



Biobanki i dane medyczne w erze sztucznej inteligencji, Big Data i medycyny personalizowanej

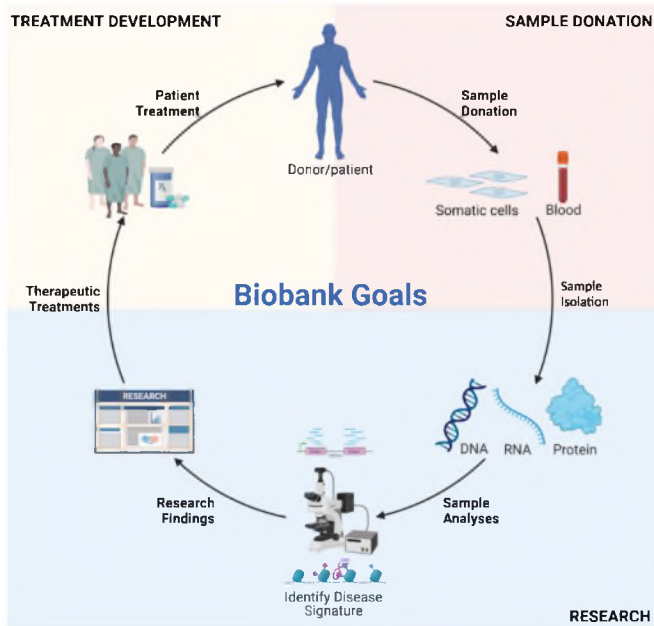
Dr Agnieszka Matera-Witkiewicz, Prof. UMW

**European, Middle Eastern & African Society for Biopreservation and Biobanking
Wroclaw Medical University Biobank**

Nowa era badań biomedycznych-biobanki i ich rola

Dostępność do dużych zbiorów próbek z dobrze opisanymi danymi

Przechowywanie w bezpiecznych i kontrolowanych warunkach



Zapewnienie bezpieczeństwa etyczno-prawnego



ANALIZY Big Data



Computational Intelligence: AI/ML/ANN



MEDYCINA TRANSLACYJNA



MEDYCINA PERSONALIZOWANA

Próbki i dane o odpowiedniej jakości-powtarzalność i odtwarzalność badań

Biobank

~~Banki tkanek i komórek; wytwórnice; laboratoria przeprowadzające analizy dotyczące wytwarzania żywności/pasz i/lub zastosowania terapeutycznego~~

ISO 20387 Biotechnology – Biobanking- General requirements for biobanking (3.5):

Podmiot prawny lub część podmiotu prawnego, który wykonuje **proces biobankowania - proces nabywania** (czynności związane z uzyskaniem i/lub przechowywaniem materiału biologicznego i/lub związanych z tym danych) **oraz przechowywania**, wraz z niektórymi lub wszystkimi działaniami związanymi ze **zbieraniem, przygotowywaniem, przechowywaniem, testowaniem, analizowaniem i dystrybucją** określonego materiału biologicznego, jak również związanych z tym informacji i danych

(ISO 20387; Standardy Jakości dla Biobanków Polskich v.2.00)



Biobanki

kluczowe narzędzie dla szerokiego zakresu nauk biomedycznych

BIOBANKI służą dwóm równoległym celom:

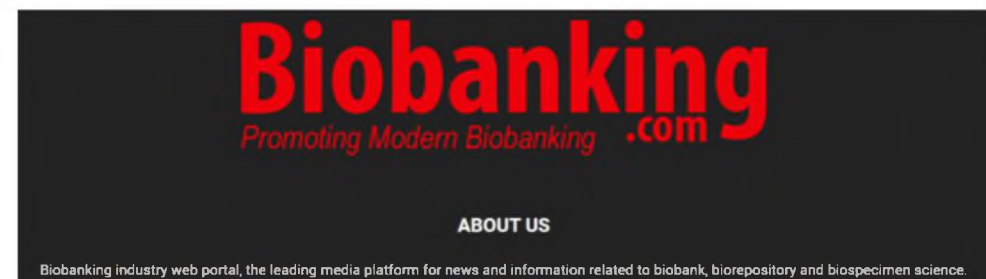
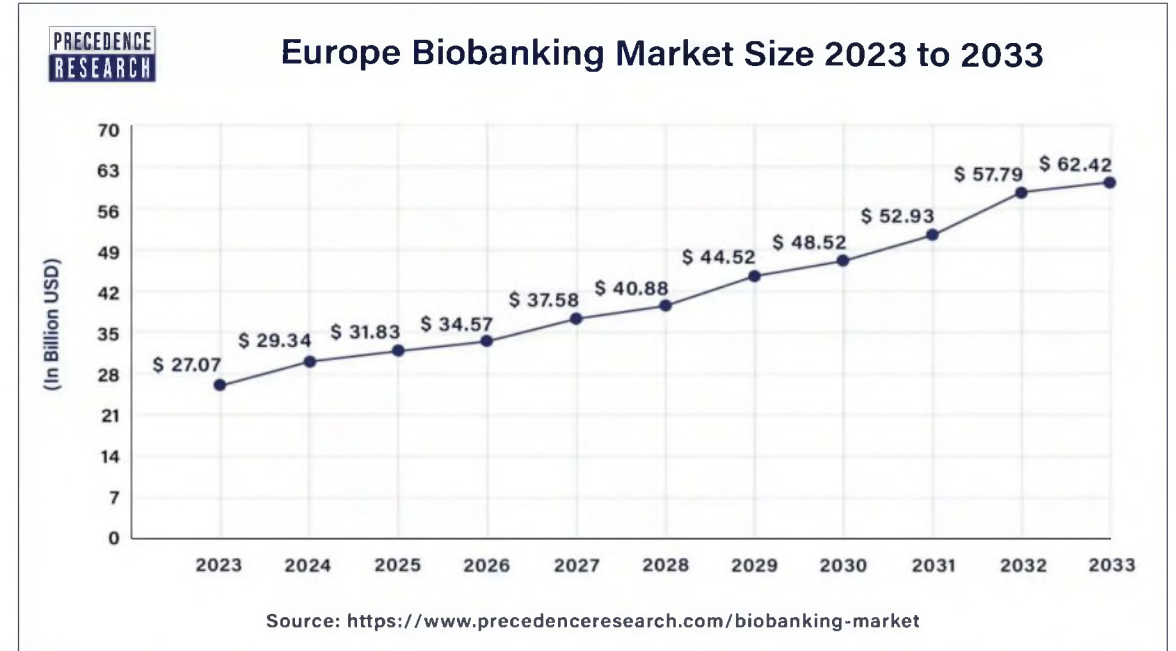
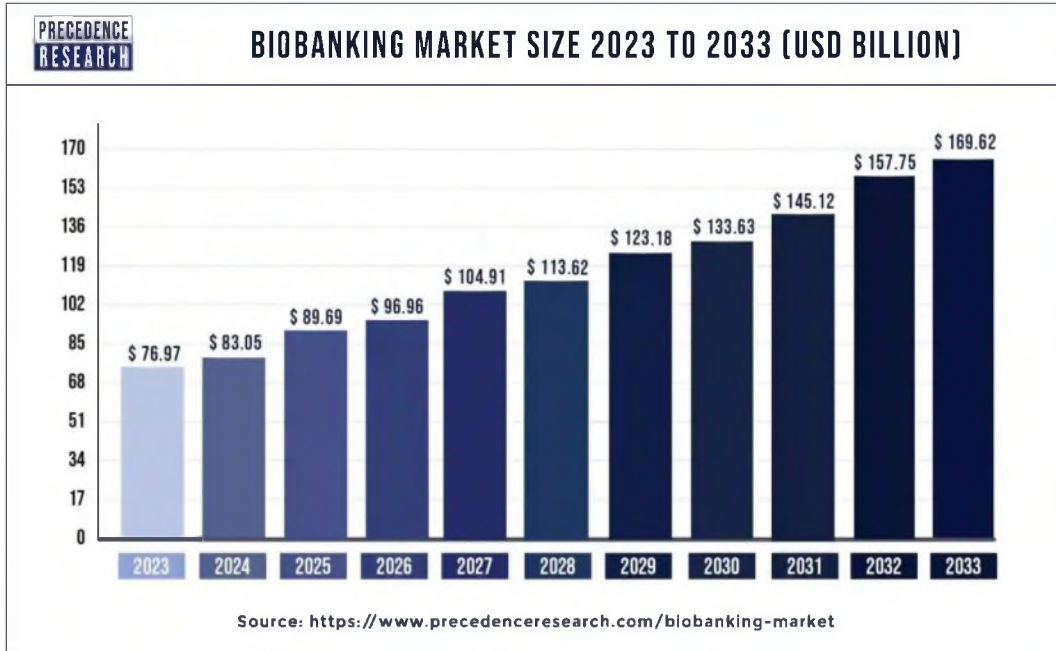
zapewniają infrastrukturę badawczą

