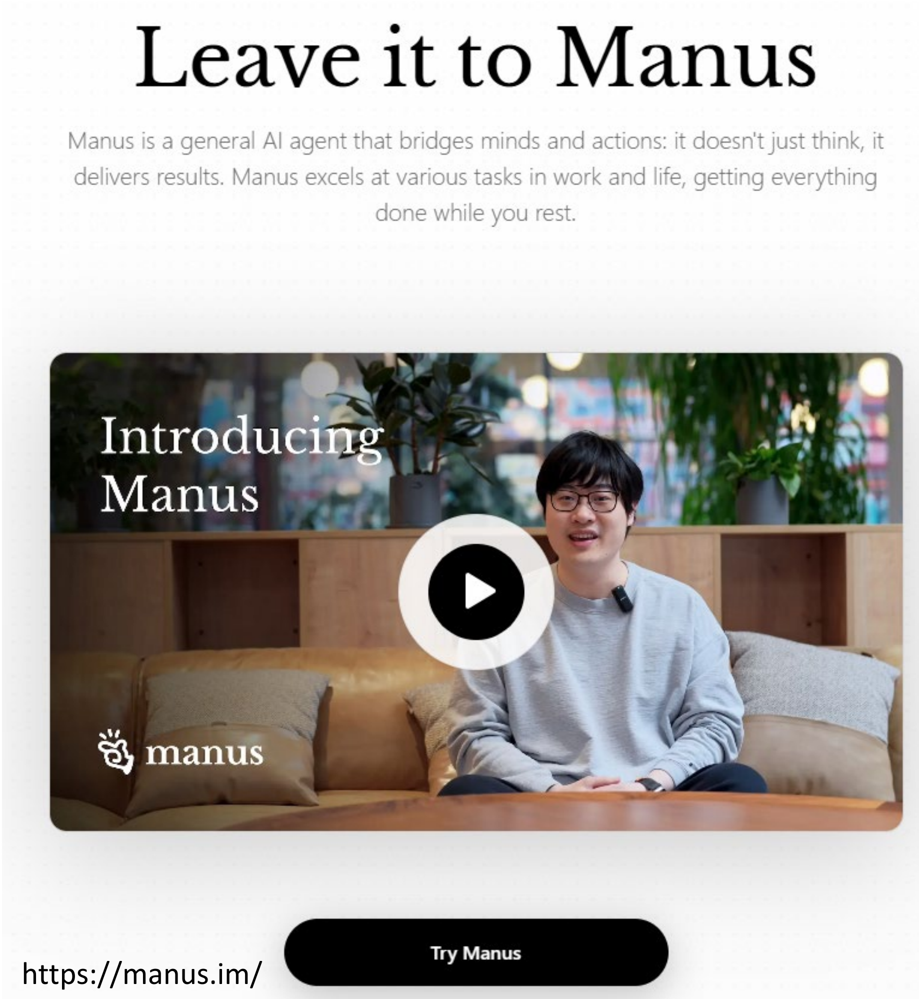
Medical Data Privacy and Ethics in the Age of Artificial Intelligence

Lecture 5: Data Ethics

Zhiyu Wan, PhD (wanzhy@shanghaitech.edu.cn)
Assistant Professor of Biomedical Engineering
ShanghaiTech University

March 7, 2025

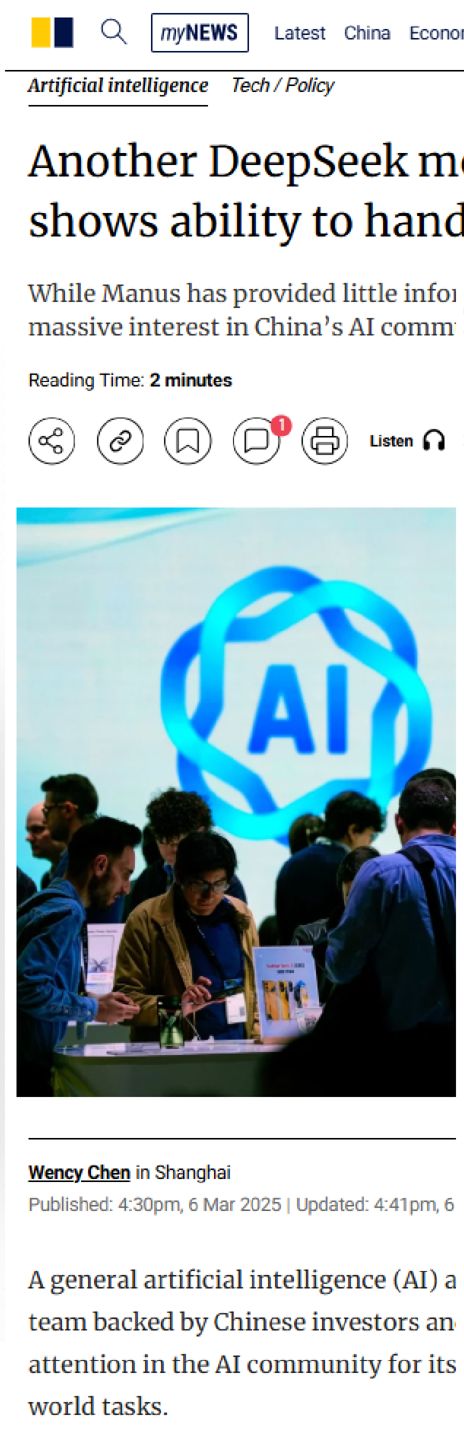
News on AGI



Leave it to Manus

Manus is a general AI agent that bridges minds and actions: it doesn't just think, it delivers results. Manus excels at various tasks in work and life, getting everything done while you rest.

https://manus.im/
https://github.com/mannaandpoem/OpenManus



myNEWS
Latest China Economy HK Asia Business Tech Lifestyle People & Culture Wo - All
Listen

Artificial intelligence *Tech / Policy*

Another DeepSeek moment? General AI agent Manus shows ability to handle complex tasks

