują podmioty udzielające świadczeń zdrowotnych do spełniania standardów interoperacyjności wskazanych przez Ministerstwo Zdrowia. Zasadniczym problemem są trudności związane z ich przestrzeganiem.

Po pierwsze, niejasne i nieczytelne dla odbiorców mogą być zasady publikacji nowych standardów – standardy e-zdrowia opisane w Portalu Interoperacyjności i Architektury odsyłają przez hipertąca do szeregu różnych stron internetowych, np. strony Centrum e-Zdrowia<sup>91</sup> (gdzie część dokumentów dostępna jest w archiwum ZIP), strony organizacji IHE<sup>92</sup>, organizacji HL7<sup>93</sup> czy też strony dedykowanej standardowi DICOM<sup>94</sup>. Część z materiałów nie jest dostępna w języku polskim. Zasadne byłoby stworzenie jednej, przejrzyste opisanej strony w Biuletynie Informacji Publicznej ministra właściwego do spraw zdrowia, która zawierałaby dokumenty wymagane do wywiązania się z konkretnych obowiązków związanych z interoperacyjnością. Także zmiany standardów powinny następować na tych samych zasadach – wzorem może być procedura z art. 8b SystInfOchZdr, która przewiduje proces konsultacji i czas na dostosowanie. Zmiany powinny umożliwiać sprawną adopcję rozszerzania struktury kolejnych dokumentów lub modyfikacji już istniejących struktur w zakresie Polskiej Implementacji Krajowej HL7 CDA.

JakZdrU wprowadziła rozwiązanie, które może okazać się w praktyce trudno egzekwowalne, a zatem nie przekładać się na poprawę sytuacji. Wymogi w tym zakresie, zaprojektowane już pod kątem załącznika II do EHDS, mogłyby zostać uregulowane w zapowiadanej przez Program rozwoju e-zdrowia w Polsce do 2027 r. ustawie o danych medycznych.

Dla zwiększenia faktycznego zaadoptowania wymogów związanych z interoperacyjnością danych, przestrzeganie wysokich standardów powinno zostać włączone do systemu jakości wynikającego z JakZdrU, np. jako element fakultatywnego systemu akredytacji.

Niezależnie od powyższego potrzebne są także projekty mające na celu wypracowanie ujednoczonego nazewnictwa (semantycznym), jak i składni (syntaktycznym) wykorzystywanych w opisach badań.

91. <https://ezdrowie.gov.pl/>

92. <https://www.ihe.net/resources/>

93. <http://www.hl7.org/>

94. <https://www.dicomstandard.org/current>



Interoperacyjność danych medycznych ma w pierwszej kolejności zapewniać lekarzowi lepszy wgląd w sytuację pacjenta w oparciu o dotychczas wytworzoną dokumentację. Wspólne standardy zapewniają łatwość przekazywania ustrukturyzowanych zbiorów danych cyfrowych, które mogą być odczytywane przez inne systemy i dalej wykorzystywane. Podobnie jak w przypadku rejestrów medycznych, lekarz odnosić też będzie pośrednie korzyści związane z rozwojem innowacyjnych narzędzi dzięki – zapewnianemu przez interoperacyjność - większemu poziomowi wykorzystywania danych.

Propozycja wpisuje się w postulat dotyczący zapewnienia funkcjonalnego wykorzystywania danych - lekarz powinien móc sprawnie korzystać z różnych danych, a także aplikacji i programów, które pomogą mu zebrać, przeanalizować oraz wykorzystać dane w procesie opieki nad pacjentem. Aby dane mogły być przesyłane i odczytywane maszynowo, niezbędna jest interoperacyjność.

### 5.3.5 Udostępnianie danych

Dane gromadzone przez lekarzy i podmioty wykonujące działalność leczniczą mogą być udostępniane innym lekarzom i podmiotom przy spełnieniu wszystkich wymaganych przez przepisy prawa warunków, np. na podstawie zgody pacjenta. Bardzo ważnym z praktycznego punktu widzenia zagadnieniem pozostaje kwestia tego, komu i na jakich warunkach lekarz może udostępniać dane pacjentów. Kluczową kwestią wymagającą rozwiązania jest stworzenie klasyfikacji danych pod względem ich wrażliwości, tak aby pacjent mógł decydować czy udostępnić swoje dane, co najczęściej pozostaje warunkiem bazowym, a jeżeli udostępnić to czy również dane o wysokiej wrażliwości.

#### 5.3.5.1 Zasady dostępu do danych medycznych i dokumentacji medycznej

**Stan obecny.** Jak zostało to już przedstawione w punkcie 5.3.1.1 raportu, obecnie obowiązujące regulacje prawne odróżniają pojęcia m.in. danych, jednostkowych danych medycznych czy dokumentacji medycznej. Co więcej, dla różnych pojęć przewidziano różne zasady dostępu, które rozproszone są po różnych aktach prawnych.

Zgodnie z art. 11 ust. 2 SystInfOchrZdr, dane osobowe i jednostkowe dane medyczne, zawarte w elektronicznej dokumentacji medycznej usługobiorcy, zgromadzone w systemie teleinformatycznym usługodawcy, są udostępniane za pośrednictwem SIM. Jednocześnie też udostępnianie tych danych bez pośrednictwa SIM, następuje na zasadach określonych w PrPacjU. Regulacja ta przewiduje więc dwa różne tryby udostępniania tych samych danych, w zależności od kanału (pośrednictwo SIM), którym następuje udostępnienie.

Przepis art. 12 ust. 6 SystInfOchrZdr wskazuje, że pracownikom medycznym i usługodawcom, w zakresie wykonywanych przez nich zadań i posiadanych uprawnień, udostępniane są dane, w tym dane osobowe i jednostkowe dane medyczne usługobiorców, przetwarzane w SIM, w zakresie niezbędnym do realizacji zadań z zakresu wymiany pomiędzy usługodawcami



danych zawartych w elektronicznej dokumentacji medycznej, jeżeli jest to niezbędne do zapewnienia ciągłości leczenia, wymiany dokumentów elektronicznych pomiędzy usługodawcami oraz pobrania danych w celu prowadzenia diagnostyki, ciągłości leczenia oraz zaopatrzenia usługobiorców w produkty lecznicze i wyroby medyczne, a także prowadzenia list oczekujących na udzielenie świadczenia. Regulacja ta wskazuje więc na stosunkowo szeroki dostęp lekarzy do danych dostępnych w SIM.

Jednak zgodnie z art. 35 SystInfOchrZdr, dostęp do danych osobowych lub jednostkowych danych medycznych usługobiorców, przetwarzanych w systemie teleinformatycznym usługodawcy lub w SIM, mają już tylko: pracownik medyczny, który wytworzył elektroniczną dokumentację medyczną zawierającą dane osobowe lub jednostkowe dane medyczne usługobiorcy; pracownik medyczny wykonujący zawód u usługodawcy, u którego została wytworzona elektroniczna dokumentacja medyczna zawierająca dane osobowe lub jednostkowe dane medyczne usługobiorcy, w związku z wykonywaniem przez niego zawodu u tego usługodawcy, jeżeli jest to niezbędne do prowadzenia diagnostyki lub zapewnienia ciągłości leczenia; lekarz, pielęgniarka lub położna udzielający usługobiorcy świadczeń opieki zdrowotnej w ramach umowy o udzielanie świadczeń opieki zdrowotnej z zakresu podstawowej opieki zdrowotnej, a także każdy pracownik medyczny w sytuacji zagrożenia życia usługobiorcy.