umożliwiająca lepsze zrozumienie/badanie różnorodności molekularnej chorób, określenie nowych celów interwencji terapeutycznej czy poszukiwania/oceny biomarkerów

otwierają drogę do wprowadzenia do praktyki klinicznej dopasowanych, spersonalizowanych terapii, dzięki przechowywaniu próbek

i danych pacjenta w warunkach nadzorowanych

Globalny rynek Biobanków został wyceniony na 76,97 miliarda USD w 2023 roku i oczekuje się, że osiągnie około 169,62 miliarda USD do 2033 roku, rosnąc w tempie 8,26% w latach 2024-2033!



Biobanki- inicjatywy międzynarodowe



Towarzystwo zajmujące się promowaniem biobankowania w krajach EMEA

- identyfikacja wyzwań w obszarze biobankowania
- promowanie i wspieranie odpowiednich standardów w biobankowaniu
- zapewnienie silnego, zjednoczonego głosu środowiska biobanków celem wpływania na światowy rozwój obszaru
- Współpraca ze środowiskiem i organizacjami zaangażowanymi lub związanymi z biobankowaniem
- Promowanie i zachęcanie do multidyscyplinarnej współpracy między biobankami, środowiskami badawczymi i innymi kluczowymi zainteresowanymi stronami
- Promowanie wielostronnego wsparcia dla inicjatywy biobankowania
- **Oferta szkoleniowa: JAKOŚĆ, ELSI&GDPR, ACADEMIC&INDUSTRY COOPERATION, SUSTAINABILITY**



Infrastruktura powołana na rzecz rozwoju biobankowania w Europie

- badawcza infrastruktura biobanków i zasobów biomolekularnych krajów UE
- misją jest zbliżenie wszystkich podmiotów zainteresowanych biobankowaniem – badaczy, przedstawicieli biobanków, przemysłu i pacjentów
- zwiększenie wykorzystania zasobów próbek materiału biologicznego i danych w innowacyjnych badaniach
- wsparcie w zakresie wdrażania i utrzymania systemów zarządzania jakością,
- służy ekspertyzą dotyczącą etycznych, prawnych i społecznych aspektów biobankowania
- Przygotowuje rozwiązania i narzędzia IT dedykowane dla biobanków i badaczy pracujących na próbkach ludzkiego materiału biologicznego
- Zrzesza kraje, nie pojedyncze biobanki



Biobanki i dane medyczne

BBMRI-ERIC's
10-Year Roadmap
for 2025-2035



Biobanking for a
Healthier World

Cel strategiczny: Accelerate datafication to enable trustworthy, fit-for-purpose data for high-quality research

- **Zapewnienie międzynarodowej interoperacyjności i połączenia z (lokalnymi, krajowymi i międzynarodowymi) ekosystemami danych medycznych oraz z rejestrami (human and non-human)**
- **Zaadresowanie kwestii ELSI „danyfikacji” poprzez monitorowanie wdrożenia i tworzenia wytycznych dot. etycznego (np. zaufana sztuczna inteligencja) oraz prawnego podejścia w medycynie (np. AI Act, EHDS, IVDR/MDR); kształtowanie polityk i wytycznych na poziomie krajowym/UE**
- **Dostosowanie i połączenie usług związanych z danymi z innych ESFRI oraz europejskimi przestrzeniami danych: EHDS, EOSC, UNCAN.eu, EUCAIM, GDI.**
- **Umożliwienie generowania danych „on-demand”, które obejmą łatwo dostępne zanonimizowane zasoby danych (w tym opracowywanie metod AI/ML, narzędzi do anonimizacji danych, oraz do oceny ryzyka związanego z prywatnością)**

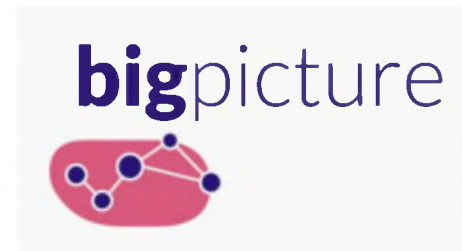


Głównym celem jest **ułatwienie korzystania z kolekcji próbek i danych**,
udostępnianie ich podmiotom zewnętrznym oraz wspieranie wysokiej jakości
badań z zakresu biomedycyny