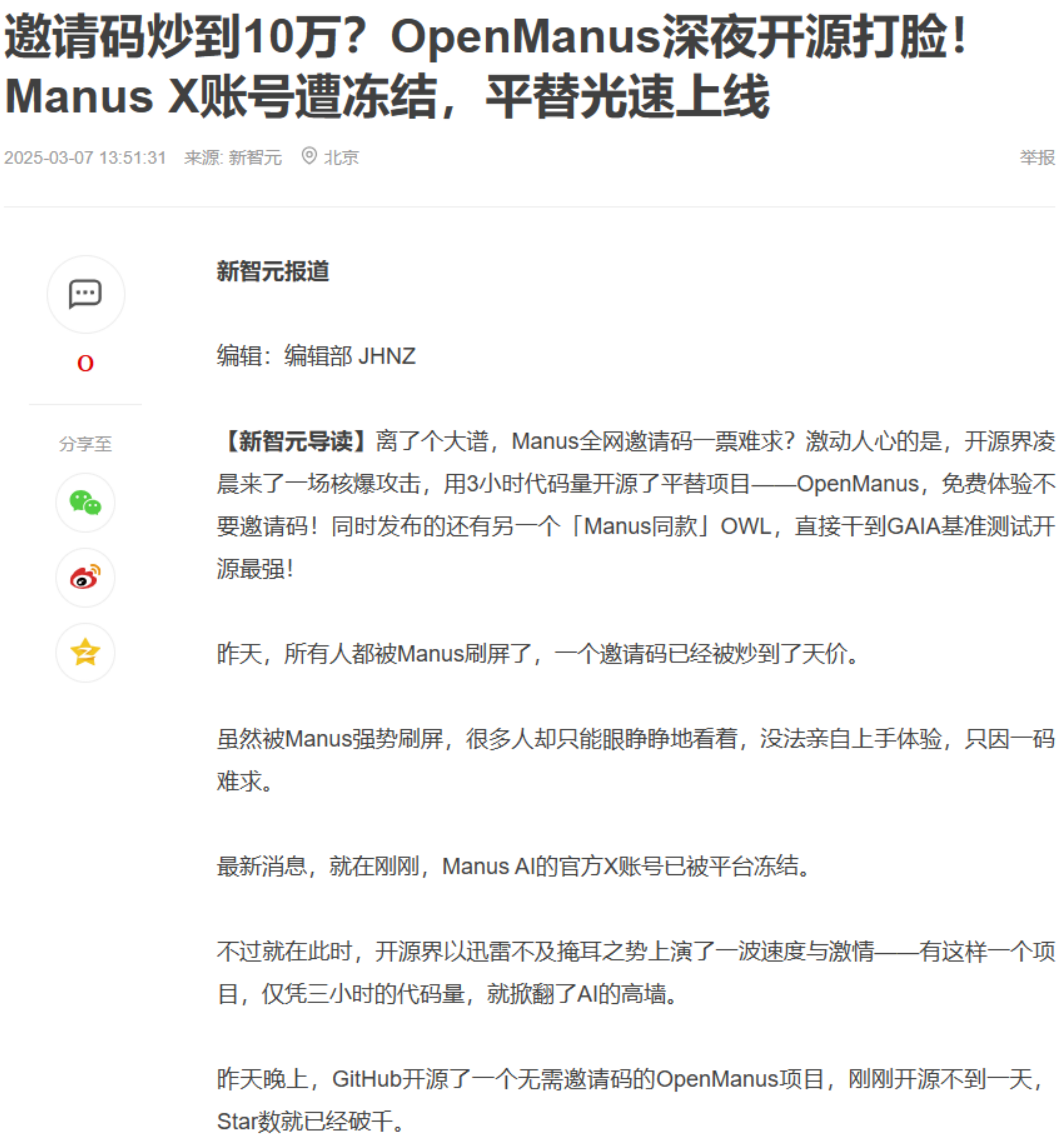
While Manus has provided little infor
massive interest in China's AI comm

Reading Time: **2 minutes**

Wency Chen in Shanghai

Published: 4:30pm, 6 Mar 2025 | Updated: 4:41pm, 6

A general artificial intelligence (AI) a
team backed by Chinese investors an
attention in the AI community for its
world tasks.



邀请码炒到10万？OpenManus深夜开源打脸！Manus X账号遭冻结，平替光速上线

2025-03-07 13:51:31 来源: 新智元 北京 举报

新智元报道

编辑：编辑部 JHNZ

【新智元导读】离了个大谱，Manus全网邀请码一票难求？激动人心的是，开源界凌晨来了一场核爆攻击，用3小时代码量开源了平替项目——OpenManus，免费体验不要邀请码！同时发布的还有另一个「Manus同款」OWL，直接干到GAIA基准测试开源最强！

昨天，所有人都被Manus刷屏了，一个邀请码已经被炒到了天价。

虽然被Manus强势刷屏，很多人却只能眼睁睁地看着，没法亲自上手体验，只因一码难求。

最新消息，就在刚刚，Manus AI的官方X账号已被平台冻结。

不过就在此时，开源界以迅雷不及掩耳之势上演了一波速度与激情——有这样一个项目，仅凭三小时的代码量，就掀翻了AI的高墙。

昨天晚上，GitHub开源了一个无需邀请码的OpenManus项目，刚刚开源不到一天，Star数就已经破千。

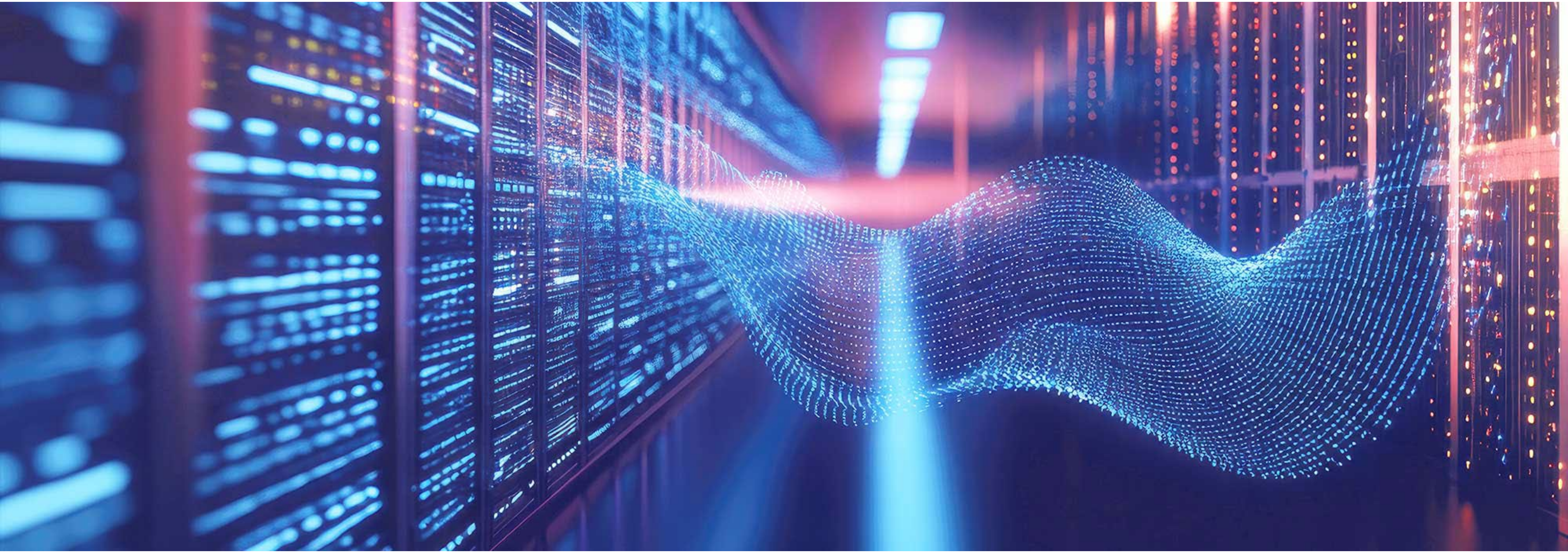
1st Quiz

- Covers lectures 1-3;
- 20 minutes;
- 10 multiple-choice questions; and
- 1 essay question (No word limit. 6 lines recommended. You can use both English (preferred) and Chinese to answer.)

