МОНГОЛ УЛСЫН ЗАСГИЙН ГАЗАР
ЭРҮҮЛ МЭНДИЙН ЯАМ

МОНГОЛ УЛСЫН ЗАСГИЙН ГАЗАР
ЦАХИМ ХӨГЖИЛ, ХАРИЛЦАА ХОЛБООНЫ ЯАМ

unicef
НҮБ-ын Хүүхдийн Сан

ЦАХИМ ЭРҮҮЛ МЭНД

# Диксон Памела Грахам

Дэлхийн Эрүүл Мэндийн Байгууллагын
Эрүүл мэндийн хамтын ажиллагааны
зөвлөлийн шинжээч,
Америкийн Нэгдсэн Улсын
Карнеги Меллон Их сургуулийн зөвлөх

# E- Health Convergence in an AI Era: Key Updates to the 7 Pillars of eHealth

**E-Health Convergences, Ministry of Health, Government of Mongolia**
April 2024

**Pam Dixon Executive Director**
**World Privacy Forum**
pdixon@worldprivacyforum.org
@privacyforum

@pamdi

National eHealth Strategy Toolkit

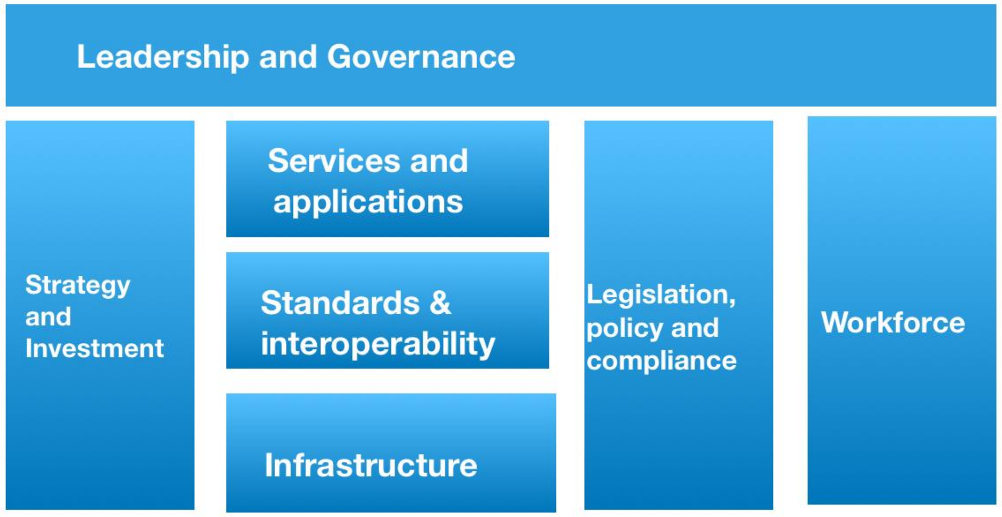
World Health Organization

ITU

# National eHealth Strategy Toolkit

**WHO & ITU, 2012**

**https://iris.who.int/bitstream/handle/10665/75211/9789241548465_eng.pdf**



Leadership and Governance

Strategy and Investment

Services and applications

Standards & interoperability

Infrastructure

Legislation, policy and compliance

Workforce

# Legislation, Policy, and Compliance

Artificial Intelligence

Digital Data

## Key Updates Regarding AI impact on the e-health data ecosystem:

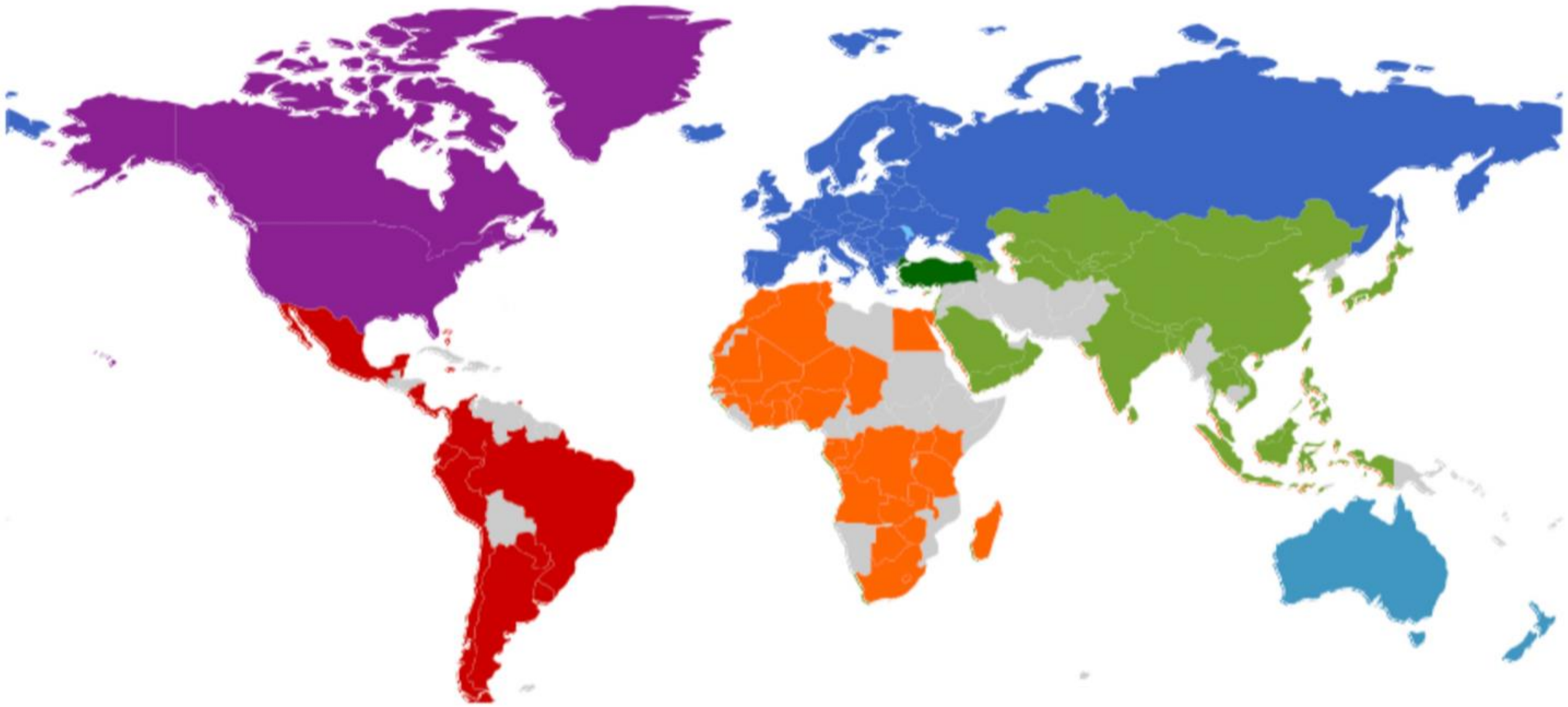
- 70+ countries have National AI strategies as of 2024. In 2019, it was just a few. 14 Countries include AI and health in their National AI Strategies.