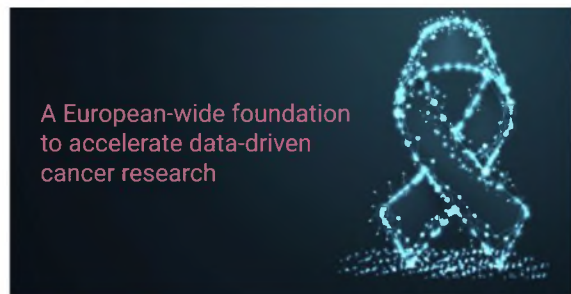
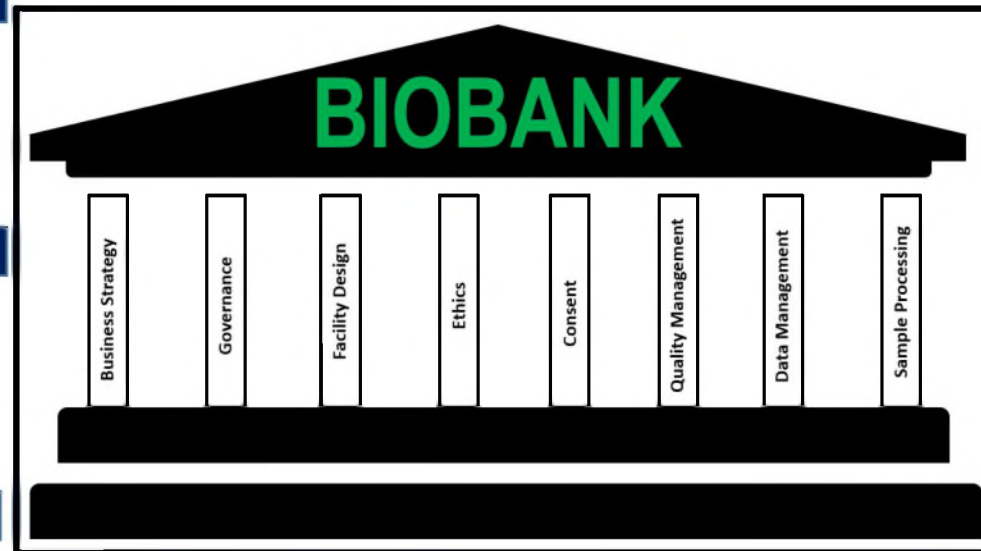
Promowanie multidyscyplinarnej współpracy pomiędzy biobankami, badaczami
oraz innymi kluczowymi zainteresowanymi stronami **w celach naukowych**

Dane w biobankach/Projekty na danych





EUROPEAN GENOME-PHENOME ARCHIVE



cancer



KONSORCJUM BBMRI.PL

UTWORZENIE POLSKIEJ SIECI BIOBANKÓW



Kolekcje w Polskiej Sieci Biobanków

dane - wejściowe pacjentów (informacje kliniczne i epidemiologiczne)

krew

dane - wyniki analiz

kwasy nukleinowe

komórki

wydzieliny/wydaliny

tkanki

utrwalony materiał histologiczny

narządy i ich fragmenty

szpik kostny

patogeny/mikroorganizmy/bezkręgowce

wyzolowane substancje biologicznie czynne (np. białka)