Learning Objectives of This Lecture

- Know five principles for implementing data ethics
- Know five stages of data life cycle

Dataaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa



From Principle to Practice (From Oaths to Checklists)

- UK Government’s Data Ethics Framework
  - Overarching principles
    - Transparency
    - Accountability
    - Fairness
  - Specific actions
    - Define and understand public benefit and user need
    - Involve diverse expertise
    - Comply with the law
    - Review the quality and limitations of the data
    - Evaluate and consider wider policy implications

https://www.gov.uk/government/publications/data-ethics-framework

Five Cs for Implementing the Data Ethics

- Consent
  - Data is frequently collected, used, and sold without consent.
  - **Acxiom, Equifax, Experian, and Transunion**, that collect data to assess financial risk.
  - In Europe, **Google** collected data from cameras mounted on cars to develop new mapping products.
  - **AT&T and Comcast** both used cable set top boxes to collect data about their users.
  - **Samsung** collected voice recordings from TVs that respond to voice commands.

Mike Loukides, Hilary Mason, DJ Patil. *Ethics and Data Science*. O'Reilly Media. 2018. (Ch. 3)

Five Cs for Implementing the Data Ethics

- Clarity
  - Lengthy legal documents
  - Observant readers of **Eventbrite**’s user agreement recently discovered that listing an event gave the company the right to send a video team, and exclusive copyright to the recordings. And the only way to opt out was by writing to the company.
  - Most **Twitter** users know that their public tweets are, in fact, public; but many don’t understand that their tweets can be collected and used for research.
  - Wilbanks’ work helps people understand what happens when they provide sensitive medical and health data to a service. (Multi-media **eConsent**)

1. Mike Loukides, Hilary Mason, DJ Patil. *Ethics and Data Science*. O’Reilly Media. 2018. (Ch. 3)
2. Doerr M, Suver C, Wilbanks J. Developing a transparent, participant-navigated electronic informed consent for mobile-mediated research. Participant-Navigated Electronic Informed Consent for Mobile-Mediated Research (April 22, 2016). 2016 Apr 22.

Five Cs for Implementing the Data Ethics

- Consistency and Trust
  - Customer data was stolen from Yahoo!, Target, Anthem, local hospitals, government data, data brokers like Experian, etc.
  - Cambridge Analytica used Facebook's data to target vulnerable customers with highly specific advertisements.
- Control and Transparency
  - Facebook asks for (but doesn't require) your political views, religious views, and gender preference. What if you change your minds?
  - Europe's General Data Protection Regulation (GDPR) requires users' data to be provided to them at their request and removed from the system if they so desire.

Mike Loukides, Hilary Mason, DJ Patil. *Ethics and Data Science*. O'Reilly Media. 2018. (Ch. 3)

Five Cs for Implementing the Data Ethics

- Consequences
  - The Children’s Online Privacy Protection Act (COPPA) protects children and their data.
  - The Genetic Information Nondiscrimination Act (GINA) was established in 2008 in response to rising fears that genetic testing could be used against a person or their family.
  - In 2006, **AOL** released anonymized search data to researchers, it proved possible to “de-anonymize” the data and identify specific users.
  - In 2018, **Strava** opened up their data to allow users to discover new places to run or bike. Strava didn’t realize that members of the US military were using GPS-enabled wearables, and their activity exposed the locations of bases and patrol routes in Iraq and Afghanistan.

Mike Loukides, Hilary Mason, DJ Patil. *Ethics and Data Science*. O’Reilly Media. 2018. (Ch. 3)

Five Cs for Implementing the Data Ethics

- Consequences
  - Safer open data for public benefit
    - UK Biobank
    - LinkedIn’s Economic Graph project
    - Google Book’s ngram viewer

Mike Loukides, Hilary Mason, DJ Patil. *Ethics and Data Science*. O’Reilly Media. 2018. (Ch. 3)

Ethics and Training

- Software security and ethics
  - SQL injection attacks taught in classes on security instead of software development.
  - **Data ethics** is taught in classes on ethics instead of other courses.
  - Courses in ethics usually helps students **think** seriously about the issues instead of **addressing** the problems such as getting informed consent or protecting privacy in real-world applications.
  - White House report "*Preparing for the Future of Artificial Intelligence*" (October 2016) highlights the need for training in both ethics and security:

Mike Loukides, Hilary Mason, DJ Patil. *Ethics and Data Science*. O'Reilly Media. 2018. (Ch. 3)

Preparing for the Future of Artificial Intelligence

- “Ethical training for AI practitioners and students is a necessary part of the solution. Ideally, every student learning AI, computer science, or data science would be exposed to curriculum and discussion on related **ethics and security topics**. However, ethics alone is not sufficient. Ethics can help practitioners understand their responsibilities to all stakeholders, but **ethical training** should be augmented with **technical tools and methods** for putting good intentions into practice by doing the technical work needed to prevent unacceptable outcomes.”

https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf

Data Lifecycle Management

- The systematic approach to managing data from its creation to its eventual disposal. The lifecycle typically follows these stages:
- **Stages of Data Lifecycle Management:**
  1. **Data Creation & Acquisition:** Data is generated from various sources such as medical records, IoT devices, surveys, or AI models.
  2. **Data Storage & Processing:** Data is stored in databases, cloud environments, or data lakes, where it is cleaned, transformed, and analyzed.
  3. **Data Usage & Sharing:** Data is used for research, analytics, AI training, decision-making, or shared across institutions under governance policies.
  4. **Data Archiving & Retention:** Inactive or old data is moved to long-term storage while ensuring accessibility and compliance with legal retention periods.
  5. **Data Disposal & Deletion:** Data is securely deleted or anonymized when no longer needed, following policies to prevent unauthorized access.