- Countries are passing health-specific AI rules, laws, best practices, and guidance. (U.S. Office of Management and Budget Advancing Governance, Innovation, and Risk Management for Agency use of AI; EU AI Act.) (https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf)

- WHO, UNESCO, and OECD have AI Principles that form International Customary Law

- AI Impact Assessments are now being conducted in e-health environments.

## Comparing National AI Strategies in Three Categories:  Agrigulture, Environment, Health: [N=70]



# Comparing National AI Strategies in Three Categories: Agrigulture, Environment, Health: [N=70]

**Health**:

1. Europe: Belgium
2. Asia: China
3. Europe: France
4. Asia: India
5. Asia: Indonesia
6. Europe: Ireland
7. Africa: Mauritius
8. Europe: Norway
9. Asia: Singapore
10. Europe: Slovenia
11. **Asia: Thailand**
12. Asia: Turkiye
13. South America: Uruguay
14. Asia: Vietnam

**Environment**:

1. Asia: China
2. Europe: France
3. Europe: Hungary
4. Asia: India
5. Asia: Indonesia
6. Europe: Ireland
7. Africa: Mauritius
8. Europe: Slovenia
9. **Asia: Thailand**
10. South America: Uruguay
11. Asia: Vietnam

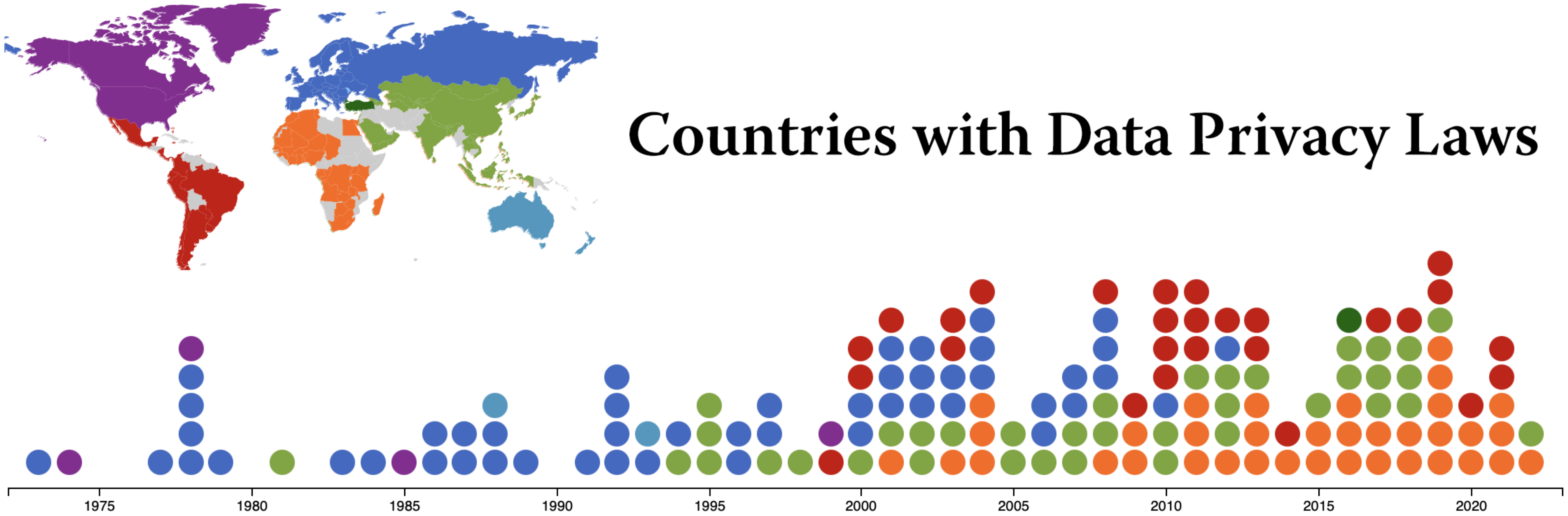
**Agriculture**

1. Europe: Hungary
2. Asia: India
3. Asia: Indonesia
4. Europe: Ireland
5. Africa: Kenya
6. Africa: Mauritius
7. **Asia: Thailand**
8. Asia: Vietnam

## Key Updates Regarding Applicable laws to the e-health data ecosystem:

- 165+ Countries with GDPR-like laws
- National, Regional laws in public and private health as well as e-health guidance and solutions.
- The 2020 experience revealed that existing infrastructure, guidance, and practices in almost all jurisdictions did not give health providers enough detailed guidance during COVID-19; the unprecedented global situation and the great need for efficiency and speed of work created many new solutions and updated best practices.
- As of 2024, many new e-health guidance practices that were established during the pandemic have now been published and are starting to become adapted to a post-pandemic environment. Some of these are around digital health, some are focused on AI.