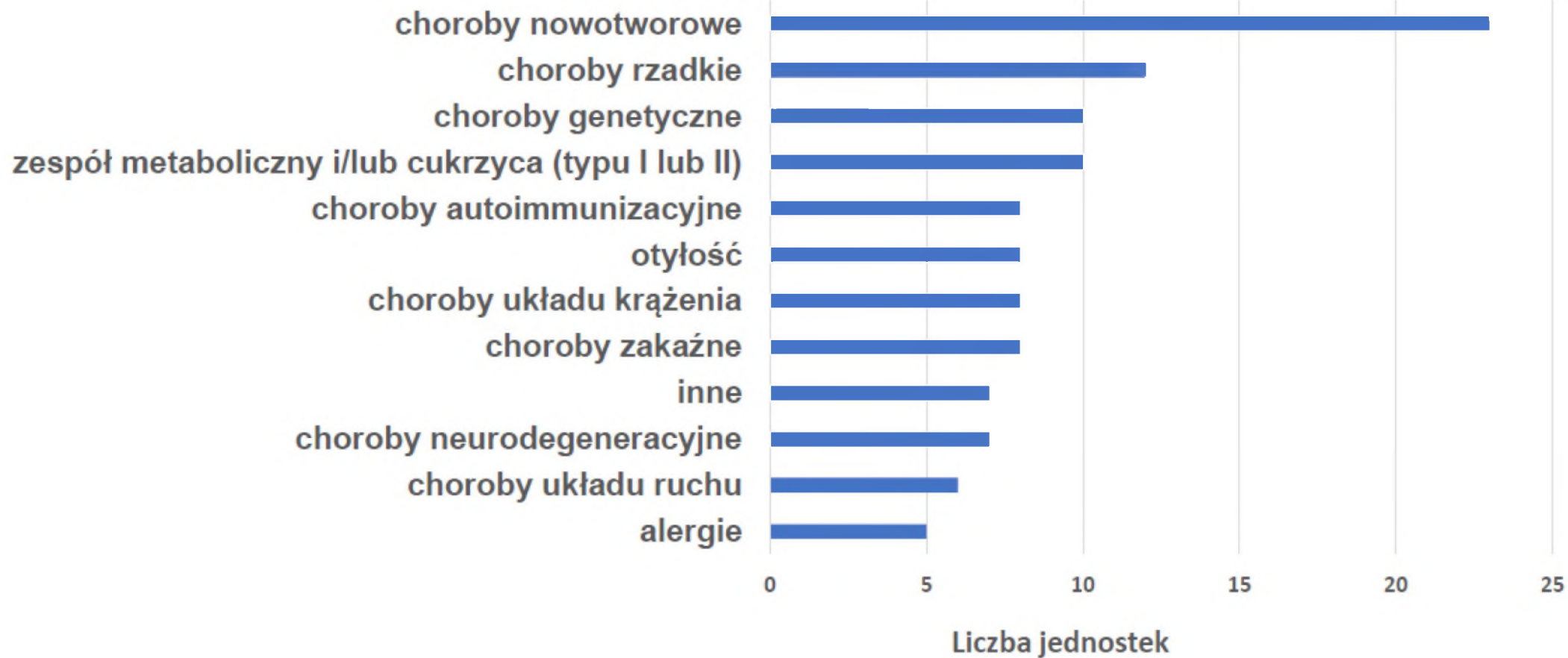
inne



0 10 20 30 40

Liczba jednostek

Choroby leżące w kręgu zainteresowań polskich biobanków



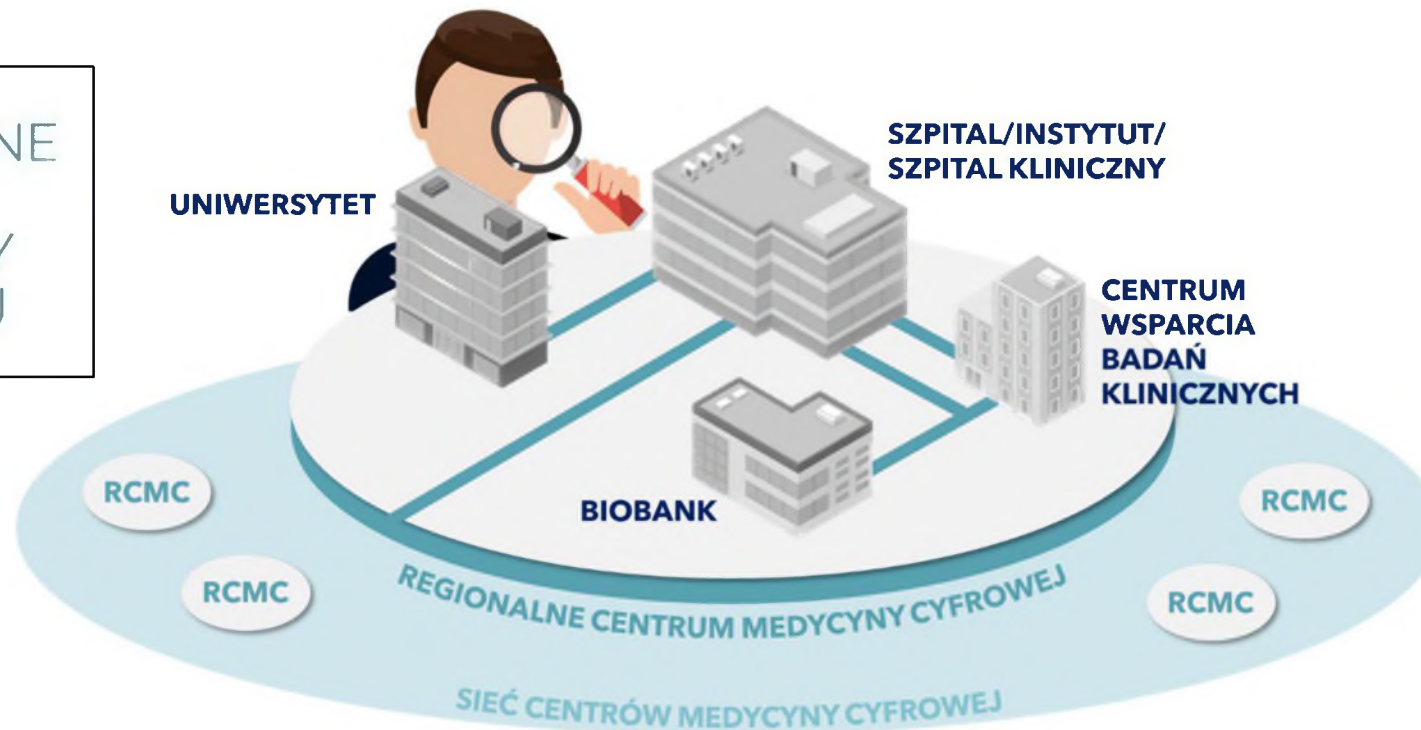
Regionalne Centra Medycyny Cyfrowej (RCMC)

będą strukturami łączącymi bazy danych uniwersytetów, szpitali klinicznych, Biobanków i innych możliwych źródeł

Celem powstania Regionalnych Centrów Medycyny Cyfrowej jest **standaryzacja pozyskiwania i przetwarzania wysokiej jakości Danych medycznych do celów naukowych** oraz **zapewnienie możliwości bezpiecznej wymiany** ustrukturyzowanych danych

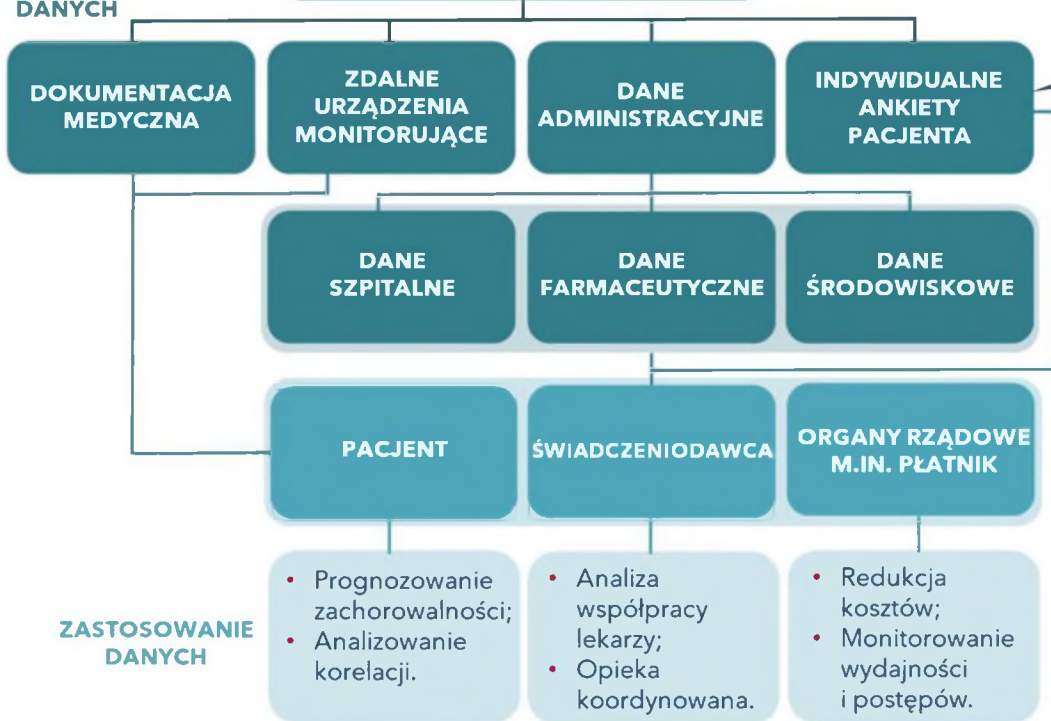


REGIONALNE
CENTRUM
MEDYCYNY
CYFROWEJ



ŹRÓDŁA DANYCH

ZBIÓR DANYCH ZDROWOTNYCH

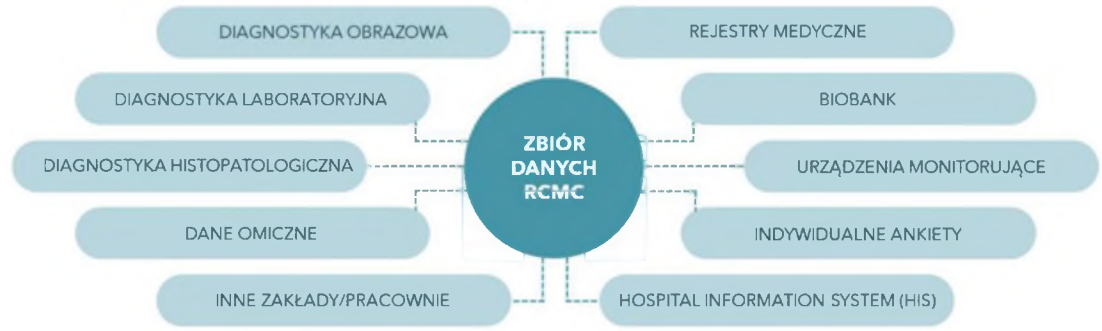


ZASTOSOWANIE DANYCH

- Prognozowanie zachorowalności;
• Analizowanie korelacji.
- Analiza współpracy lekarzy;
• Opieka koordynowana.
- Redukcja kosztów;
• Monitorowanie wydajności i postępów.

Centrum Wsparcia Badań Klinicznych

(Case Report Form – eCRF)



RCMC = Mini EHDS?
EHDS = total RCMC na Europę?