W innych przypadkach udostępnienie danych osobowych lub jednostkowych danych medycznych z systemu teleinformatycznego usługodawcy lub z SIM następuje za zgodą usługobiorcy lub jego przedstawiciela ustawowego. Wyrażając zgodę, wskazuje się zakres czasowy i przedmiotowy dostępu do tych danych. Co ważne, przywołane uregulowania nie naruszają przepisów o dostępie do danych zawartych w dokumentacji medycznej w sposób określony w PrPacjU.

W świetle ostatniej przywołanej ustawy, a dokładniej art. 26 ust. 1 PrPacjU, podmiot udzielający świadczeń zdrowotnych udostępnia dokumentację medyczną pacjentowi lub jego przedstawicielowi ustawowemu, bądź osobie upoważnionej przez pacjenta. Dalsze ustępy przywołanego przepisu wskazują zasady dostępności dokumentacji medycznej po śmierci pacjenta, a także katalog podmiotów uprawnionych do dostępu do dokumentacji medycznej bez zgody pacjenta. Dostęp ten przysługuje m.in. podmiotom udzielającym świadczeń zdrowotnych, jeżeli dokumentacja ta jest niezbędna do zapewnienia ciągłości świadczeń zdrowotnych.

Na jeszcze innych zasadach udostępnia się dane przetwarzane w rejestrach medycznych. W przypadku rejestrów ustawowych przepisy dotyczące poszczególnych rejestrów wyraźnie wskazują katalog uprawnionych do dostępu podmiotów, np. zgodnie z art. 15 ust. 7 SystInfOchrZdrU, administrator danych udostępnia dane zawarte w Centralnym Wykazie Usługobiorców usługodawcom, w określonym w tym przepisie zakresie, w celu umożliwienia automatycznego działania systemów teleinformatycznych usługodawców. Podobnie w przypadku rejestrów tworzonych przez ministra zdrowia, z tym, że zawarte w nich dane mogą być udostępniane dowolnym podmiotom w celu prowadzenia badań naukowych i do celów statystycznych w formie uniemożliwiającej ich powiązanie z konkretną osobą fizyczną (por. 5.3.6.1 raportu). Obok tego mamy

generalny tryb dostępu do informacji wynikający z ustawy o dostępie do informacji publicznej, OtwDanU, a także DGA i ZarzadDanU<sup>95</sup>.

Powyższe regulacje tworzą – w kontekście dostępu do danych - nieintuicyjny, nieprzejrzysty system. W praktyce wszelkie wątpliwości interpretacyjne w tym zakresie, jakie podnoszone bywają przez podmioty wykonujące działalność leczniczą, rozstrzygane są często na niekorzyść udostępnienia, jako że wiążą się z ryzykiem naruszenia prywatności pacjenta.

Warto zwrócić uwagę, że obowiązki związane z udostępnianiem dokumentacji medycznej lub jednostkowych danych medycznych odnoszą się do jednorazowych sytuacji, tj. po wptynięciu wniosku dane lub dokumenty są przekazywane uprawnionym podmiotom. Taki stan rzeczy nie uwzględnia okoliczności związanych z tym, że dane i dokumenty mogą być dalej uzupełniane. Jest to szczególnie ważne w kontekście podmiotów uprawnionych do dostępu, takich jak podmioty udzielające świadczeń zdrowotnych w ramach zapewniania ich ciągłości, Agencja Badań Medycznych, Agencja Oceny Technologii Medycznych i Taryfikacji, sądy i prokuratura. Przepisy prawa nie przewidują obowiązku uzupełniania przestanych już materiałów o nowe dokumenty i dane, które mogą mieć istotne znaczenie pod kątem zadań tych podmiotów. Obowiązek o trochę podobnym charakterze przewiduje art. 19 RODO, zgodnie z którym administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.



### Perspektywa zmian

Dobłą okazją do uporządkowania i większego ujednoczenia zasad dostępu do danych medycznych będzie zapowiadana w Programie rozwoju e-zdrowia w Polsce do 2027 r. ustawa o danych medycznych. Jak można się spodziewać, do tego czasu będzie obowiązywać już ZarzadDanU, która także obejmuje swoim zakresem zasady dostępu do danych przetwarzanych przez część podmiotów wykonujących działalność leczniczą, w tym m.in. samodzielne publiczne zakłady opieki zdrowotnej. Tym samym ustawa o danych medycznych powinna uwzględniać też tryby dostępu przewidziane przez inne akty prawne. Wprowadzenie ustawy o danych medycznych stanowi szansę, aby ujednoczyć przepisy, które regulują dostęp do dokumentacji medycznej – m.in. poprzez wprowadzenie zmian w innych ustawach i przepisy odsyłające.

Jak zostało to już zauważone, nieco odmienną siatką pojęciową posługuje się EHDS, który zawiera też inne regulacje dotyczące udostępniania danych. Zgodnie z art. 4 EHDS, w przypadku przetwarzania danych w formacie elektronicznym pracownicy systemu ochrony zdrowia mają dostęp do elektronicznych danych dotyczących zdrowia osób fizycznych, które leczą, niezależnie od państwa członkowskiego ubezpieczenia i państwa członkowskiego leczenia. Państwa członkowskie zapewniają pracownikom ochrony zdrowia dostęp co najmniej do priorytetowych kategorii elektronicznych danych dotyczących zdrowia, o których to kategoriach mowa w art. 5 EHDS, a także mogą ustanowić przepisy określające kategorie elektronicznych danych osobowych dotyczących

95. W momencie powstawania raportu wciąż na etapie projektu ustawy.

zdrowia wymaganych przez różne zawody związane z ochroną zdrowia. EHDS w art. 33 i nast. określa też zasady udostępniania danych medycznych do wtórnego wykorzystywania.

Mając na uwadze okoliczność, że dokumentacja medyczna może być na bieżąco uzupełniana, warto opracować wytyczne dotyczące powiadomień dla wybranych kategorii jej potencjalnych, ustawowo wyznaczonych odbiorców (np. inne podmioty lecznicze, sądy, prokuratura) o wytworzeniu nowych danych lub dokumentów. Bez tego występować będzie ryzyko, że lekarz lub sędzia podejmować będzie decyzję w oparciu o niepełny obraz stanu zdrowia pacjenta. Potencjalnie powiadomienia o takim charakterze mogłyby być generowane automatycznie przez system centralny. Co ważne, kategorie odbiorców powiadomień powinny być starannie wyselekcjonowane pod kątem niezbędności dostępu do wiedzy o aktualnym stanie zdrowia pacjenta.

W tym temacie warto zwrócić też uwagę na usługi pośrednictwa danych oraz altruizm danych, czyli pojęcia wprowadzone przez DGA, które mają zwiększyć zakres udostępnianych danych i zmienić model ich udostępniania przez udział wyspecjalizowanych „pośredników”.



### Możliwe działania

W pierwszej kolejności pożądane jest wspomniane już uporządkowanie oraz większe ujednoczenie zasad dostępu do danych medycznych, możliwie w ramach jednej ustawy. Obecne zasady wynikają z całego szeregu przepisów rozsianych po różnych aktach prawnych i tworzą skomplikowany, nieprzejrzysty system, który sam w sobie może być postrzegany jako swoista przeszkoda w dostępie do danych.