(Assisted by ChatGPT)

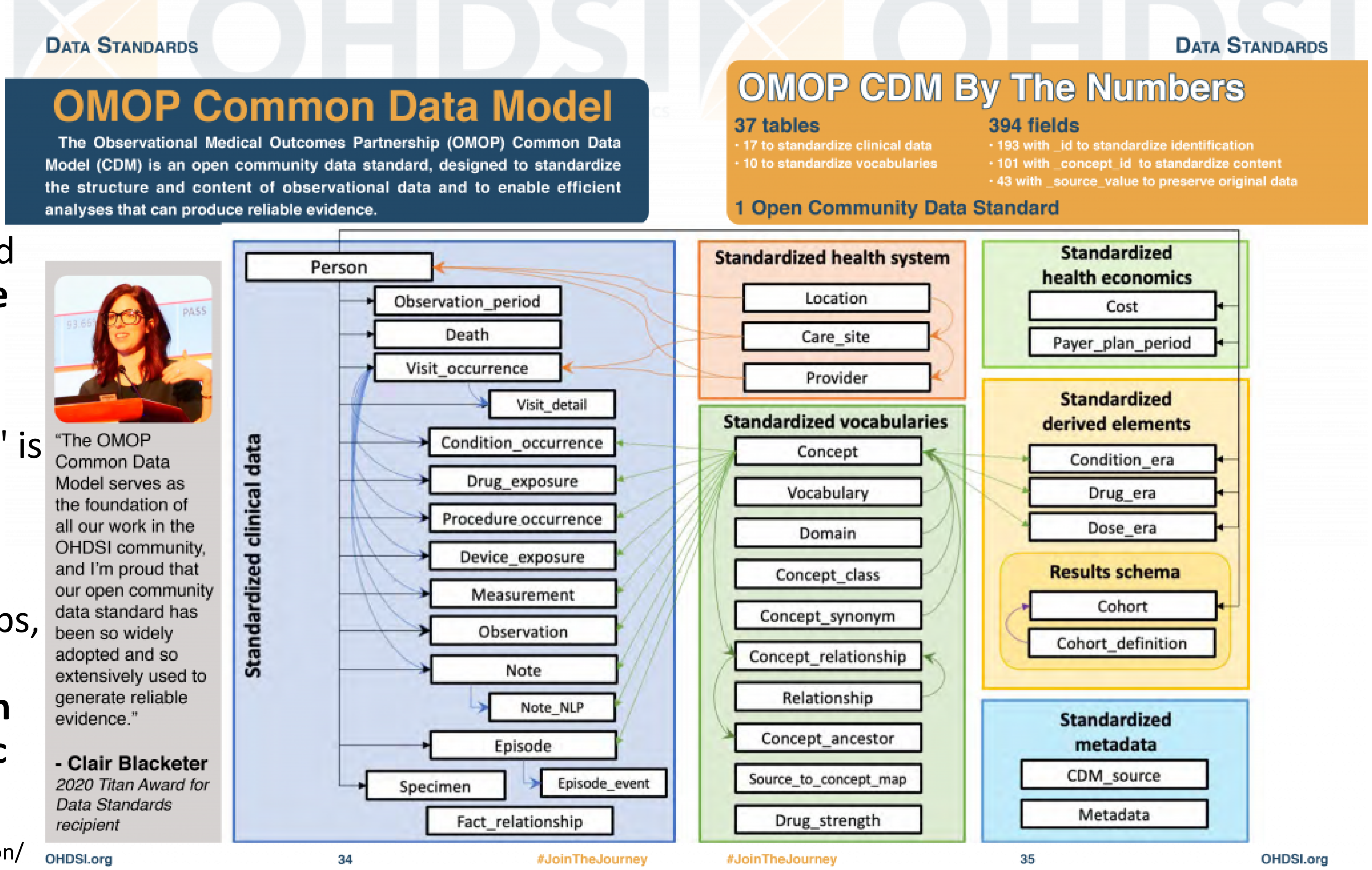
Data Governance

- The framework that ensures the proper management, security, quality, and compliance of data within an organization. It involves policies, procedures, and technologies that oversee data collection, storage, usage, and sharing.
- **Key Components of Data Governance:**
  - **Data Policies & Standards:** Defines guidelines on data handling, storage, access, and security.
  - **Data Quality Management:** Ensures accuracy, completeness, consistency, and reliability of data.
  - **Data Security & Privacy:** Implements access controls, encryption, anonymization, and compliance with regulations like GDPR, HIPAA, and China’s PIPL.
  - **Data Stewardship:** Assigns responsibilities to individuals (data stewards) who oversee data integrity and compliance.
  - **Compliance & Legal Regulations:** Ensures data use aligns with national and international laws.
  - **Data Architecture & Metadata Management:** Organizes and catalogs data for better discoverability and usability. (E.g., International Classification of Diseases (ICD) codes, Observational Medical Outcomes Partnership (OMOP) Common Data Model)

(Assisted by ChatGPT)

Standardized Data: The OMOP Common Data Model

- OMOP can be considered a type of data that can be used to build a **knowledge graph** within the healthcare domain.
- A "knowledge graph" is a broad concept representing a network of entities and their relationships, used to **organize complex information** and **enable semantic querying.**



DATA STANDARDS

OMOP Common Data Model

The Observational Medical Outcomes Partnership (OMOP) Common Data Model (CDM) is an open community data standard, designed to standardize the structure and content of observational data and to enable efficient analyses that can produce reliable evidence.

"The OMOP Common Data Model serves as the foundation of all our work in the OHDSI community, and I'm proud that our open community data standard has been so widely adopted and so extensively used to generate reliable evidence."

- Clair Blacketer
2020 Titan Award for Data Standards recipient

Standardized clinical data: Person, Observation_period, Death, Visit_occurrence, Visit_detail, Condition_occurrence, Drug_exposure, Procedure occurrence, Device_exposure, Measurement, Observation, Note, Note_NLP, Episode, Specimen, Episode_event, Fact_relationship

Standardized health system: Location, Care_site, Provider

Standardized vocabularies: Concept, Vocabulary, Domain, Concept_class, Concept_synonym, Concept_relationship, Relationship, Concept_ancestor, Source_to_concept_map, Drug_strength

Standardized health economics: Cost, Payer_plan_period

Standardized derived elements: Condition_era, Drug_era, Dose_era

Results schema: Cohort, Cohort_definition

Standardized metadata: CDM_source, Metadata

OHDSI.org 34 #JoinTheJourney

DATA STANDARDS

OMOP CDM By The Numbers

37 tables
- 17 to standardize clinical data
- 10 to standardize vocabularies

394 fields
- 193 with _id to standardize identification
- 101 with _concept_id to standardize content
- 43 with _source_value to preserve original data