DANE W BIOBANKU



Dane związane z uczestnikiem badania,
w tym jego dane medyczne oraz dane naukowe wygenerowane z próbki

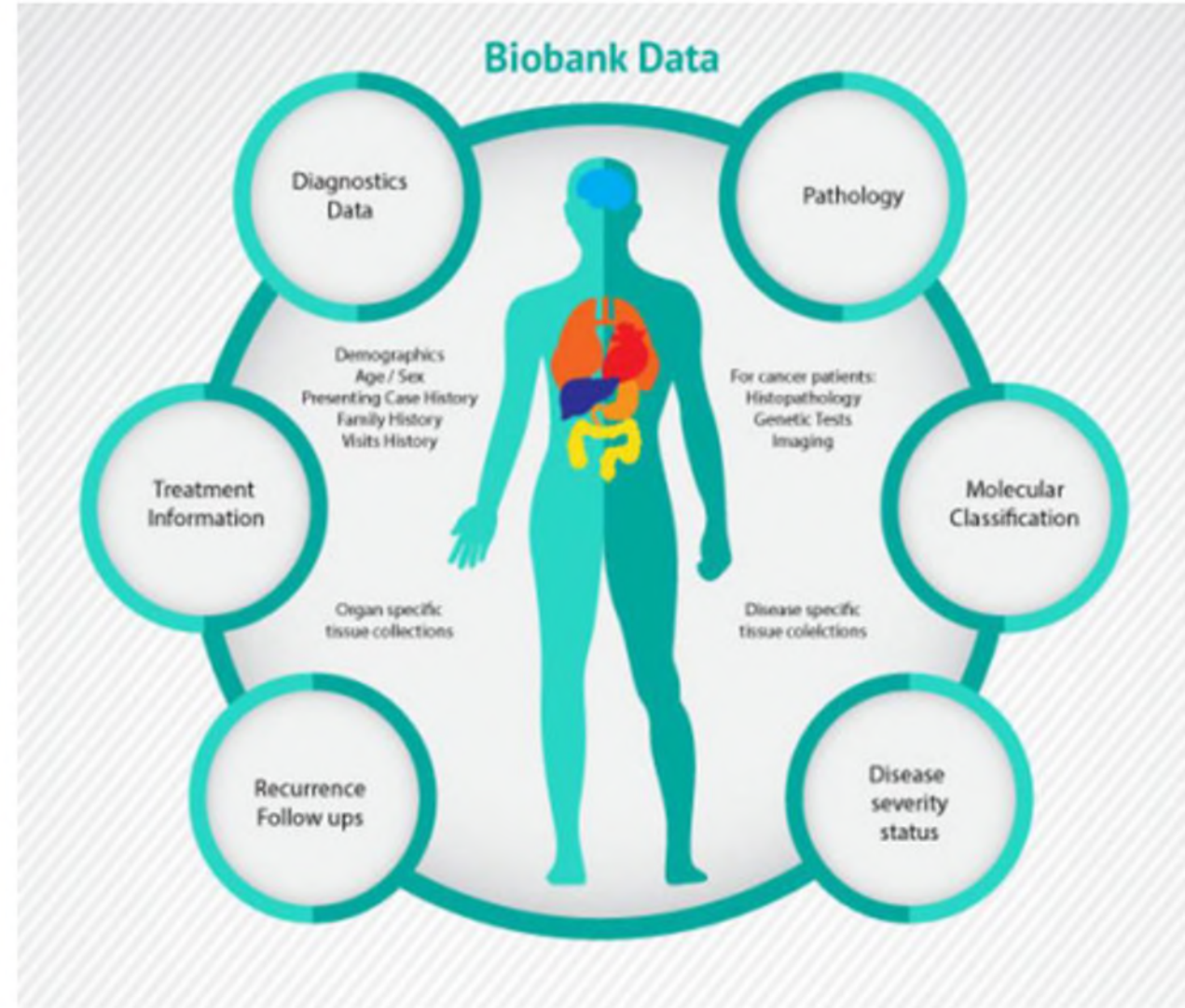
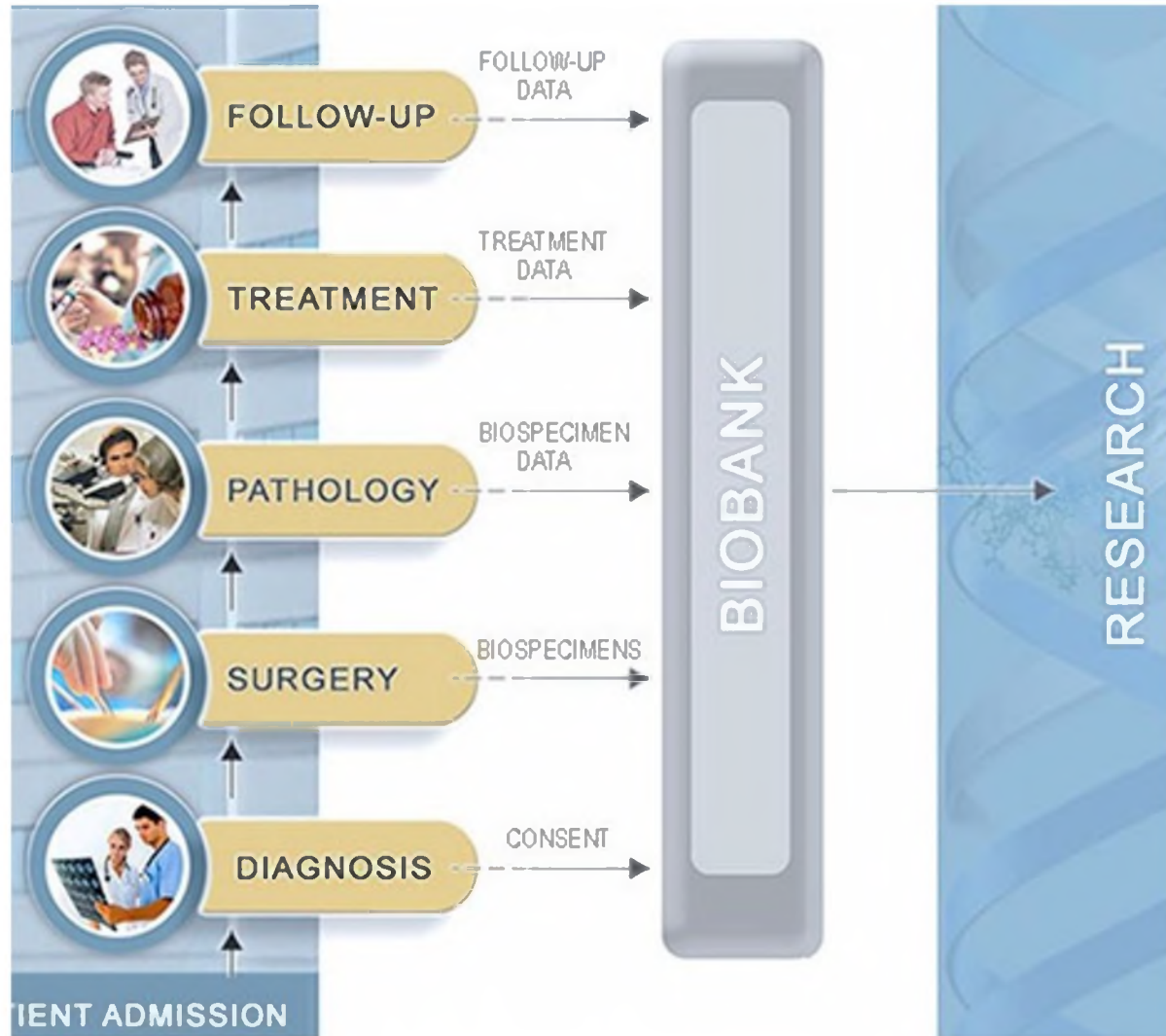