Nowy system powinien opierać się na siatce pojęciowej i zasadach wprowadzanych przez EHDS, w szczególności odróżniać elektroniczne dane osobowe dotyczące zdrowia oraz elektroniczne dane nieosobowe dotyczące zdrowia, a także ich pierwotne lub wtórne wykorzystywanie. Pojęcia te są punktem wyjścia dla odpowiedniego i zgodnego z RODO uregulowania zasad dostępu, które w przypadku danych osobowych pacjentów powinny być dużo bardziej rygorystyczne. Dostęp do nieosobowych danych dotyczących zdrowia powinien być zaś stosunkowo szeroki, niezależnie od źródła tych danych.

Należy przy tym ustanowić na poziomie ustawowym jasne i wyraźne cele przetwarzania danych medycznych w systemach administrowanych przez stronę publiczną oraz związane z nimi funkcjonalnie zasady dostępu do poszczególnych zbiorów danych. Nie powinno dochodzić do sytuacji, w których dostęp do danych jest nadużywany, a dane medyczne wykorzystywane są niezgodnie z ich ustawowym przeznaczeniem.

Zasadne jest także wspieranie rozwoju usług pośrednictwa danych oraz altruizmu danych w ochronie zdrowia, tak aby jak największy ich zasób był łatwo dostępny przy wykorzystaniu wyspecjalizowanych w tym zakresie podmiotów.



## Uzasadnienie

Obecny stan prawny w tej materii jest efektem przyjmowanych na przestrzeni ostatnich kilkunastu lat nowelizacji, które dostosowywały prawo do aktualnych możliwości systemu P1. Część z nich była przyjmowana jeszcze przed uruchomieniem konkretnych usług. W efekcie powstał niejasny system, który z perspektywy lekarza lub innego użytkownika danych może być trudny do zrozumienia, a przez to zniechęcający do jego wykorzystywania. Niespójność tak ważnych dla ochrony prywatności pacjentów przepisów wiąże się też z występowaniem ryzyka interpretacyjnego, co dodatkowo może obniżać chęć dzielenia się danymi. W efekcie takiego stanu rzeczy lekarz może mieć ograniczony dostęp do danych, bo zobowiązana do ich udostępnienia placówka medyczna nie będzie chciała ich przekazać z uwagi na własną interpretację prawa. Lekarz tracić będzie w związku z tym także pośrednie korzyści związane z rozwojem innowacyjnych narzędzi dzięki wykorzystywaniu danych.

Propozycja wpisuje się w postulat dotyczący dostępności danych – lekarz powinien mieć łatwy i szybki dostęp do danych pacjentów z różnych źródeł. To zależy zaś od zasad udostępniania danych.

### 5.3.5.2 Udostępnianie danych a umowy powierzenia przetwarzania danych

**Stan obecny.** W sektorze ochrony zdrowia w dalszym ciągu dochodzi do nagminnego zawierania umów powierzenia przetwarzania danych osobowych w sytuacjach, w których nie jest to uzasadnione – odbiorca danych jakim jest podmiot wykonujący działalność leczniczą nie będzie bowiem zazwyczaj działał jako podmiot przetwarzający, tzw. procesor, ale zupełnie nowy, niezależny administrator danych. Sytuacja taka jest niepożądana, bowiem część podmiotów leczniczych, nie dość, że poświęca dodatkowy czas na przygotowanie i negocjowanie takiej umowy, to dodatkowo przyjmuje na siebie możliwe do uniknięcia zobowiązania, co podnosi ryzyko kontraktowe. Podstawowe zasady i konkretne przykłady związane z zawieraniem umów powierzenia przetwarzania danych osobowych zawiera zatwierdzony przez PUODO kodeks postępowania dotyczący ochrony danych osobowych przetwarzanych w małych placówkach medycznych<sup>96</sup>. Do umów odnosi się także „Kodeks postępowania dla sektora ochrony zdrowia”, do którego mogą przystępować zarówno podmioty publiczne, jak i prywatne.



## Perspektywa zmian

Planowane zmiany prawne nie adresują tego zagadnienia. Co więcej, coraz większa liczba podmiotów zaangażowanych w jakiś sposób w przetwarzanie danych medycznych, np. podmioty zajmujące się pośrednictwem danych, może tylko pośrednio spotęgować problem.

96. Kodeks postępowania dotyczący ochrony danych osobowych przetwarzanych w małych placówkach medycznych; Warszawa 2022 r.



## Możliwe działania

Do poprawy sytuacji przyczyni się szersze stosowanie zatwierdzonych kodeksów postępowania. Dla dalszej popularyzacji tematu wskazane byłoby wydanie oficjalnych wytycznych przez PUODO, które zawierałyby bardziej rozbudowany katalog najbardziej typowych sytuacji, w których tego rodzaju umowy należy lub nie powinno się zawierać.

Bardzo ważnym tematem jest także udostępnianie danych osobowych (w relacji od administratora do administratora), które w przypadku ochrony zdrowia występuje stosunkowo często. Obecnie obowiązuje przepisy nie narzucają określonych standardów takiego udostępniania, nie ma wymogu zawierania umowy, który regulowałaby ten proces, choć nierzadko ma on dużo większe znaczenie dla ochrony danych osobowych niż powierzenie ich przetwarzania. Zasadne byłoby w związku z tym przyjęcie pod patronatem PUODO wytycznych w tym zakresie, w tym nawet gotowych do wykorzystania wzorów umów.



## Uzasadnienie

Jak zostało to zasygnalizowane, nadmierne zawieranie zupełnie niepotrzebnych umów powierzenia przetwarzania danych wiąże się z dodatkowym obciążeniem administracyjnym oraz ryzykiem kontraktowym. Jest to szczególnie istotne w przypadku lekarzy prowadzących jednoosobową działalność gospodarczą, którzy mogą być stronami takich potencjalnie dla nich niekorzystnych umów. Jednocześnie też brakuje standardów dla równie ważnych procesów udostępniania danych pomiędzy różnymi administratorami, co prowadzi do różnych praktyk. Wiąże się to z dodatkowym ryzykiem dla samych danych, jak i ryzykiem prawnym dla podmiotów zaangażowanych w ich wymianę.

Propozycja wpisuje się w postulat dotyczący zapewnienia funkcjonalnego wykorzystywania danych - lekarz powinien móc sprawnie korzystać z różnych danych, a także aplikacji i programów, które pomogą mu zebrać, przeanalizować oraz wykorzystać dane w procesie opieki nad pacjentem. Niepotrzebne umowy powierzenia przetwarzania mogą nakładać zbędne ograniczenia i wiązać się z możliwym do uniknięcia ryzykiem kontraktowym.

### 5.3.5.3 Anonimizacja i pseudonimizacja danych medycznych

**Stan obecny.** Zgodnie z definicją legalną z art. 4 pkt 5. RODO, pseudonimizacja danych oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Jak zatem wynika z powyższej definicji, pseudonimizacja jest pewną operacją dokonywaną na danych osobowych, jest procesem ich przetwarzania. Pseudonimizacja jest przy tym procesem w pełni odwracalnym. Spseudonimizowane dane osobowe, które przy użyciu dodatkowych informacji można przypisać osobie fizycznej, należy uznać za informacje możliwe do zidentyfikowania.