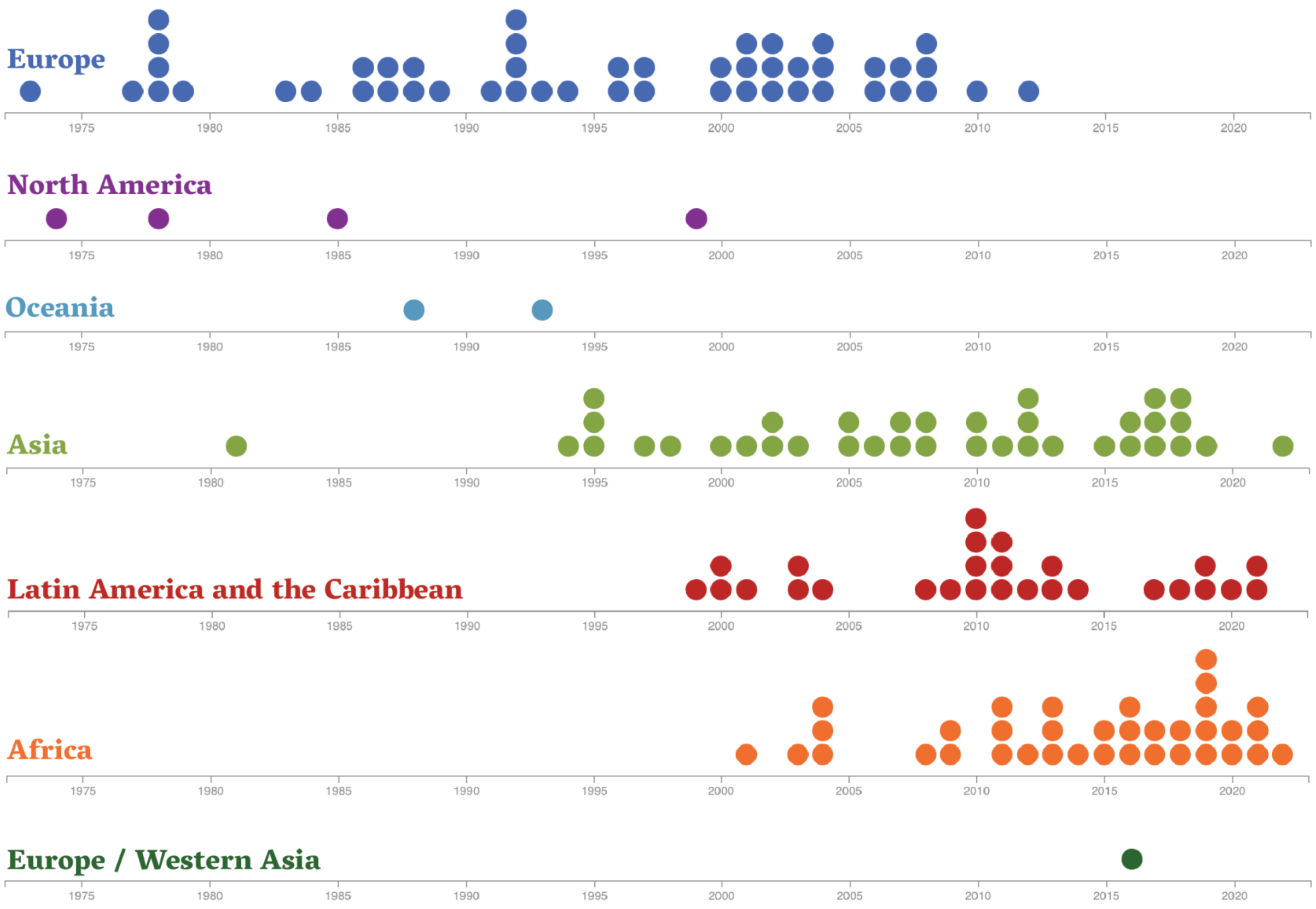
# Countries with Data Privacy Laws



WORLD PRIVACY FORUM

# Countries with Data Privacy Laws

## Regional Trends

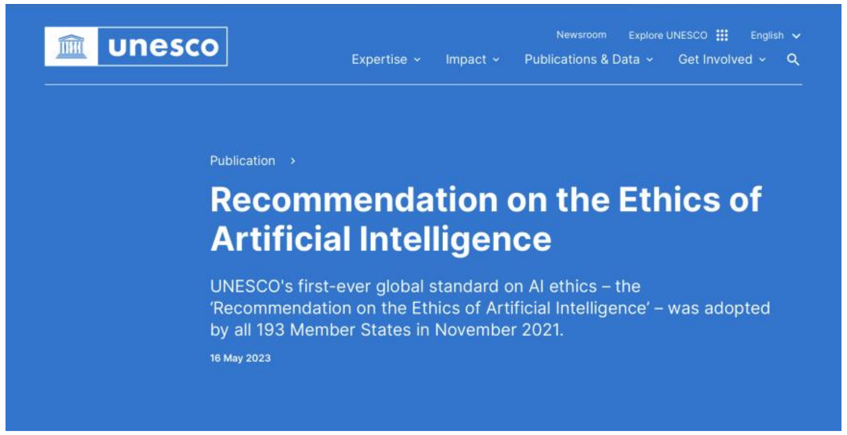


Updated October 2023

WORLD PRIVACY FORUM

# Standards & Interoperability

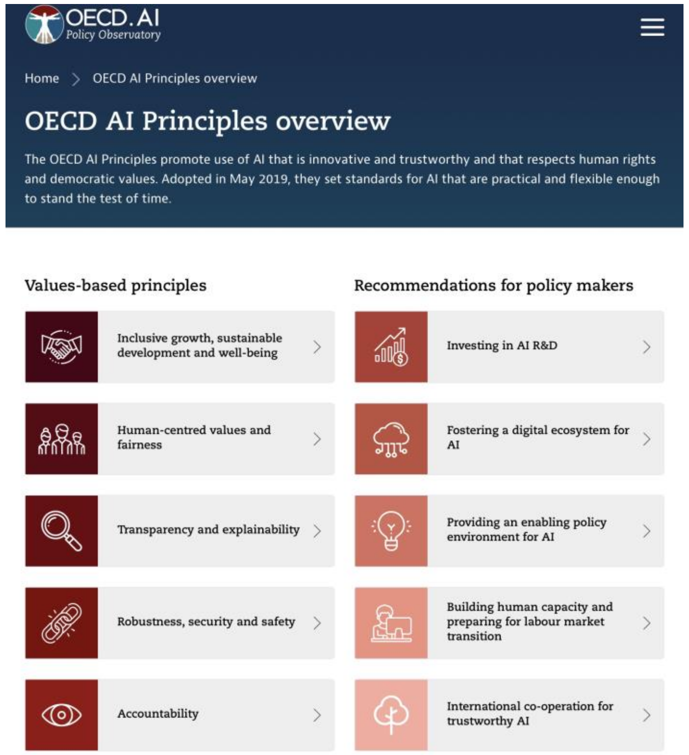
Artificial Intelligence



## Recommendation on the Ethics of Artificial Intelligence

UNESCO's first-ever global standard on AI ethics – the 'Recommendation on the Ethics of Artificial Intelligence' – was adopted by all 193 Member States in November 2021.

16 May 2023



## OECD AI Principles overview

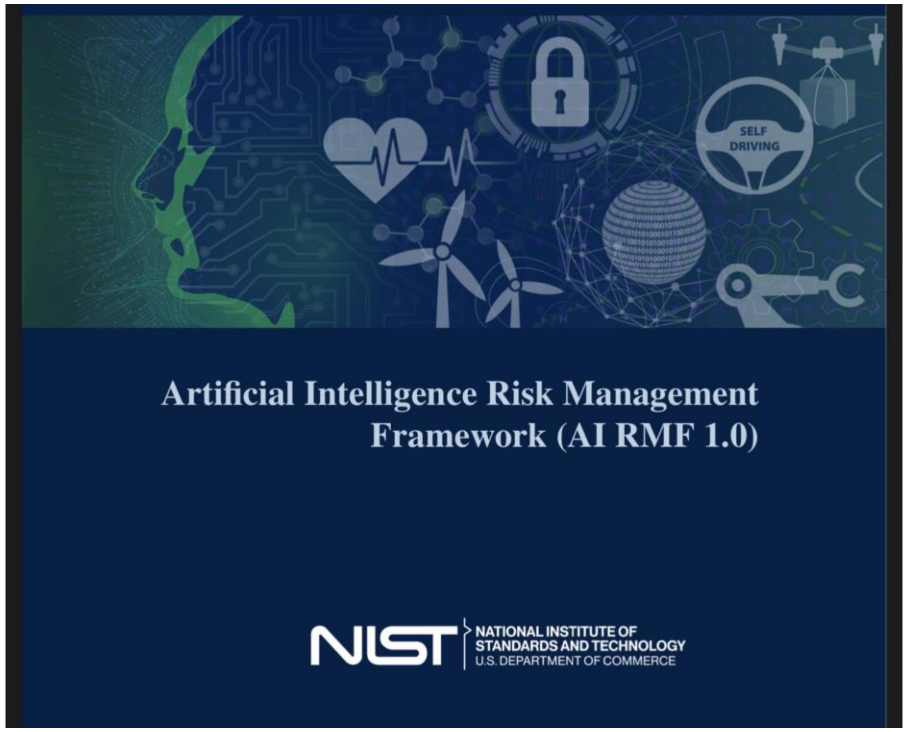
The OECD AI Principles promote use of AI that is innovative and trustworthy and that respects human rights and democratic values. Adopted in May 2019, they set standards for AI that are practical and flexible enough to stand the test of time.

### Values-based principles

- Inclusive growth, sustainable development and well-being
- Human-centred values and fairness
- Transparency and explainability
- Robustness, security and safety
- Accountability

### Recommendations for policy makers

- Investing in AI R&D
- Fostering a digital ecosystem for AI
- Providing an enabling policy environment for AI
- Building human capacity and preparing for labour market transition
- International co-operation for trustworthy AI



Artificial Intelligence Risk Management Framework (AI RMF 1.0)

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