Dane wynikające z dopełnienia obowiązku zabezpieczenia praw uczestnika badania



Dane z procesów przedanalizacyjnych/dane z procesów biobankowania

DANE MEDYCZNE W BIOBANKU



RYZYKA DLA UCZESTNIKA BADANIA W BIOBANKU

- **przy pobieraniu próbek**- nie powstaje żadne dodatkowe ryzyko medyczne poza ryzykiem związanym ze zwykłym pobraniem materiału jak przy standardowym pobraniu do badań

- **przy wykorzystaniu próbek**- gromadzenie i przechowywanie próbek **wiąże się z gromadzeniem i przetwarzaniem danych osobowych oraz danych o stanie zdrowia**-danych wrażliwych

W jaki sposób biobanki mogą zmniejszyć ryzyko naruszenia dóbr osobistych uczestnika badania?

Regulacje prawne, wytyczne i standardy dla obszaru biobankowania



Brak dedykowanych aktów prawnych!!



DOBROWOLNE !!



1. Ustawa o ochronie danych osobowych
2. **Bezpieczny i nadzorowany dostęp** do próbek i danych – wykluczający nadużycia
3. **Stosowanie systemów anonimizacji/pseudonimizacji/ocena DPIA**
4. **Komisja bioetyczna**-pozytywne opinie na konkretne badanie/biobankowanie?
5. **Świadoma zgoda uczestnika badania/Informacja o projekcie**
6. **Ochrona prywatności uczestnika badania** - rozdzielenie informacji pozwalających na jego identyfikację (nazwisko oraz pesel) od pozostałych danych (np. demograficznych, antropometrycznych, wyników badań...)
7. **Zabezpieczenie danych przed utratą** (przypadkową lub hackerską), kopie zapasowe
8. **Standardy bezpieczeństwa i procedury systemowe dot. bezpieczeństwa- wymagania systemów dedykowanych biobankowaniu**

BRAK DEDYKOWANEJ USTAWY O BIOBANKOWANIU





BBMRI-ERIC®

The European research infrastructure for biobanking and biomolecular resources in health and life sciences

STANDARDS FOR BIOMEDICAL RESEARCH

EXAMPLES

- ISO 20387:2018 Biobanking – Requirements for biobanking
- ISO 15189:2012 Medical laboratories – Requirements for quality and competence
- ISO 17025:2005 General requirements for the competence of testing and calibration laboratories
- ISO 17020:2012 Conformity assessment – Requirements for the operation of various types of bodies performing inspections
- ISO/TS 20658:2017 Medical laboratories — Requirements for collection, transport, receipt, and handling of samples
- ISO 9001:2015 Quality management systems Requirements
- ISO 19011:2011 Guidelines for auditing management systems
- And others... search www.iso.org, www.cen.eu, www.bbmri-eric.eu/services/standardisation/

INTEGRATED MANAGEMENT

SYSTEMS (IMS)

ISO 9001:2015
QUALITY MANAGEMENT
SYSTEMS -
REQUIREMENTS

CEN/TS – ISO
PRE-EXAMINATION
SAMPLE HANDLING

ISO 20387:2018
GENERAL
REQUIREMENTS FOR
BIOBANKING

IMS
COMBINES MULTIPLE
MANAGEMENT SYSTEM
STANDARDS

ISO 15189:2015
MEDICAL
LABORATORIES
REQUIREMENTS FOR
QUALITY AND
COMPETENCE

How to operate a biobank sustainably successfully: OM in Biobanking,
January 27, 2020_DK



Standardy Jakości dla Biobanków Polskich

Standardy jakości dla biobanków polskich v. 2.00

pod redakcją

Agnieszki Matera-Witkiewicz
Joanny Gleńskiej-Olender
Karoliny Zagórskiej
Izabeli Uhrynowskiej-Tyszkiewicz
Małgorzaty Witoń

Spis treści

Wstęp 7

Recenzje 8

1. Zarządzanie organizacją/instytucją 10
 2. Zarządzanie jakością 16
 3. Dokumentacja i zapisy 22
 4. Zarządzanie zasobami ludzkimi 40
 5. Aspekty etyczne i prawne 50
 6. Dostawy, gospodarka materiałami 72
 7. Urządzenia w Biobanku 80
 8. Identyfikowalność 102
 9. Higiena środowiska i pracownika 112
 10. Procesy technologiczne i kontrola jakości procesów technologicznych 132
 11. Odchylenia, niezgodny produkt, dane bądź usługa 146
 12. Audyty 154
 13. Doskonalenie 164
 14. Współpraca naukowa 172
 15. Bezpieczeństwo 178
- Piśmiennictwo 181
Słownik 183

Agnieszka Matera-Witkiewicz
Joanna Gleńska-Olender
Izabela Uhrynowska-Tyszkiewicz
Małgorzata Witoń · Karolina Zagórska

Manual of Biobank Quality Management

Standardy i kodeks dedykowane biobankowaniu w Polsce

Standardy jakości dla biobanków polskich v. 2.00

pod redakcją

Agnieszki Matery-Witkiewicz
Joanny Głębskiej-Oleander
Karoliny Zagórskiej
Izabelli Uhrynowskiej-Tyszkiewicz
Małgorzaty Witoń

15

15.	Bezpieczeństwo	181
15.1.	Procedury bezpieczeństwa	181
15.2.	Bezpieczeństwo materiału biologicznego	182
15.3.	Bezpieczeństwo informacji	182
15.4.	Podstawowe metody zabezpieczania infrastruktury IT i przetwarzania danych	186
15.4.1.	Świadomość funkcjonowania Biobanku w organizacji	186
15.4.2.	Ogólne zasady bezpiecznej wymiany informacji	186
15.4.3.	Bezpieczeństwo przetwarzanych danych	187
15.4.4.	Podstawowe metody zabezpieczania dostępu do pomieszczeń	188
15.4.5.	Systemy operacyjne i oprogramowanie	188
15.4.6.	Oprogramowanie antywirusowe	189
15.4.7.	Zarządzanie użytkownikami i hasłami	189
15.4.8.	Sieć LAN	189
15.4.9.	Zasilanie awaryjne	190
15.4.10.	Podstawowe cechy systemu informatycznego Biobanku	190
15.4.11.	Kopie bezpieczeństwa	191
15.4.12.	Usługi zewnętrzne, w tym przetwarzanie danych w chmurze	192
15.4.13.	Personel	193