Informacja poddana pseudonimizacji nie traci zatem charakteru danych osobowych, na co zwraca uwagę motyw 26 preambuły RODO: spseudonimizowane dane osobowe, które przy użyciu dodatkowych informacji można przypisać osobie fizycznej, należy uznać za informacje o możliwej do zidentyfikowania osobie fizycznej. Dane spseudonimizowane są wciąż danymi osobowymi. Dlatego pseudonimizacja jest generalnie uznawana za środek bezpieczeństwa, a nie metodę anonimizacji<sup>97</sup>. Typowym przykładem pseudonimizacji danych osobowych będzie zatem postępowanie się numerem identyfikacyjnym i ograniczonym zestawem danych osobowych zamiast pełnego zestawu danych. Taki numer identyfikacyjny powinien być przechowywany oddzielnie, wraz z informacjami umożliwiającymi identyfikację osoby, i dodatkowo być odpowiednio zabezpieczony.

RODO nie zawiera definicji legalnej procesu anonimizacji danych anonimowych. Uznaje się, że anonimizacja jest procesem, w którym informacje umożliwiające identyfikację osoby są nieodwracalnie usunięte lub zmienione w taki sposób, aby nie istniała już możliwość bezpośredniego lub pośredniego zidentyfikowania podmiotu informacji nawet przez administratora informacji działającego samodzielnie lub we współpracy z jakąkolwiek inną stroną. W procesie anonimizacji usuwa się lub modyfikuje informacje, które mogą stanowić dane osobowe w rozumieniu RODO, pozostawiając inne, które nie pozwalają już na identyfikację osoby, której te dane dotyczą, a nadal mogą być użyteczne dla określonego celu. ISO definiuje anonimizację jako proces, w którym dane osobowe są nieodwracalnie zmieniane w taki sposób, że podmiot danych nie może być już zidentyfikowany bezpośrednio lub pośrednio, przez samego administratora danych lub we współpracy z jakąkolwiek inną stroną<sup>98</sup>. Proces anonimizacji musi być trwały i nieodwracalny. Dane zanonimizowane nie stanowią już danych osobowych. Skoro w pełni zanonimizowane dane nie są danymi osobowymi, nie podlegają tym samym wymogom i ograniczeniom, które nakłada się na przetwarzanie danych osobowych zgodnie z RODO. Niemniej, anonimizacja jest techniką stosowaną w celu uzyskania nieodwracalnej anonimizacji, dlatego też założeniem wyjściowym jest to, że poddane niej dane osobowe musiały zostać zgromadzone i przetworzone zgodnie z mającymi zastosowanie standardami dotyczącymi utrzymywania danych w formie uniemożliwiającej identyfikację. RODO nie odwołuje się do żadnej konkretnej techniki anonimizacji, zatem to od poszczególnych administratorów danych zależy, czy wybrany przez nich proces „anonimizacji” jest wystarczająco solidny. Istnieją różne praktyki i techniki anonimizacji o różnych stopniach dokładności, np. podejście oparte na randomizacji czy podejście oparte na uogólnianiu.

97. UODO, Stosowanie technicznych środków bezpieczeństwa w aspekcie zgłoszeń naruszeń do UODO oraz ocena wagi naruszenie w oparciu o zalecenia Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA), Mariola Więckowska, 2019, <https://uodo.gov.pl/pl/file/1812>

98. <https://incisive-project.eu/wp-content/uploads/2021/11/2021-Personal-data-pseudonymization-and-anonymization-in-research-%E2%80%93-selected-issues.pdf>

Występujące wątpliwości interpretacyjne dotyczą przede wszystkim tego, jak należy oceniać nieodwracalność skutku anonimizacji. Wyróżnia się dwa zasadnicze podejścia w tym zakresie:

**podejście obiektywne** – w tej perspektywie dane są uznawane za zanonimizowane jedynie wtedy, gdy nikt (w tym administrator danych wejściowych) nie jest w stanie zidentyfikować podmiotu, którego dane dotyczą;

**podejście subiektywne** – w tej perspektywie wystarczającym dla uznania, że dane są danymi zanonimizowanymi jest stwierdzenie, że strona posiadająca dane dotyczące podmiotu danych nie może, postępując zgodnie z przepisami prawa, zidentyfikować tego podmiotu danych.

Ustawodawca europejski, EROD, ustawodawca polski lub PUODO nie wskazują, kiedy ryzyko ponownej identyfikacji uznać należy za akceptowalne. W Polskiej judykaturze poza kilkoma orzeczeniami dotyczącymi w uzasadnieniu tego tematu na ten moment brakuje jeszcze utrwalonej linii orzeczniczej dotyczącej anonimizacji oraz pseudonimizacji.

Co więcej, zarówno proces pseudonimizacji, jak i anonimizacji, stanowią pewną operację lub zestaw operacji dokonywanych na danych osobowych, a zatem – w konsekwencji – są w dalszym ciągu przetwarzaniem danych osobowych<sup>99</sup>. W związku z tym procesy te muszą spełniać wymóg zgodności poprzez uwzględnienie odpowiednich podstaw prawnych i okoliczności dalszego przetwarzania. W przypadku niespełnienia tego wymogu, jak należy konsekwentnie uznać, procesy te nie stanowią dalszego przetwarzania danych, a niezależne procesy przetwarzania danych, co wymagać będzie wykazania innych podstaw prawnych. Wydają się to potwierdzać także definicje przyjęte przez RODO, tj. przetwarzanie oznacza „operację” lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych, a pseudonimizacja oznacza „przetworzenie” danych osobowych. Można więc uznać, że przetworzenie wiąże się z co najmniej jedną określoną operacją na danych osobowych, a więc tym samym wiąże się z przetwarzaniem danych, co wymaga już podstawy prawnej.

Zgodnie z art. 5 ust. 1 pkt lit. b RODO, dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i przetwarzane dalej w sposób zgodny z tymi celami. Dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 RODO<sup>100</sup> za niezgodne z pierwotnymi celami. Zasada ta nie może być rozumiana jako zakaz przetwarzania danych osobowych w innym celu niż cel, dla którego zostały zebrane, lecz jako zakaz przetwarzania danych w celu niezgodnym z pierwotnie określonym<sup>101</sup>. Tym samym można uznać, że RODO nie zabrania przetwarzania danych w celu innym niż cel, w którym dane zostały zebrane, a jedynie przetwarzania danych w celu niezgodnym z celem zebrania danych.

99. Por. opinia 05/2014 Grupy Roboczej art. 29 w sprawie technik anonimizacji, 0829/14/PL WP216, s. 3.

100. Przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych podlega odpowiednim zabezpieczeniom dla praw i wolności osoby, której dane dotyczą, zgodnie z niniejszym rozporządzeniem. Zabezpieczenia te polegają na wdrożeniu środków technicznych i organizacyjnych zapewniających poszanowanie zasady minimalizacji danych. Środki te mogą też obejmować pseudonimizację danych, o ile pozwala ona realizować powyższe cele. Jeżeli cele te można zrealizować w drodze dalszego przetwarzania danych, które nie pozwalają albo przestały pozwalać na zidentyfikować osoby, której dane dotyczą, cele należy realizować w ten sposób.

101. P. Litwinski (red.), Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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) [w:] P. Litwinski (red.) Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz.