# [Background: the development of international principles and soft law regarding AI and machine learning]

- Although AI and machine learning has been present for many decades, it was after 2010 that focus on developing policy guidance for AI became increasingly prominent.

- By 2015, there was a profusion of AI/ML principles in various stages of development. However, many of these efforts were not inclusive, either geographically or in other ways.

- In 2018, the **OECD** (based in Paris, France) began a course of work to develop international soft law guidelines. OECD used the model of its Privacy Guidelines, which have formed the basis of much international privacy law. The *OECD Principles on AI* were published and ratified in 2019. These principles created soft law in ratifying countries. https://oecd.ai/en/ai-principles

- In 2021, **UNESCO** followed OECD and published its *Recommendation on the Ethics of AI*. These recommendations are considered to be important global principles. https://www.unesco.org/en/artificial-intelligence/recommendation-ethics

- In 2021, **WHO** published its principles for AI in the health context

- In 2023, **NIST** published its *AI Risk Management Framework*, among the first major international multistakeholder frameworks to address implementation. https://pages.nist.gov/AIRMF/

## Key Updates Regarding Formal Standards and Guidance on AI in the health data ecosystem:

- IEEE: Standard for Performance and Safety Evaluation of AI-Based Medical Devices. IEEE Std 2802-2022 , May 2023, doi: 10.1109/IEEESTD.2023.10117469.