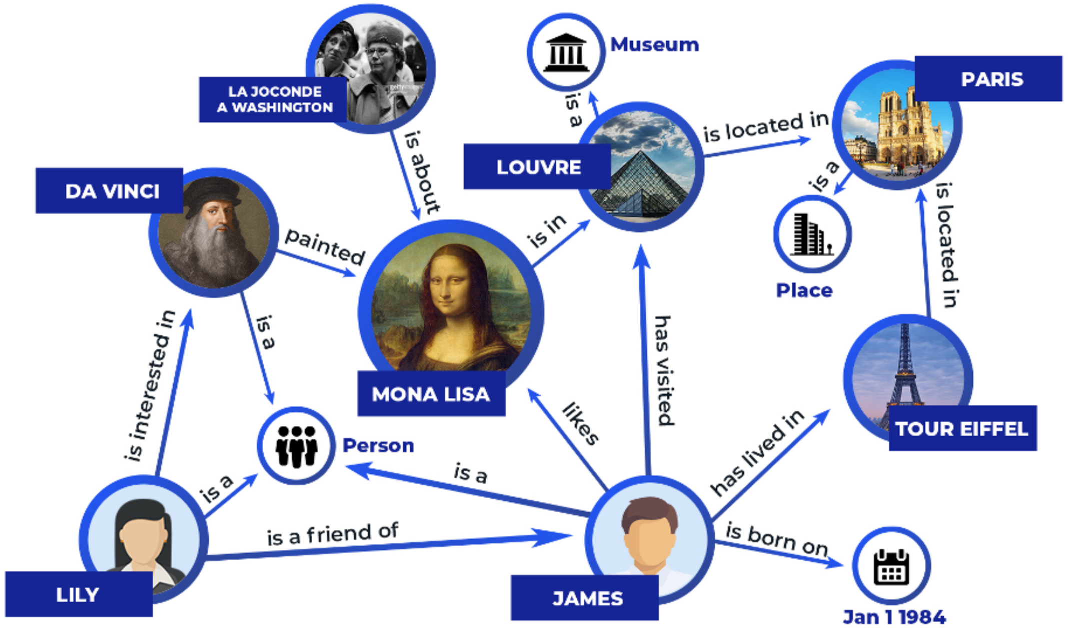
1 Open Community Data Standard

#JoinTheJourney 35 OHDSI.org

https://www.ohdsi.org/data-standardization/

LLMs VS KGs

- Large language models (LLMs) and knowledge graphs (KGs) are both technologies that help machines understand and process information. LLMs are good at **generating human-like text**, while KGs are good at **organizing and structuring data**.



An example of knowledge graph

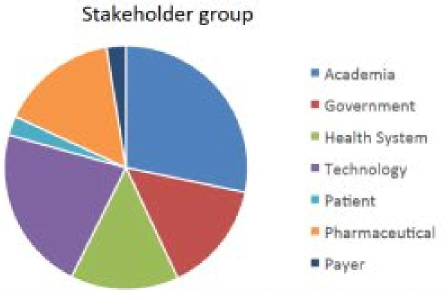
(Assisted by Gemini)

OHDSI

OBSERVATIONAL HEALTH DATA SCIENCES AND INFORMATICS

What OHDSI is:

- ✓ **Open Source**
- ✓ **Community**
- ✓ **Data**



Why Choose OHDSI/OMOP:

- ✓ **Fast, reliable** studies across a series of datasets and data types
- ✓ **Reduced cost of ownership** including understanding coding schemes, writing statistical programs across databases or developing software
- ✓ **Expanded data access** via the OHDSI network and remote multi-center database studies

OHDSI Collaborators:

- 3,758 collaborators
- >1,100 organizations
- 83 countries from 6 continents

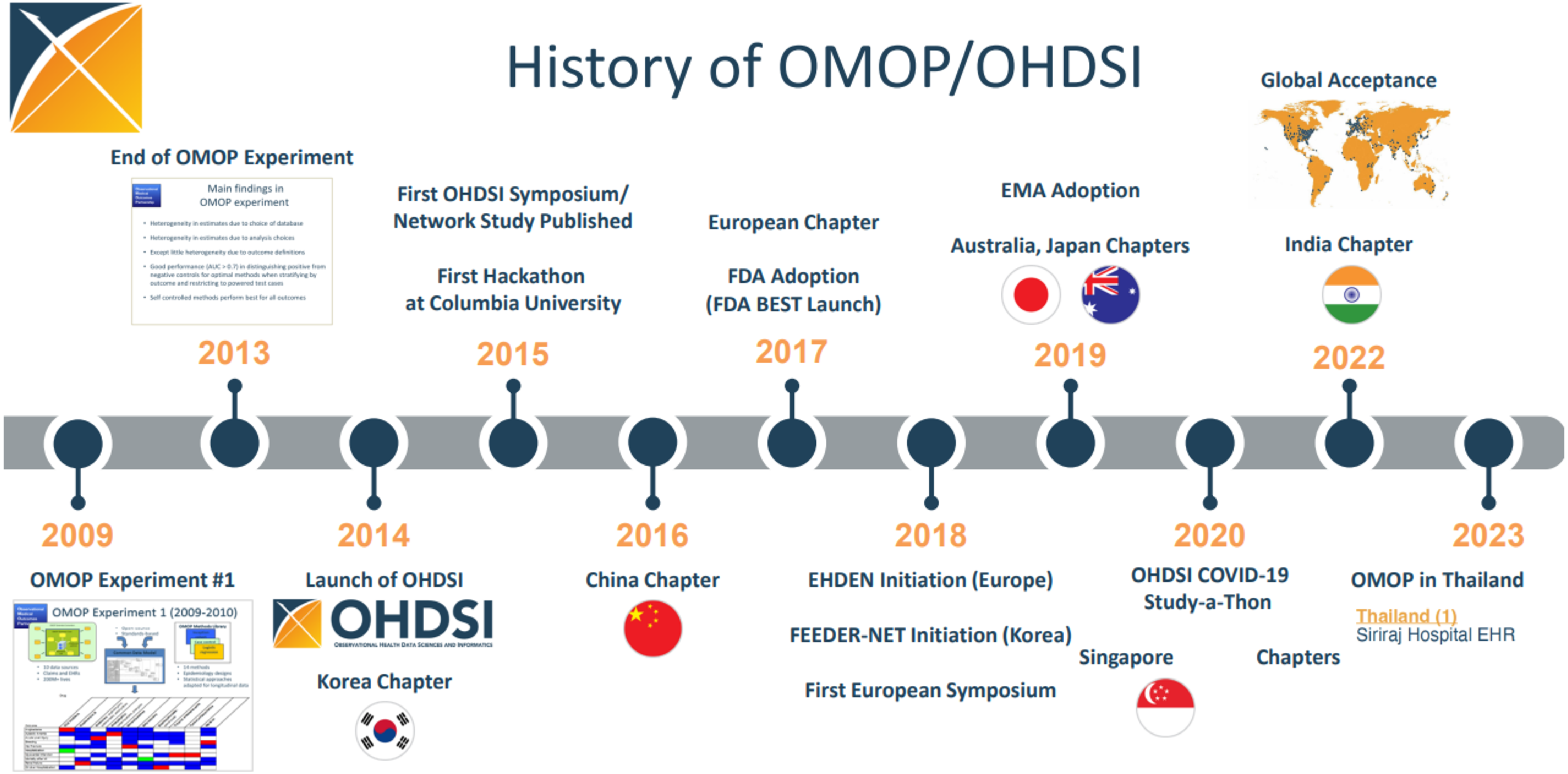
OHDSI Network:

- 534 data sources
- 49 countries
- 956M unique patient records

https://ohdsi.org/

https://www.ohdsi.org/wp-content/uploads/2024/06/3.-OHDSI-OMOP-Introduction.pdf

History of OMOP/OHDSI (Observational Health Data Sciences and Informatics)



History of OMOP/OHDSI

2009

OMOP Experiment #1

OMOP Experiment 1 (2009-2010)

2013

End of OMOP Experiment

Main findings in OMOP experiment

- Heterogeneity in estimates due to choice of database
- Heterogeneity in estimates due to analysis choices
- Except little heterogeneity due to outcome definitions
- Good performance (AUC > 0.7) in distinguishing positive from negative controls for optimal methods when stratifying by outcome and restricting to powered test cases
- Self controlled methods perform best for all outcomes

2014

Launch of OHDSI

Korea Chapter

2015

First OHDSI Symposium/
Network Study Published

First Hackathon
at Columbia University

2016

China Chapter

2017

European Chapter

FDA Adoption
(FDA BEST Launch)

2018

EHDEN Initiation (Europe)

FEEDER-NET Initiation (Korea)

First European Symposium

2019

EMA Adoption

Australia, Japan Chapters

2020

OHDSI COVID-19
Study-a-Thon

Singapore Chapters

2022

Global Acceptance

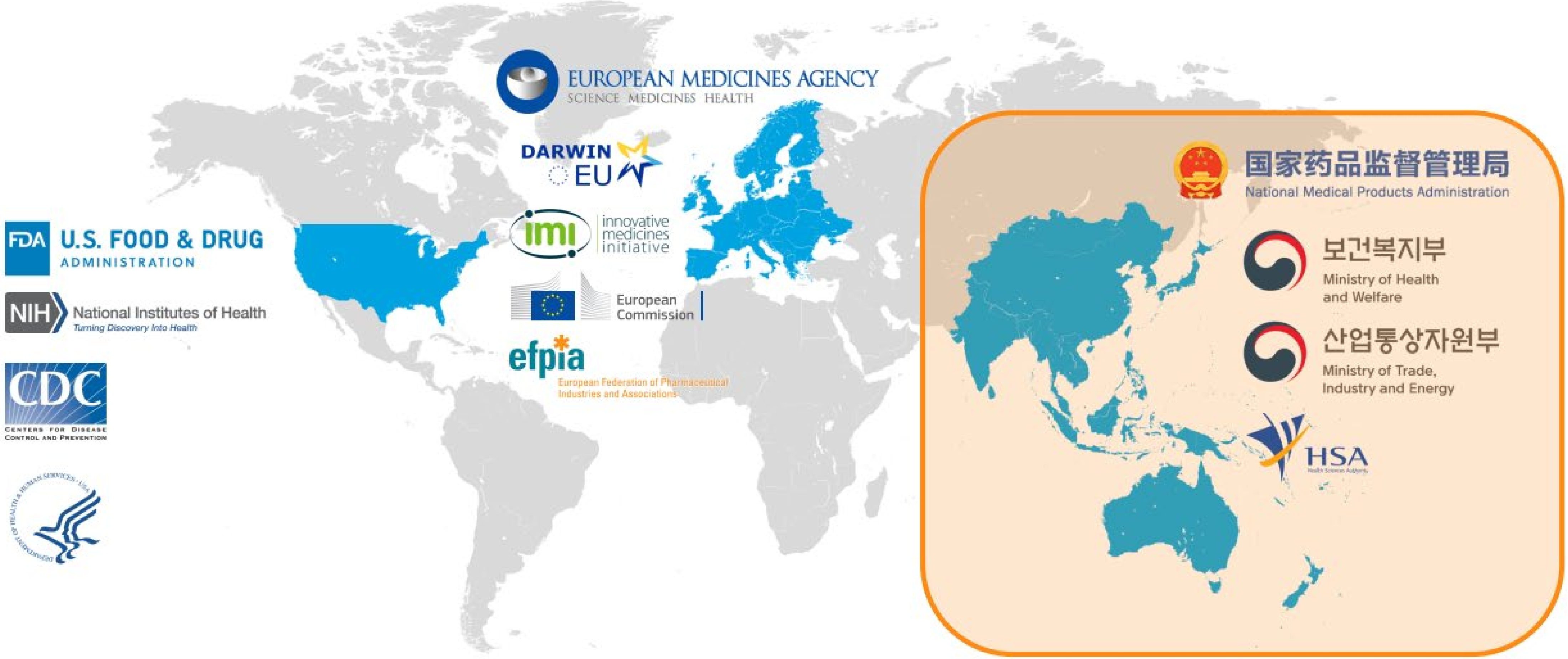
India Chapter

2023

OMOP in Thailand

Thailand (1)
Siriraj Hospital EHR

Global OHDSI Adoptions

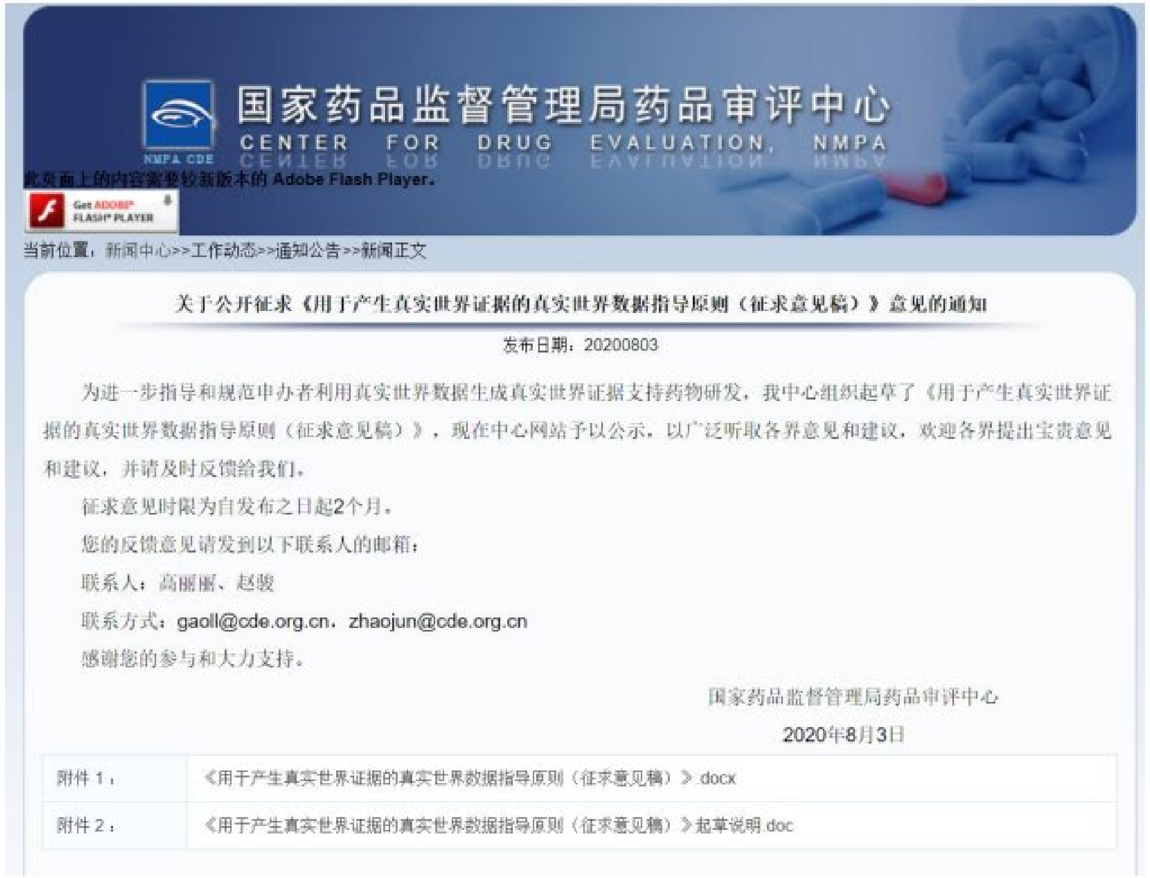

U.S. FOOD & DRUG ADMINISTRATION
FDA
NIH National Institutes of Health
Turning Discovery Into Health
CDC
CENTERS FOR DISEASE CONTROL AND PREVENTION
EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH
DARWIN EU
imi innovative medicines initiative
European Commission
efpia
European Federation of Pharmaceutical Industries and Associations
国家药品监督管理局
National Medical Products Administration
보건복지부