Jak wskazuje Grupa Robocza art. 29<sup>102</sup>, możliwe jest, że przy wstępnym określaniu celu ani administrator, ani osoba, której dane dotyczą, nie myśleli o dodatkowych celach, chociaż później okazało się, że dane mogą być rzeczywiście bardzo przydatne do innych celów. W niektórych z tych sytuacji zmiana celu może być dozwolona, a dalsze przetwarzanie może zostać uznane za nie niezgodne, pod warunkiem spełnienia testu zgodności. Pozytywny wynik testu zgodności (tj. stwierdzenie, że cel dalszego przetwarzania jest zgodny z celem pierwotnego przetwarzania) pozwala na prowadzenie dalszego przetwarzania bez konieczności uzyskania odrębnej podstawy prawnej (np. zebrania zgody). Regulacje prawne nie zawierają dalszych wskazówek dotyczących tego, jak przeprowadzić test zgodności. Jak wskazywała Grupa Robocza art. 29, test zgodności może opierać się o formalne kryteria (formal assessment), bazując na informacji przekazanej osobie, której dane dotyczą, albo oceniać także kwestie merytoryczne (substantive assessment), takie jak np. kontekst przetwarzania<sup>103</sup>.



### Perspektywa zmian

Planowane zmiany prawne nie adresują wyczerpująco tego zagadnienia. Program rozwoju e-zdrowia w Polsce do 2027 r. przewiduje, że na potrzeby badań i analiz powstanie spójny standard pseudonimizacji danych pacjentów. Rodzi to jednak poważne niebezpieczeństwo, iż będziemy mieli do czynienia z pseudopseudonimizacją danych. Standard powinien zostać opracowany tak, by znając go nie było można dowolnych danych poddanych pseudonimizacji rzywrócić do formy pełnej. Wyzwaniem może być zapewnienie anonimowości pacjenta przy jednoczesnym zachowaniu ciągłości danych. DGA czy EHDS tymczasem opierają się na zastanym na gruncie RODO rozumieniu anonimizacji i pseudonimizacji danych. Brak podobnego standardu pseudonimizacji oraz anonimizacji danych pacjentów może znacząco utrudniać ich stosowanie.



### Możliwe działania

Dla właściwego stosowania zasad DGA czy EHDS, ale też szerzej, zapewnienia w praktyce dostępności danych anonimowych, kluczowe jest przyjęcie dedykowanych regulacji prawnych lub jasnego standardu w zakresie przeprowadzenia anonimizacji i pseudonimizacji danych medycznych, który wskazywać będzie w jasny sposób właściwe podstawy dla wykonywania tych operacji na danych oraz rekomendowane metody. Konieczne jest wypracowanie warunków, których spełnienie pozwoli określić, czy określone dane medyczne nie poddają się rzeczywistej anonimizacji czy też pozwalają zidentyfikować pacjenta, pomimo braku takich danych jak pesel, imię, nazwisko, adres min.. Tego rodzaju normy mogłyby być regulowane aktami prawa powszechnie obowiązującego lub poprzez zatwierdzone kodeksy branżowe.

102. Zespół roboczy ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, na określenie Zespołu roboczego powszechnie używano również nazwy „Grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych” lub „Grupa robocza art. 29”. Na mocy RODO został zastąpiony przez Europejską Radę Ochrony Danych. Nie wpływa to jednak automatycznie na nieaktualność wcześniejszych wytycznych Grupy Roboczej art. 29.

103. Grupa Robocza Art. 29 w Opinii 03/2013 w sprawie ograniczenia celu (WP 203), dostępnej na stronie [www.giodo.gov.pl](http://www.giodo.gov.pl), str. 21.





Zwiększenie dostępu do danych medycznych poddanych anonimizacji i pseudonimizacji stanowi jeden z kluczowych warunków poszerzenia dostępu do zbiorów danych, które mogą być wykorzystywane przez lekarzy (i nie tylko) w celach naukowych lub badawczo-rozwojowych. Dane te służą być in. in. rozwojowi innowacyjnych produktów i usług oraz projektowaniu polityki publicznej w obszarze ochrony zdrowia, co oznacza potencjalnie pośrednie korzyści dla pacjentów, lekarzy i innych osób wykonujących zawody medyczne – dostęp do nowych narzędzi i skuteczniejsza organizacja systemu.

Propozycja wpisuje się w postulat dotyczący celów naukowych i rozwojowych - lekarz powinien móc wykorzystać dane medyczne w celach naukowych i badawczych. W wielu przypadkach wystarczający będzie dostęp do danych anonimowych, który z uwagi na charakter tych danych powinien być jak najłatwiejszy.

Należy równocześnie mieć na względzie, że zwiększenie dostępu do danych medycznych poddanych pseudonimizacji może być wykorzystane w celach innych, w tym podczas postępowań zmierzających do wyciągnięcia konsekwencji wobec lekarzy.

### 5.3.6 Udostępnianie i przetwarzanie danych w celach naukowych i badawczo- rozwojowych

Olbrzymi potencjał związany z danymi medycznymi dotyczy możliwości ich udostępniania w celach prowadzenia badań naukowych oraz prac badawczo-rozwojowych, w tym rozwijania algorytmów sztucznej inteligencji. Uwolnienie danych – przy zachowaniu ich poufnego charakteru oraz wysokiej jakości – stwarza szansę na szybki rozwój wielu nowych innowacyjnych rozwiązań. Jednak należy mieć na uwadze, iż obecnie większość istniejących danych medycznych ma dla badań naukowych ograniczone znaczenie, gdyż ich wiarygodność jest wątpliwa. Dopiero wprowadzenie gromadzenia danych w oparciu o tworzone zgodnie z rygorystyczną metodologią rejestru jakości dostarczają wartościowych danych dla badań naukowych i trenowania sztucznej inteligencji.

#### 5.3.6.1 Przestanki udostępniania danych w celach naukowych

**Stan obecny.** Obowiązujące przepisy prawa przewidują dedykowane zasady dostępu do dokumentacji medycznej i danych medycznych, które miałyby być wykorzystywane w celach naukowych.

W pierwszej kolejności przywołać należy art. 26 ust. 4 PrPacjU, zgodnie z którym dokumentacja medyczna prowadzona przez podmiot wykonujący działalność leczniczą może być udostępniona także szkole wyższej lub instytutowi badawczemu do wykorzystania w celach naukowych, bez ujawniania nazwiska i innych danych umożliwiających identyfikację osoby, której dokumentacja dotyczy. W tym przypadku ustawodawca posłużył się zwrotem „może być udostępniona”, co sugeruje, że placówka medyczna wcale nie ma obowiązku jej udostępnienia. Dostęp może uzyskać tylko stosunkowo wąski krąg podmiotów – szkoły wyższe lub instytuty badacze,

co wyklucza możliwość udostępnienia danych innym podmiotom zainteresowanym dostępem do anonimowych danych. Nie jest do końca jasne, jak należy rozumieć cel naukowy - zgodnie z motywem 159 preambuły RODO przetwarzanie danych osobowych do celów badań naukowych „należy interpretować szeroko”, co uzasadniałoby objęcie nim także prac o charakterze badawczo-rozwojowym. Wreszcie, w świetle RODO może powstać zasadnicza wątpliwość, jak rozumieć wymóg przekazania dokumentacji „bez ujawniania nazwiska i innych danych umożliwiających identyfikację osoby, której dokumentacja dotyczy” w świetle zasad anonimizacji i pseudonimizacji (w szczególności obiektywnej i subiektywnej teorii anonimizacji danych) – por. punkt 5.3.5.3 raportu. Wątpliwość ta jest szczególnie istotna - oznacza dla podmiotu udostępniającego zasadnicze ryzyko prawne. Obecne przepisy prawne dotyczące dokumentacji medycznej są też nieprecyzyjne pod kątem udostępniania dokumentacji medycznej do celów naukowych po śmierci pacjenta.