- WHO Guidance for the Ethics and Governance of AI for Health https://www.who.int/publications/i/item/9789240029200

## Most providers are familiar with technical standards. There are also data use policy standards and practices:

- Public health ecosystems may contain high volumes of identifiable health data. **Data minimization** is an important Privacy by Design concept that can be applied to allow for data to be used, while still protecting individuals and groups from harms of, for example, data breaches and fraud.
- **Purpose specification** is an important element of preparing for COVID-19 ecosystems. What promises are made when the data is collected? Who will use the data, and for what purpose?
- **Data use timelines** are important to include in a public health analysis. How long will the data be used? Just for an emergency, or longer? Making these decisions early will be very helpful.

# Services & Applications

## Artificial Intelligence

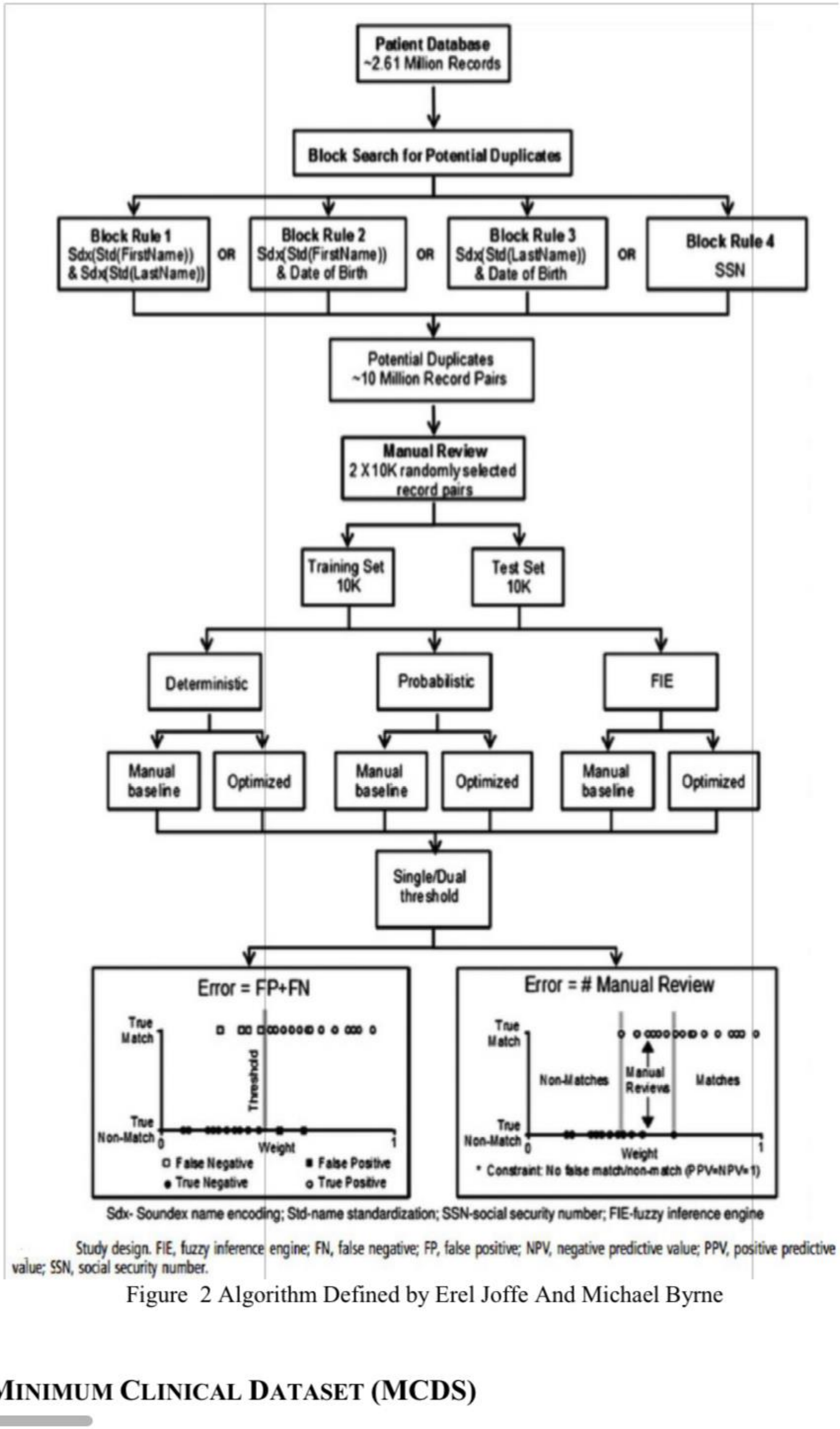
## Two Use Cases:

- Medical Devices and AI: US FDA
- Master Patient Index and use of AI

# Use Case: Master Patient Index and AI

## Review on Master Patient Index:

https://arxiv.org/pdf/1803.05994v1.pdf



Sdx- Soundex name encoding; Std-name standardization; SSN-social security number; FIE-fuzzy inference engine

Study design. FIE, fuzzy inference engine; FN, false negative; FP, false positive; NPV, negative predictive value; PPV, positive predictive value; SSN, social security number.