Ministry of Health and Welfare
산업통상자원부
Ministry of Trade, Industry and Energy
HSA

China Government's Guides on RWE & RWD

From Center for Drug Evaluation (CDE), National Medical Products Administration (NMPA)

- **1st guide** was released in Jan 2020, introducing the definition, data source requirement, design, and evaluation of using RWE for drug effectiveness study and safety monitoring.

- **2nd guide** was released in Aug 2020, focusing on the details and importance of the source, safety, curation, quality assurance and maintenance of RWD, so that reliable RWE could be produced



国家药品监督管理局药品审评中心
CENTER FOR DRUG EVALUATION, NMPA
NMPA CDE
此页面上的内容需要较新版本的 Adobe Flash Player。
Get ADOBE FLASH PLAYER

当前位置：新闻中心>>工作动态>>通知公告>>新闻正文

关于公开征求《用于产生真实世界证据的真实世界数据指导原则（征求意见稿）》意见的通知

发布日期：20200803

为进一步指导和规范申办者利用真实世界数据生成真实世界证据支持药物研发，我中心组织起草了《用于产生真实世界证据的真实世界数据指导原则（征求意见稿）》，现在中心网站予以公示，以广泛听取各界意见和建议，欢迎各界提出宝贵意见和建议，并请及时反馈给我们。

征求意见时限为自发布之日起2个月。

您的反馈意见请发到以下联系人的邮箱：

联系人：高丽丽、赵骏

联系方式：gaoll@cde.org.cn，zhaojun@cde.org.cn

感谢您的参与和大力支持。

国家药品监督管理局药品审评中心
2020年8月3日

附件 1：	《用于产生真实世界证据的真实世界数据指导原则（征求意见稿）》.docx
附件 2：	《用于产生真实世界证据的真实世界数据指导原则（征求意见稿）》起草说明.doc

China Government’s Guides on RWE & RWD

CDM & OHDSI Citations in the 2^{nd} Guide, Section 4 – Real World Data Curation

CDM Introduction in Guide:

- Under multidisciplinary collaboration, CDM was created with standardized structure, format and vocabulary, to achieve multi-center data integration and collaboration.

References in Guide:

- EMA. A Common Data Model for Europe – Why? Which? How? https://www.ema.europa.eu/en/events/common-data-model-europe-why-which-how
- OHDSI – Observational Health Data Sciences and Informatics, https://www.ohdsi.org

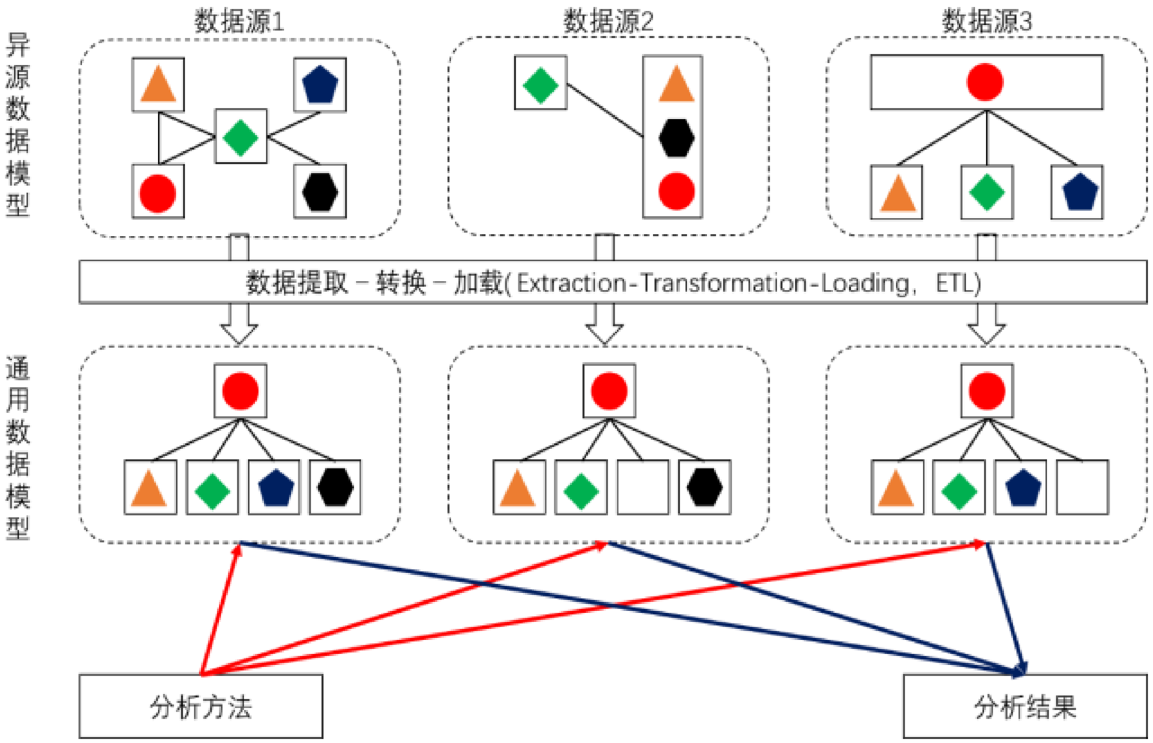
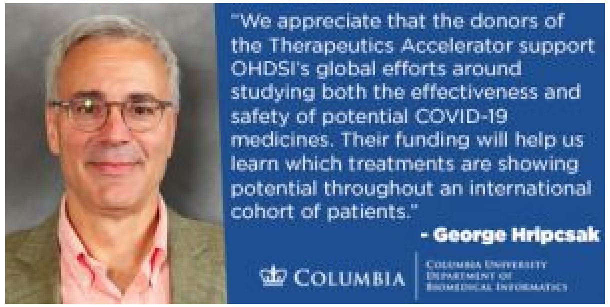