Na innych zasadach następuje dostęp do danych zgromadzonych w rejestrach medycznych w celach naukowych – zgodnie z art. 19 ust. 7 SystInfOchZdrU, dane zawarte w rejestrach medycznych mogą być udostępniane w celu prowadzenia badań naukowych i do celów statystycznych w formie uniemożliwiającej ich powiązanie z konkretną osobą fizyczną. Podobnie więc jak w przypadku art. 26 ust. 4 PrPacjU, ustawodawca nie przesądził, czy chodzi tu o anonimizację czy pseudonimizację. Ustawodawca zapewnił jednak stosunkowo szeroki dostęp do danych, nie ograniczając go do określonej kategorii podmiotów, jak ma to miejsce w przypadku dostępu do dokumentacji medycznej.



### Perspektywa zmian

EHDS w art. 33 wprost wskazuje, że organy ds. dostępu do danych dotyczących zdrowia udzielają dostępu do elektronicznych danych dotyczących zdrowia wyłącznie w przypadku gdy zamierzony cel przetwarzania realizowany przez wnioskodawcę jest zgodny m.in. z działalnością edukacyjną lub dydaktyczną w sektorach ochrony zdrowia lub opieki zdrowotnej, badaniami naukowymi dotyczącymi sektorów ochrony zdrowia lub opieki zdrowotnej, działaniami w zakresie rozwoju i innowacji w odniesieniu do produktów i usług przyczyniających się do ochrony zdrowia publicznego lub zabezpieczenia społecznego lub zapewniających wysoki poziom jakości i bezpieczeństwa opieki zdrowotnej, produktów leczniczych lub wyrobów medycznych, czy też działaniami w zakresie trenowania, testowania i oceny algorytmów, w tym w wyrobach medycznych, systemach sztucznej inteligencji i aplikacjach z zakresu e-zdrowia, przyczyniających się do ochrony zdrowia publicznego lub zabezpieczenia społecznego lub zapewniających wysoki poziom jakości i bezpieczeństwa opieki zdrowotnej, produktów leczniczych lub wyrobów medycznych.

Organy ds. dostępu do danych dotyczących zdrowia przekazują elektroniczne dane dotyczące zdrowia w formie zanonimizowanym, jeżeli takie dane umożliwiają osiągnięcie celu przetwarzania przez użytkownika danych, biorąc pod uwagę informacje przekazane przez użytkownika danych. Jeżeli zanonimizowane dane nie umożliwiają osiągnięcia celu przetwarzania przez użytkownika danych, biorąc pod uwagę informacje przekazane przez użytkownika danych, organy ds. dostępu do danych dotyczących zdrowia udzielają dostępu do elektronicznych danych dotyczących zdrowia w formie spseudonimizowanym. Informacje niezbędne do odwrócenia procesu pseudonimizacji

są dostępne wyłącznie dla organu ds. dostępu do danych dotyczących zdrowia. Użytkownicy danych nie mogą deanonimizować elektronicznych danych dotyczących zdrowia przekazanych im w formie spseudonimizowanym. Nieprzestrzeganie przez użytkownika danych środków zastosowanych przez organ ds. dostępu do danych dotyczących zdrowia w celu zapewnienia pseudonimizacji podlega odpowiednim karom.

Mechanizm umożliwiający dostęp do danych zapewnia też DGA. Jak wskazuje motyw 16. Preambuły do tego aktu, by ułatwiać wykorzystywanie danych będących w posiadaniu podmiotów sektora publicznego do celów badań naukowych i zachęcać do takiego ich wykorzystywania, zachęca się podmioty sektora publicznego do opracowywania zharmonizowanego podejścia i zharmonizowanych procesów na rzecz zapewnienia łatwego dostępu do takich danych do celów badań naukowych leżących w interesie publicznym. Mogłoby to obejmować między innymi opracowywanie sprawnych procedur administracyjnych, normalizację formatowania danych, metadane zawierające informacje w zakresie wyboru metodyki i gromadzenia danych oraz normalizację pól danych, które umożliwiają łatwe łączenie zbiorów danych sektora publicznego pochodzących z różnych źródeł, w zakresie w jakim jest to przydatne do celów analizy. Celem tych praktyk powinno być promowanie wykorzystywania do celów badań naukowych danych sfinansowanych i wytworzonych przez sektor publiczny zgodnie z zasadą „otwarte jak to najbardziej możliwe, zamknięte jak to konieczne”.



### Możliwe działania

Pomimo dyskusyjnej wartości dla celów naukowych obecnie dostępnych danych medycznych zasadne wydaje się doprecyzowanie przesłanek udostępniania dokumentacji medycznej i danych medycznych w celach naukowych tak, by nie budziły one wątpliwości pod kątem RODO, oraz dostosowanie katalogu podmiotów, które mogą ją uzyskać, do rozwiązań wprowadzanych przez DGA oraz EHDS – kluczowy jest cel wykorzystania danych, a nie forma prawna lub charakter wniosku o nie podmiotu, w szczególności w zakresie dostępu do danych anonimowych. W tym zakresie możliwe jest podjęcie działania już teraz, bez czekania na regulację EHDS.

Osobnym zagadnieniem są koszty związane z dokonywaniem operacji anonimizacji i pseudonimizacji danych osobowych. Wraz z planowanym m.in. na gruncie EHDS poszerzeniem obowiązków związanych z udostępnianiem danych w tej postaci podmioty wykonujące działalność leczniczą powinny otrzymać wsparcie organizacyjne niezbędne do ich realizacji, np. dostęp do rozwiązań IT lub środki na ich zakup. Wspomniane podmioty powinny mieć również zagwarantowaną możliwość pobierania opłaty niezbędnej do pokrycia kosztów administracyjnych takiego procesu (podobnie jak przy wydawaniu kolejnych kopii dokumentacji medycznej). Podobne rozwiązanie przewiduje projektowany art. 42 EHDS, zgodnie z którym posiadacze danych mogą pobierać opłaty za udostępnianie elektronicznych danych dotyczących zdrowia na potrzeby wtórnego wykorzystywania.



Obecnie obowiązujące regulacje prawne nie zostały dostosowane do standardów wynikających z RODO, w szczególności nie jest jasne, czy wymagają anonimizacji czy pseudonimizacji danych medycznych, co stanowi istotne ryzyko prawne dla udostępniających placówek. W przypadku dokumentacji medycznej zawężenie podmiotów uprawnionych do otrzymania „anonimowej” dokumentacji jest nieproporcjonalne do potencjalnych korzyści społecznych, które mogą wyniknąć z jej wykorzystania. Podobnego ograniczenia nie przewidują np. zasady dostępu do danych zgromadzonych w rejestrach medycznych. O ile rzeczywiście pewne wątpliwości z obawy o nadużycia może budzić przyznanie zbyt łatwego i powszechnego dostępu do danych zgromadzonych w dokumentacji medycznej każdemu zainteresowanemu, o tyle stosowanie wyłącznie kryterium podmiotowego jako zabezpieczenia jest nieadekwatne. Pożądany standard, który przewiduje EHDS, z powodzeniem może być znacznie szybciej zaimplementowany w krajowym systemie prawnym.