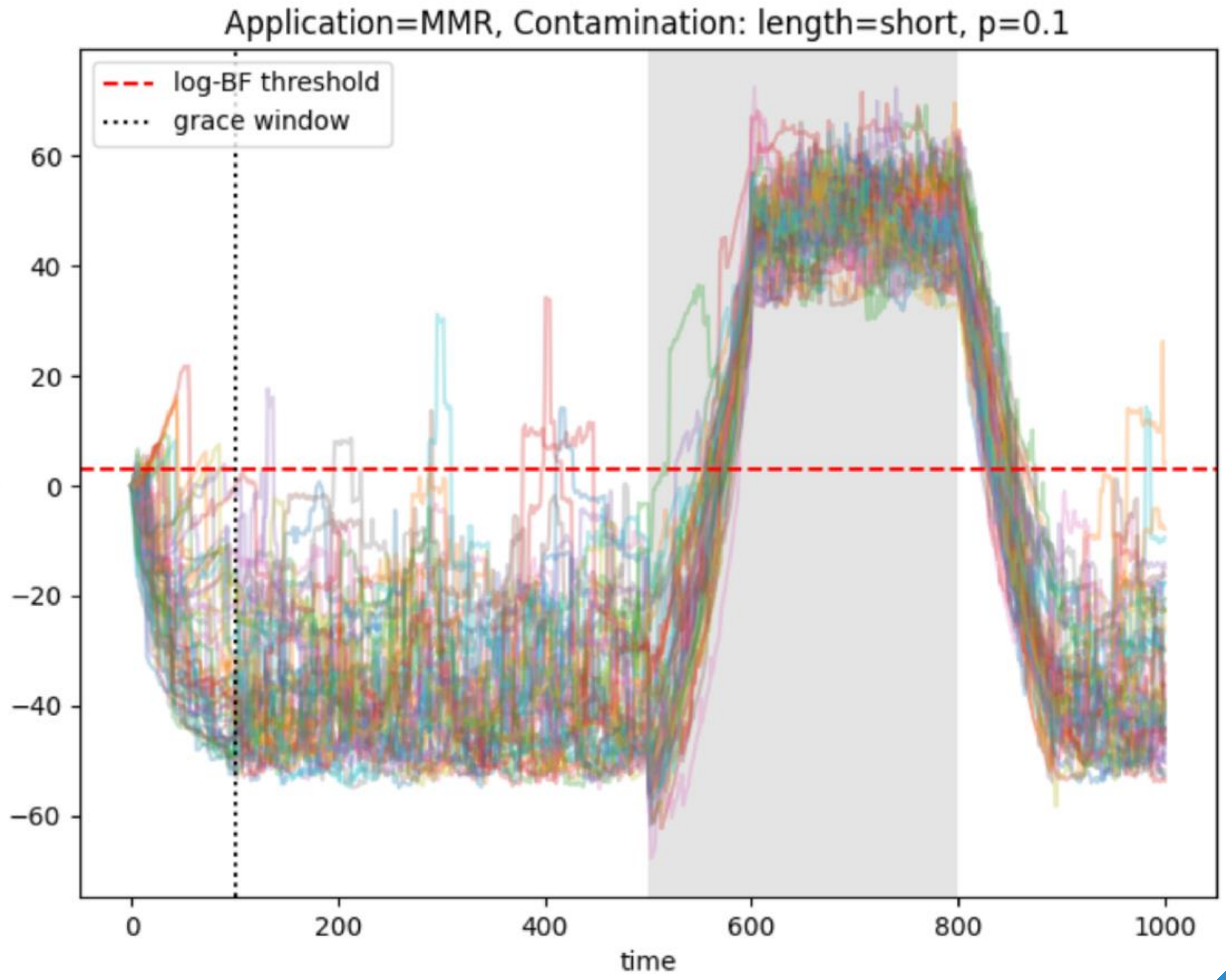
Figure 2 Algorithm Defined by Erel Joffe And Michael Byrne

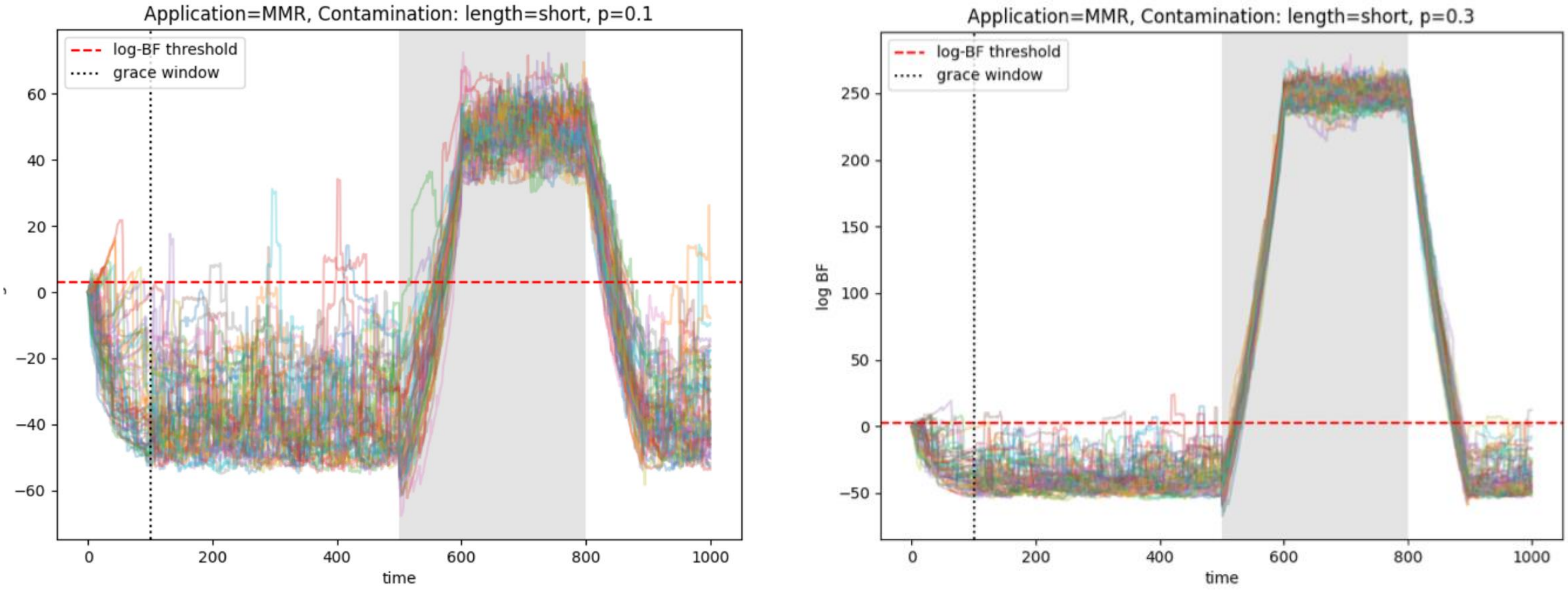
3. MINIMUM CLINICAL DATASET (MCDS)