1.	CEL KODEKSU	6
2.	DEFINICJE	6
3.	ZASADY PRZETWARZANIA DANYCH OSOBOWYCH I INNYCH DANYCH OSOBOWYCH SZCZEGÓLNYCH KATEGORII (DANYCH WRAZLIWYCH) DLA CELÓW BADAŃ NAUKOWYCH	9
4.	ZGODA OSOBY, KTÓREJ DANE DOTYCZĄ, NA PRZETWARZANIE DANYCH DLA CELÓW NAUKOWYCH	13
5.	WTÓRNE PRZETWARZANIE DANYCH OSOBOWYCH DLA CELÓW BADAŃ NAUKOWYCH	18
5.1.	Wtórne przetwarzanie danych osobowych dla celów badań naukowych	18
5.2.	Wtórne przetwarzanie danych osobowych pochodzących z dokumentacji medycznej	20
6.	PRZETWARZANIE DANYCH ANONIMOWYCH, ZANONIMIZOWANYCH I POCHODZĄCYCH OD OSÓB ZMARŁYCH	21
6.1.	Dane anonimowe i zanonimizowane	22
6.2.	Dane osób zmarłych (motyw 27 preambuły RODO)	22
7.	SPOSOBY OCHRONY DANYCH PRZETWARZANYCH DLA CELÓW NAUKOWYCH	24
7.1.	Zalecenia ogólne	25
7.2.	Zalecenia techniczne służące zapewnieniu bezpieczeństwa danych przetwarzanych przez biobanki	26
8.	PRAWA OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE DLA CELÓW BADAŃ NAUKOWYCH	32
8.1.	Prawo do wycofania zgody i zaprzestania przetwarzania danych	32
8.2.	Prawo do sprostowania danych	33
8.3.	Prawo do informacji o przetwarzanych danych, w tym do informacji istotnych dla zdrowia pacjenta-uczestnika badania wykrytych przypadkowo w trakcie prowadzenia badań (<i>incidental findings</i>)	33
8.4.	Prawo do informacji o skutkach anonimizacji danych	34
8.5.	Prawa osób niezdolnych do wyrażenia zgody	35
8.6.	Prawo do skargi dotyczącej przestępczego postawienia Kodeksu	35
9.	ADMINISTRATOR DANYCH I INSPEKTOR DANYCH	36
10.	OBOWIĄZEK ZGŁASZANIA NARUSZEŃ	37
11.	TRANSGRANICZNA WYMIANA DANYCH	38
12.	LIKwidACJA BIOBANKU	40
13.	PRZYJĘCIE I STOSOWANIE KODEKSU	41
14.	KONTROLA PRZESTRZEGANIA I WSPÓLPRACA NA RZECZ OKRESOWEGO PRZEGLĄDU	

KODEKS POSTĘPOWANIA W SPRAWIE PRZETWARZANIA DANYCH OSOBOWYCH DLA CELÓW BADAŃ NAUKOWYCH PRZEZ BIOBANKI W POLSCE

Przygotowany przez zespół ds. etycznych prawnych i społecznych aspektów biobankowania (ELSI) działający w ramach Konsorcjum BBMRI.pl w związku z realizacją projektu

Utworzenie sieci biobanków w Polsce w obrębie Infrastruktury Badawczej Biobanków i Zasobów Biomolekularnych BBMRI-ERIC

Redakcja

dr hab. Jakub Pawlikowski (UML)

dr Dorota Krekora-Zajac (UW)

mgr Błażej Marciniak (UŁ)

Wersja z dnia 10 grudnia 2020 r.

Wymagania międzynarodowych standardów dedykowanych biobankowaniu w odniesieniu do danych



ISO 20387:2018

Biotechnology — Biobanking — General requirements for biobanking

4. Wymagania ogólne

4.1.1 Biobank powinien **posiadać procedury** dotyczące biobankowania MB i **powiązanych z nim danych**. Obejmuje to procesy **przechowywania, zarządzania danymi, niszczenia**

6.3 Obiekty/dedykowane obszary i warunki środowiskowe

6.3.2 Biobank**powinien określić, kontrolować i utrzymywać obiekty/dedykowane obszary** w celu zapewnienia warunków wymaganych dla zgodności z określonymi kryteriami kontroli jakości (QC). Obejmuje to procedury mające na celu utrzymanie przydatności do zamierzonego celu..... **powiązanych z MB danych**.

6.4 Procesy, wyroby i usługi dostarczane z zewnątrz

6.4.1.4 Biobank powinien zapewnić, aby **procesy, wyroby i usługi dostarczane z zewnątrz nie wpływały negatywnie na zdolność biobanku do ciągłego zabezpieczania i dostarczania****powiązanych danych**

7.3 Przyjęcie i dystrybucja MB i związanych z nim danych

7.3.2.2 Biobank powinien określić **kryteria akceptacji**. Identyfikacja MB i **powiązanych z nim danych powinna być weryfikowana przy nabyciu/przyjęciu** zgodnie z określonymi kryteriami akceptacji.

7.3.3.2 **Przekazując....dane** użytkownikowi spoza biobanku, biobank ma zapewnić, iż **udokumentowana umowa** lub prawnie wiążący dokument (np. umowa, pisemne i podpisane zobowiązanie, wiążąca elektroniczna akceptacja warunków) **przedstawia warunki regulujące zabezpieczenie i wykorzystywanie ... danych.**

8.5. Działania odnoszące się do ryzyk i szans

8.5.2 Biobank powinien opracować, wdrożyć i dokumentować:

b) plan(-y) działania w celu zabezpieczeniadanych w przypadku katastrofy

7.10 Zarządzanie informacją i danymi

7.10.1 Biobank powinien określić **wymagane informacje i dane dotyczące materiału biologicznego oraz posiadać system umożliwiający śledzenie**. Biobank powinien dołożyć wszelkich starań, aby **wspierać interoperacyjność takich informacji i danych**.

7.10.2 Biobank powinien **brać pod uwagę kwestie związane z przyszłym rozszerzeniem swoich możliwości, aby pozwolić na dalsze dodawanie i/lub przetwarzanie danych** powiązanych z materiałem biologicznym.

7.10.3 Procedura wdrażania, modyfikacji i użytkowania oprogramowania systemu komputerowego, sprzętu komputerowego i baz danych powinna być wdrożona, gdy są one wykorzystywane do biobankowania. Procedura ta **powinna obejmować co najmniej integralność danych, środki kontroli bezpieczeństwa i system tworzenia kopii zapasowych zapobiegający utracie lub uszkodzeniu danych**.

7.10.5 Zaleca się, aby **biobank zapewnił zainteresowanym stronom dostęp do katalogu dostępnego MB i powiązanych z nim danych**.

7.10.6 Biobank powinien **utrzymać dostęp do odpowiednich danych powiązanych z materiałem biologicznym, w zakresie niezbędnym do celów badawczych**.