Sygnalizowane kierunki zmian mają na celu zwiększenie dostępu do zbiorów danych, które mogą być wykorzystywane przez lekarzy (i nie tylko) w celach naukowych lub badawczo-rozwojowych. Dane te służyć będą m.in. rozwojowi innowacyjnych produktów i usług oraz projektowaniu polityki publicznej w obszarze ochrony zdrowia, co oznacza potencjalnie pośrednie korzyści dla pacjentów, lekarzy i innych osób wykonujących zawody medyczne – dostęp do nowych narzędzi i skuteczniejszą organizację systemu.

Propozycja wpisuje się w postulat dotyczący celów naukowych i rozwojowych - lekarz powinien móc wykorzystać dane medyczne w celach naukowych i badawczych. W wielu przypadkach wystarczający będzie dostęp do danych anonimowych, co wymaga jasnego odróżnienia tych danych oraz wypracowania różnych ścieżek dostępu.

### 5.3.6.2 Ryzyka na gruncie RODO

**Stan obecny.** Przetwarzanie danych medycznych w celach naukowych, prowadzenia prac badawczo-rozwojowych oraz w związku z rozwijaniem i wykorzystaniem algorytmów AI wiąże się z wyzwaniami w świetle podstawowych zasad RODO. Pierwsze z nich związane jest z zasadą przejrzystości przetwarzania. Przetwarzanie danych medycznych w ramach prowadzenia prac badawczo-rozwojowych i przez rozwiązania AI może być mało przejrzyste (np. tzw. black box problem) i w związku z tym może powodować trudności z wykonaniem obowiązków informacyjnych. Kolejne wyzwanie dotyczy określenia zakresu przetwarzania – tworzenie dużych zbiorów danych, w szczególności z uwagi na uwarunkowania technologiczne związane z rozwojem algorytmów AI, może utrudniać ocenę proporcjonalności przetwarzania tych danych i spełnienia związanych z tym wymogów.

Kolejne wyzwanie dotyczy określenia zakresu przetwarzania – tworzenie dużych zbiorów danych, w szczególności z uwagi na uwarunkowania technologiczne związane z rozwojem algorytmów AI, może utrudniać ocenę proporcjonalności przetwarzania tych danych i spełnienia związanych z tym wymogów.

Trzecie dotyczy dalszego przetwarzania i możliwej zmiany celu przetwarzania danych – jako że rozwiązania AI polegają na zdolności do adaptacji w zależności od dostarczanych danych i procesu uczenia maszynowego, w celu zachowania przydatności danych niezbędne może okazać się dalsze przetwarzanie danych, którego dopuszczalność uwarunkowana jest spełnieniem przesłanek wskazanych w RODO.

W kontekście wykorzystywania danych w celach poznawczych i rozwojowych ważne jest dalsze przetwarzanie danych medycznych, które jest dopuszczalne bez zgody podmiotu danych, pod warunkiem spełnienia przesłanek, o których mowa w art. 6 ust. 4 RODO, tj. stwierdzenia zgodności celu dalszego przetwarzania i celu pierwotnego przetwarzania (test zgodności). Instytucja dalszego przetwarzania jest istotna w przypadku przetwarzania danych medycznych w celu prowadzenia badań naukowych, ponieważ umożliwiłaby realizację interesu publicznego w postaci rozwoju medycyny i sektora ochrony zdrowia przy jednoczesnym zapewnieniu odpowiedniego poziomu ochrony danych osobowych. Do tej pory dalsze przetwarzanie danych medycznych budzi jednak szereg wątpliwości interpretacyjnych, które zniechęcają do jego stosowania.

W związku z powyższymi najczęstszymi podstawami przetwarzania danych medycznych w celach naukowych lub prowadzenia prac badawczo-rozwojowych, w tym w celu rozwoju algorytmów AI, są art. 9 ust. 2 lit. a RODO, czyli wyraźna zgoda podmiotu danych, a także art. 9 ust. 2 lit. j RODO, czyli niezbędność przetwarzania do celów badań naukowych, na podstawie prawa Unii lub prawa państwa członkowskiego. Oparcie się na ww. podstawach wiąże się jednak z pewnymi wyzwaniami. W przypadku zgody dużym utrudnieniem mogą być względy organizacyjne, w tym spełnienie obowiązków informacyjnych. W przypadku celu naukowego wątpliwości interpretacyjne dotyczą adekwatnych standardów ochrony danych przewidzianych w przepisach krajowych.



### Perspektywa zmian

Sygnalizowane wyzwania związane z RODO nie są w wyraźny sposób adresowane przez planowane zmiany prawne. System obiegu danych wynikający z EHDS, DGA i DA będzie opierał się bezpośrednio na przepisach prawa, a część kwestii związanych z wykorzystywaniem danych adresować będzie AI Act.

Wyzwanie związane z dalszym przetwarzaniem w dużej mierze zaadresowane zostanie przez DGA oraz EHDS, które tworzą system wtórnego wykorzystywania danych. W szczególności EHDS wskazuje w art. 33 zakres danych możliwych do wykorzystania oraz w art. 34 cele, dla których elektroniczne dane dotyczące zdrowia mogą być przetwarzane do wtórnego wykorzystywania.

W kontekście właściwych podstaw prawnych dobrym przykładem może być BadKlinU. Dzięki stosownej regulacji ustawowej możliwe stało się odstępianie od czysto biurokratycznego wymogu uzyskiwania zgody na przetwarzanie danych osobowych uczestników badań klinicznych (obok świadomej zgody na udział w badaniu, której towarzyszy m.in. informacja o zasadach przetwarzania danych podczas badania).



## Możliwe działania

Już obecnie, jak i w niedalekiej przyszłości, gdy zostaną przyjęte wszystkie planowane zmiany prawne, zasadne jest opracowanie wytycznych, które udzielać będą praktycznych wskazówek - jak dokładnie należy postępować przy przetwarzaniu danych medycznych w celach naukowych i badawczych, tj. jakie podstawy stosować i jakie wymogi spełnić. Przyczyni się do to ograniczenia ryzyka interpretacyjnego. Uzasadnione jest także stworzenie kodeksu branżowego z art. 40 RODO lub wypracowanie wytycznych przez PUODO określających zasady dotyczące przetwarzania danych o stanie zdrowia w celach badań naukowych.

Zasadne jest ponadto utworzenie spójnych ram prawnych dotyczących przetwarzania danych osobowych w celach badawczych na poziomie krajowym, by poszerzyć możliwość wykorzystywania jako podstawy prawnej art. 9 ust. 2 lit. j RODO, czyli niezbędność przetwarzania do celów badań naukowych, na podstawie prawa Unii lub prawa państwa członkowskiego.



## Uzasadnienie

Przyjęcie sugerowanych zmian w tym obszarze przełoży się na większy dostęp do danych w celach naukowych. Dla lekarzy, którzy występować będą w roli badaczy, oznacza to większe bezpieczeństwo prawne. Pozostali lekarze odnieść mogą pośrednie korzyści związane z rozwojem innowacyjnych narzędzi dzięki wykorzystywaniu tak uzyskiwanych danych.