# Use Case: Medical Device and AI

## Data Drift Monitoring in Medical Devices:

https://arxiv.org/pdf/2310.14893.pdf





# Before and after “data drift” decontamination

# Infrastructure

## Artificial Intelligence

## Digital Data Flows and Mapping the Data Ecosystem

## Updated considerations regarding health data flows and health data flow infrastructures:

**Multi-jurisdictional**: Health data flows are important at the local, national, regional, and international levels. (Post-pandemic changes).

**High volume**: The generation of public health data is so large and complex that it can no longer be saved or analyzed using conventional data processing methods. COVID-19 was a “Big Data” pandemic. It created changes in how health data is handled.

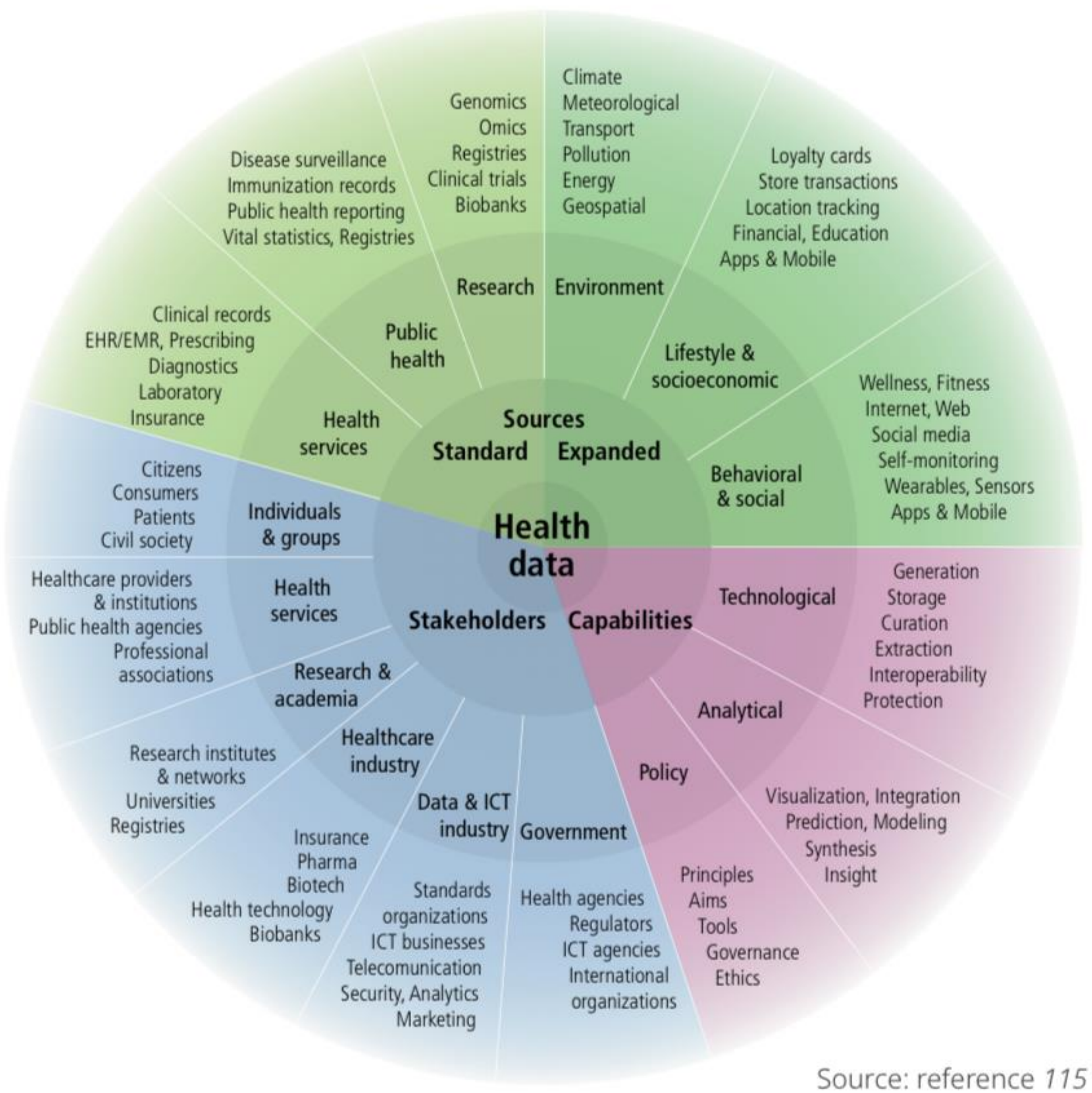
**High velocity**:  The speed with which health data is generated, processed, and analyzed has increased dramatically. Ideally, the data processing will occur within fractions of a second, also known as “real time.”  This speed also requires greater automation of data and privacy governance.

**High complexity**: The diversity of data types and sources in health data is a challenge that still needs to be solved fully.