Wymagania międzynarodowych standardów dedykowanych danym



ISO/IEC 27001:2022

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

**SYSTEM ZARZĄDZANIA
BEZPIECZEŃSTWEM INFORMACJI**

- ✓ spełnienie wymagań prawnych,
- ✓ stały nadzór nad procesami przetwarzania informacji,
- ✓ wzrost świadomości i standaryzacja postępowania pracowników odnośnie bezpieczeństwa informacji,
- ✓ zmniejszenie ryzyka utraty danych, kradzieży sprzętu i włamań do systemów informatycznych,
- ✓ minimalizowanie negatywnych skutków naruszeń bezpieczeństwa,
- ✓ cykliczną weryfikację stosowanych zabezpieczeń,
- ✓ odpowiednią identyfikację zagrożeń związanych z bezpieczeństwem informacji i zmniejszenie ich wpływu na działalność biobanku,
- ✓ zachowanie poufności, integralności i dostępności informacji,
- ✓ możliwość zapewnienia ciągłości działania organizacji w sytuacji kryzysowej

Biobanki i mechanizm dzielenia się danymi badawczymi

- zawsze w oparciu o **zgode uczestnika badania**
- zgodnie z *Ustawą z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystaniu informacji sektora publicznego*
- na warunkach zapewniających **maksymalne bezpieczeństwo osób fizycznych/zastosowanie co najmniej pseudonimizacji**
- zgodne z polityką Państwa i EU na rzecz utworzenia **European Open Science Cloud, Programem Otwierania Danych na lata 2021-2027**
- Zgodnie z ideą otwartych danych badawczych „**otwarte w największym możliwym zakresie, zamknięte tylko na tyle ile to konieczne**”
- **zgodnie z zasadą FAIR (F – Findable – łatwe do odnalezienia i wyszukiwania, A – Accessible – dostępne dla wszystkich zainteresowanych, I – Interoperable – interoperacyjne, realne do zintegrowania/połączenia z innymi zestawami, R – Reusable – możliwość wielokrotnego użycia)**

Obszary wymagające podjęcia działań w zakresie **świadomości** prowadzenia badań z użyciem danych

- **zgoda na użycie danych** w modelach AI/ML, ANN?- czy potrzebna/czy odrębna klauzula, a może wystarczy informacja o wykorzystaniu danych do badań w obszarze X?
- **brak wiedzy** dotyczącej:
 - ? **sposobu udostępniania danych** (zgoda uczestnika, konieczność zawarcia umowy),
 - ? **zapisy w umowie** (jaki zakres danych, sposób postępowania z danymi, zabezpieczenie danych, rodzaj planowanych analiz, likwidacja danych po analizach, bezpieczna przestrzeń dla prowadzenia analiz, narzędzia użyte do analiz i potencjalne zagrożenie wykorzystania danych do doskonalenia uczenia w ramach stosowania narzędzi bezpłatnych...)
- **konieczność zaangażowania**: KB, IOD, Działów Prawnych
- **standaryzacja danych**
- **umiejętność oszacowania wartości zbioru danych**



Obszary wymagające podjęcia działań w zakresie **świadomości** prowadzenia badań z użyciem danych

1. Wtórne wykorzystanie danych zdrowotnych: dotyczy użycia zakodowanych danych pacjentów do celów badawczych- możliwe zagrożenia:

✓ **Ryzyko odkodowania danych**, szczególnie gdy łączone będą z innymi zbiorami danych

(**przykład:** naukowcy, łącząc dane zdrowotne z danymi geolokalizacyjnymi, byli w stanie zidentyfikować pacjentów w małej społeczności, naruszając ich prywatność)

✓ **Brak jednolitych standardów anonimizacji:** stosowanie różnych metod może skutkować nierównomiernym poziomem ochrony danych

(**przykład:** Dane uczestników badania udostępnione dwóm instytucjom badawczym stosującym różne standardy anonimizacji, co doprowadziło do różnego stopnia ochrony prywatności pacjentów)

✓ **Niezgodność z krajowymi regulacjami:** Różnice w regulacjach ochrony danych między państwami mogą powodować trudności w legalnym i bezpiecznym udostępnianiu danych

(**przykład:** instytucja z kraju A udostępniła dane instytucji z kraju B, gdzie obowiązywały mniej restrykcyjne przepisy dotyczące ochrony danych, prowadząc do niezamierzonego naruszenia prywatności)

✓ **Niejasne umowy regulujące wykorzystanie danych lub ich brak:** Brak precyzyjnych zapisów może doprowadzić do użycia danych w sposób niezgodny z pierwotnym celem

(**przykład:** firma farmaceutyczna, która otrzymała dostęp do danych bez odpowiedniej umowy, wykorzystywała je do celów marketingowych, czego nie przewidywano)

2. Ochrona danych zdrowotnych: Zapewnienie bezpieczeństwa danych zdrowotnych zgodnie z przepisami RODO oraz dodatkowymi standardami ochrony, aby zagwarantować ich poufność, integralność oraz dostępność

✓ **Niewystarczające zabezpieczenia techniczne:** Brak odpowiednich systemów zabezpieczeń może prowadzić do wycieku danych osobowych

Przykład: Instytucja nie stosowała odpowiedniego szyfrowania bazy danych, przez co podczas ataku hakerskiego dane pacjentów zostały skradzione

✓ **Brak procedur postępowania przy naruszeniach bezpieczeństwa danych:** Brak gotowych planów reagowania na incydenty zwiększa ryzyko pogłębienia skutków naruszenia

Przykład: Po wykryciu włamania do systemu informatycznego instytucja nie miała procedury, co spowodowało znaczne opóźnienie w powiadomieniu pacjentów i organów nadzoru, potęgując szkody

✓ **Niejasne zasady dotyczące kasowania i przechowywania danych:** Brak ustalonych procedur kasowania i przechowywania danych po zakończeniu projektów zwiększa ryzyko ich nieautoryzowanego dostępu lub przechowywania ich dłużej niż jest to konieczne.

Przykład: Instytucja badawcza przechowywała dane pacjentów na niechronionym serwerze długo po zakończeniu badań, co doprowadziło do wycieku informacji w wyniku cyberataku.



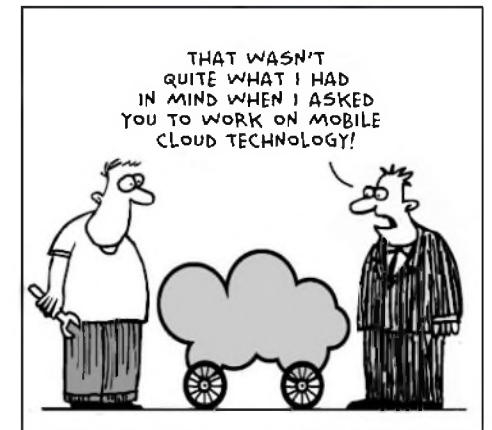
✓ **Brak monitoringu dostępu do danych:** Brak narzędzi monitorujących dostęp do danych utrudnia wykrycie nieuprawnionego dostępu lub nadużyć.

Przykład: Pracownik przez kilka miesięcy miał nieautoryzowany dostęp do danych pacjentów, co zostało wykryte dopiero podczas rutynowego audytu bezpieczeństwa

✓ **Zabezpieczenia urządzeń mobilnych i przenośnych: ryzyko zgubienia lub kradzieży urządzeń zawierających dane medyczne:** Brak odpowiedniego zabezpieczenia tych urządzeń może skutkować utratą poufnych informacji zdrowotnych.

Przykład: Lekarz korzystający z laptopa, na którym znajdowały się niezabezpieczone dane medyczne pacjentów, zgubił sprzęt podczas podróży służbowej, narażając placówkę na poważny wyciek danych.

.....



EHDS, GDPR AND OTHER DATA SECURITY REQUIREMENTS IMPLEMENTATION