Propozycja wpisuje się w postulat dotyczący celów naukowych i rozwojowych - lekarz powinien móc wykorzystać dane medyczne w celach naukowych i badawczych. Niejasne przepisy i związane z tym ryzyko nie powinno być czynnikiem zniechęcającym.

### 5.3.6.3 Status prawny badacza i podstawa przetwarzania przez niego danych

**Stan obecny.** Lekarze występują w badaniach klinicznych w roli badaczy (w tym głównych badaczy). Na polskim rynku badań klinicznych spotyka się różne modele związane z przetwarzaniem danych osobowych, w których badacz uznawany jest za niezależnego od sponsora administratora danych, współadministratora lub podmiot przetwarzający (tzw. procesora). Wybór określonego z nich zależy m.in. od faktycznej roli badacza przy opracowywaniu i realizacji badania.

Jak wskazała EROD, jeżeli badacz i sponsor decydują się wspólnie rozpocząć badanie kliniczne, współpracują ze sobą przy opracowywaniu protokołu badania (tj. celu, metodologii, projektu badania, gromadzonych danych, kryteriów wykluczenia i włączenia uczestników, ponownego wykorzystania bazy danych w stosownych przypadkach itp.), to mogą być uważani za współadministratorów w tym badaniu klinicznym, ponieważ wspólnie określają i uzgadniają ten sam cel i podstawowe sposoby przetwarzania<sup>104</sup>. W ocenie EROD w przypadku, gdy badacz nie uczestniczy w sporządzaniu protokołu (po prostu akceptuje protokół już opracowany przez sponsora), a protokół został opracowany wyłącznie przez sponsora, badacza należy traktować jako podmiot przetwarzający, a sponsora jako administratora w tym badaniu klinicznym.

104. Wytyczne Europejskiej Rady Ochrony Danych 07/2020 dotyczące pojęć administratora i podmiotu przetwarzającego zawartych w RODO; 2021 r. str. 40

Powyższe rozróżnienie ma kluczowe znaczenie pod kątem właściwych podstaw przetwarzania danych przez badacza. W przypadku, w którym występuje on jako procesor, zawarta musi zostać z nim umowa powierzenia przetwarzania danych, która legitymizować będzie ten proces. Jeżeli badacz występuje jako administrator lub współadministrator, musi wykazać odpowiednią podstawę przetwarzania. W tym zakresie BadKlinU wprowadziła kluczową zmianę - poprzez uchylenie obowiązku zbierania zgody uczestnika na przetwarzanie jego danych osobowych umożliwiła stosowanie innych podstaw przetwarzania z art. 9 ust. 2 RODO, w tym art. 9 ust. 2 lit. j RODO, czyli przesłankę niezbędności przetwarzania do celów badań naukowych, która pozwala na zachowanie większej spójności z zasadami prowadzenia badań klinicznych.



### Perspektywa zmian

Nie są planowane obecnie żadne zmiany prawne, które w istotny sposób wpłynęłyby na powyżej przedstawiony stan rzeczy. Rozporządzenie 536/2014 oraz przyjęta w tym roku BadKlinU wprowadziły istotną reformę, która z uwagi na nowatorskość wprowadzanych rozwiązań wciąż może budzić wątpliwości interpretacyjne.



### Możliwe działania

Mając na uwadze różnorodną praktykę związaną z ochroną danych osobowych w badania klinicznych, warto opracować wytyczne, które jasno wskazywać będą, przy spełnieniu jakich konkretnie warunków lekarz jako badacz powinien pełnić rolę niezależnego od sponsora administratora danych, współadministratora lub podmiotu przetwarzającego. Wytyczne powinny też wskazywać, jakie mogą być podstawy prawne przetwarzania danych przez badacza będącego administratorem lub współadministratorem danych. W tym zakresie pożądana jest współpraca pomiędzy Agencją Badań Klinicznych oraz Urzędem Ochrony Danych Osobowych.



### Uzasadnienie

Przyjęcie powyższych wytycznych służyć będzie standaryzacji postępowania w tym zakresie, co ograniczy szereg potencjalnych wątpliwości interpretacyjnych. Oznacza to o wiele większe bezpieczeństwo prawne lekarza jako badacza.

Propozycja wpisuje się w postulat dotyczący celów naukowych i rozwojowych - lekarz powinien móc wykorzystać dane medyczne w celach naukowych i badawczych. Niejasne przepisy i związane z tym ryzyko nie powinno być czynnikiem zniechęcającym.

### 5.3.6 Dopuszczalność ograniczenia RODO

**Stan obecny.** Zgodnie z art. 8 ust. 1 BadKlinU, przy realizacji badań klinicznych będących badaniami naukowymi dopuszcza się ograniczenie stosowania wskazanych w tym przepisie regulacji RODO tylko jeżeli jest prawdopodobne, że prawa określone w tych regulacjach uniemożliwią lub poważnie utrudnią realizację celów badania klinicznego będącego badaniem naukowym, a jednocześnie ograniczenia te są konieczne do realizacji tych celów. Przywołana regulacja jest postawą do ograniczenia zastosowania przepisów art. 15, art. 16, art. 18 i art. 21 RODO, czyli przepisów dotyczących prawa dostępu do danych osobowych osoby, której dane dotyczą, prawa do sprostowania danych, prawa do ograniczenia przetwarzania oraz prawa do wniesienia sprzeciwu. Zastosowanie art. 15 RODO może zostać ograniczone do czasu zakończenia badania klinicznego, a zastosowanie art. 16, art. 18 i art. 21 RODO może obejmować także okres po zakończeniu badania. badania, gromadzonych danych, kryteriów wykluczenia i włączenia uczestników, ponownego wykorzystania bazy danych w stosownych przypadkach itp.), to mogą być uważani za współadministratorów w tym badaniu klinicznym, ponieważ wspólnie określają i uzgadniają ten sam cel i podstawowe sposoby przetwarzania<sup>104</sup>. W ocenie EROD w przypadku, gdy badacz nie uczestniczy w sporządzaniu protokołu (po prostu akceptuje protokół już opracowany przez sponsora), a protokół został opracowany wyłącznie przez sponsora, badacza należy traktować jako podmiot przetwarzający, a sponsora jako administratora w tym badaniu klinicznym.



#### Perspektywa zmian

Zmiany wpływające na powyższy zakres nie są planowane.



#### Możliwe działania

W celu popularyzacji możliwości przewidzianych przez art. 8 BadKlinU warto wydać oficjalne wytyczne jak w praktyce należy stosować przywołane ograniczenia, tj. wskazać, kto i kiedy podejmuje decyzję o ich zastosowaniu i co dokładnie powinno jej towarzyszyć, np. przeprowadzenie oceny skutków przetwarzania.



#### Uzasadnienie

Wskazane rozwiązanie wciąż jest pewną nowością w dotychczasowych zasadach prowadzenia badań klinicznych. Aby ograniczyć pojawiające się wątpliwości związane z jego stosowaniem warto z góry je zidentyfikować oraz wyjaśnić. Zwiększy to poziom bezpieczeństwa prawnego lekarza jako badacza.

Propozycja wpisuje się w postulat dotyczący celów naukowych i rozwojowych - lekarz powinien móc wykorzystać dane medyczne w celach naukowych i badawczych. Niejasne przepisy i związane z tym ryzyko nie powinno być czynnikiem zniechęcającym.