Fig. 2 in Guide – Diagram on Converting Source Data to CDM



"We appreciate that the donors of the Therapeutics Accelerator support OHDSI's global efforts around studying both the effectiveness and safety of potential COVID-19 medicines. Their funding will help us learn which treatments are showing potential throughout an international cohort of patients."

- George Hripcsak

COLUMBIA
Columbia University Department of Biomedical Informatics

International Conference on Artificial Intelligence in Medicine (AIME) 2024, Salt Lake City, Utah, USA, July 9-12

Data Governance and Data Lifecycle Management

- **Data governance ensures proper oversight at each stage of the data lifecycle**, enforcing policies on data security, quality, and ethical use.
- **Data lifecycle management supports governance** by defining how data is handled over time, from creation to deletion, ensuring compliance and efficiency.
- Both are crucial for **medical AI, biomedical research, and privacy-preserving technologies** to maintain data security, integrity, and compliance while enabling innovation.

(Assisted by ChatGPT)

Importance of Biomedical Data Sharing

- Accelerating **Medical Research**
  - Shared biomedical data enable researchers to **develop new treatments**, conduct large-scale studies, and **validate findings** across different populations.
  - It fosters **collaboration** among researchers, leading to breakthroughs in disease understanding and drug discovery.
- Enhancing **AI and Machine Learning Models**
  - High-quality, diverse datasets improve the **performance** and **generalizability** of AI-driven diagnostic tools and predictive models.
  - Training AI on larger datasets helps **reduce bias** and ensures better accuracy in clinical decision-making.

(Assisted by ChatGPT)

Importance of Biomedical Data Sharing

- Improving **Public Health** Outcomes
  - Data sharing facilitates **early detection** of disease outbreaks and trends, enabling public health interventions.
  - It supports epidemiological studies and global health **monitoring** efforts.
- Facilitating **Personalized Medicine**
  - Integrating biomedical data **across institutions** helps tailor treatments to individual patients, improving therapeutic outcomes.
  - **Genomic data sharing** plays a crucial role in precision medicine by identifying patient-specific disease risks.
- Optimizing **Healthcare Systems**
  - Shared clinical data (to analyzers) can **enhance hospital efficiency**, improve patient care coordination, and reduce medical errors.
  - It helps policymakers design **evidence-based** healthcare policies and resource allocation strategies.

(Assisted by ChatGPT)

Privacy Challenges in Biomedical Data Sharing

- Patient Confidentiality and Data Protection
  - Medical records contain highly sensitive personal information, and unauthorized access or breaches can lead to **identity theft** or **discrimination**.
  - **Compliance with privacy regulations** (e.g., GDPR, HIPAA) is necessary to protect patient rights.

More about privacy regulations in the West on March 21 in Week 5

- Re-identification Risks
  - Even **de-identified** datasets can be **re-identified** when combined with other publicly available data.
  - Advanced **machine learning** techniques can **infer** patient identities, raising privacy concerns.

More about re-identification on April 4 in Week 7

(Assisted by ChatGPT)

Privacy Challenges in Biomedical Data Sharing

- Balancing Data Utility and Privacy

  More about protection techniques in Weeks 9 - 12

  - Privacy-preserving techniques like **differential privacy, federated learning, and synthetic data generation** are needed to enable data sharing while minimizing risks.

    More about game-theoretic models in Week 9

  - Researchers must find the **right balance** between data utility and privacy protection to ensure both scientific progress and ethical responsibility.

- Data Security Threats
  - Cybersecurity risks, including data breaches and **hacking**, threaten the **integrity** of biomedical databases.

    More about access control on April 25 in Week 10

  - Institutions must implement robust **encryption**, **access controls**, and secure storage solutions.

    More about encryption technologies in Week 11

(Assisted by ChatGPT)

Privacy Challenges in Biomedical Data Sharing

- Bias and Inequities in Data Sharing
  - Limited representation of diverse populations in biomedical datasets can result in **biased** AI models and unequal healthcare outcomes. (Due to protection)
  - Institutions should ensure **fair and equitable** data sharing to improve model fairness. (Balancing fairness and Privacy)
- Ethical and Legal Concerns

  More about informed consent on May 14 in Week 13

  - Ethical dilemmas arise regarding **informed consent**, especially when patients are unaware of how their data is being used.
  - Varying **legal frameworks** across countries create challenges in global biomedical data sharing.

More about privacy regulations on March 21 in Week 5

(Assisted by ChatGPT)

Readings for the Next Week

- Xu J, Xiao Y, Wang WH, Ning Y, Shenkman EA, Bian J, Wang F. Algorithmic fairness in computational medicine. EBioMedicine. 2022 Oct 1;84.
  - ❑ https://www.thelancet.com/pdfs/journals/ebiom/PIIS2352-3964(22)00432-7.pdf
- Optional
  - ❑ Kearns M, Roth A. *The ethical algorithm: The science of socially aware algorithm design*. Oxford University Press; 2019 Oct 4. (Ch.2)

ON A PIECE OF PAPER

- One thing you learned or felt was valuable from today’s class & reading

- Muddiest point: what, if anything, feels unclear, confusing or “muddy”