**High sensitivity to design choices**: there are many trade-offs in design choices (for example, in databases and in contact tracing), and it is crucial to work through all of the possibilities through the lifecycle of the data flows, uses, and storage.

# WHO: The health data ecosystem

https://creativecommons.org/licenses/by-nc-sa/3.0/igo



Source: reference *115*

E. Vayena, J. Dzenowagis, M. Langfeld, 2016

## Step One: A Key Infrastructure Activity is Mapping the Health Data Ecosystem

*Think in terms of **ecosystems** and **data flows**, not just individual apps or databases*

Digital health data lives in ecosystems made up of hardware, software, and infrastructure that controls data and data flows. Ecosystems have many different configurations, and the data can be handled many ways, including databases, (federated, centralized, decentralized) cloud storage, storage at the "edge," and many other configurations and technology combinations.

Each ecosystem is different, and needs to implement rules according to its design. Privacy by Design means the design is planned prior to creating the ecosystem. Privacy is built in by default. This starts by understanding what your ecosystem will look like, how it will act, and by assessing and mitigating those risks before ever building the system. This will require mapping machines, medical devices, databases, and all the points of the health ecosystem where data flows.

## STEP TWO: Ecosystem Risk Assessment / Privacy Impact Assessment

- Privacy Impact Assessments are well understood among Data Protection Authorities. Full ecosystem risk assessments go farther than a PIA.

- Risk assessments will need to be customized to the ecosystem you have planned.

- The risk assessment of a system needs to consider all of the systems you want to create, along with the technologies and the risks inherent to those technologies. It is helpful for legal, policy, and technical experts to work collaboratively in conducting a full ecosystem risk assessment / PIA.

- To create a deep enough assessment, ensure that each ecosystem component that has been planned is matched to privacy, security, human rights, legal instruments, policies, and governance.

- If the health system is utilizing AI, conduct an AI Impact Assessment.

## Ecosystem Risk Assessment
## Questions to help assess ecosystems:

- What will **your** desired data ecosystem look like?
- How much data?
- How fast will the data arrive and be analyzed and then utilized?
- How long will you keep the data?
- What encryption will be used?
- What computing components are involved?
- How long will the ecosystem last?
- How much will it cost?
- Who will use and access your system?
- How will you ensure access control?
- Who are the beneficiaries of the system?

## Questions to help assess ecosystems, continued:

- Gather a full view of the existing technologies, databases, data systems, and analytical capacities that are already in place:
  - Who manages / owns the existing technology?
  - Could any existing technology be adapted or used in the project?
  - Could the existing ecosystems / infrastructure allow you to reach your desired outcome?
  - If you discover gaps in hardware or other components, what new technology would you need?
- What **new** technologies must you have or add, without which the project will fail?
- What are the financial incentives for your project to succeed?
- Are there sufficient incentives that will allow you to see your vision through to completion?

## Data and Privacy Risk Assessment specifically to data design:

- Are you utilizing the minimum data necessary?
- Is the data consented, accurate, and de-identified as much as possible?
- How will this raw data create risks?
- How will the data analysis create risks? Are there outcomes that could harm people or communities?
- What are the possible unintended consequences of these data and data analyses?
- What impact on other existing ecosystems will the introduction of this data have?
- What is your plan for system security?
- What policies, legal and regulatory frameworks, informal systems, cultural and social systems, do you plan to apply specifically to the data and data analysis systems?
- ***What are your controls for uses of the data and data analysis?***

### *From the ICO Big Data Report: (p. 105)*

- Have individuals been made aware of the use of their personal data?
- Could our analysis involve sensitive personal data – for example, in the analysis of social-media posts?
- Is the dataset representative and accurate?
- What are our retention policies for the data?
- Are the datasets held across multiple and disparate systems?
- Do the systems have appropriate inbuilt security measures?
- Does our proposed analysis involve cloud processing?
- Will a third-party organisation do the analytics for us?
- Could anonymised data be re-identified?
- Will we be able to explain the reasons behind any decisions we make that result from the big data analytics?

### *Regarding the GDPR and GDPR-equivalent legislation:*

- Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- Does the project involve you using new technology that may be perceived as being privacy intrusive?
- Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?

# Leadership

## Artificial Intelligence

## Core considerations for leaders when thinking about utilizing health data and planning for e-health data governance:

The importance of detailed planning in order to protect privacy and at the same time to provide public benefit is central to beneficial and effective leadership in the modern e-health environment:

- Depending on how it is designed, implemented, and used, health data ( and the analysis it typically undergoes) can produce a wide range of consequences that impact individuals, groups of people, and institutions.

- **Beneficial consequences are the goal**. To create good outcomes, considerable work and planning is required. Negative consequences can result from improper planning, and can sometimes even happen where there has been good planning in place. Contingency planning is essential.

- e-Health data it is almost always a part of a much larger technology and policy ecosystem.
  - State of data protection legislation: 164 + jurisdictions
  - Many regulations are similar to GDPR

- During the pandemic, a global ecosystem of public health data flows emerged, for example, country-level data inputs to the World Health Organization in addition to government-level efforts at the national level and regional level. The pandemic created significant increases in digitalization of health data.

# Conclusion:

If we work in cooperation, with all of the stakeholders, with the aim of protecting patients, protecting privacy and security, and protecting public health, there are no obstacles. All parties can achieve their stated goals, but it will require cooperation.

- Work toward evolving data standards
- Work toward faster and secure data flows
- Work toward automating some aspects of data and privacy governance
- Ensure all stakeholders are meeting together and all views and needs are being addressed
- Ensure a proper balance, which may change frequently.
- Ensure there is a plan for ongoing improvement and frequent communication about progress toward goals.

**Pam Dixon, Executive Director**

**World Privacy Forum**

pdixon@worldprivacyforum.org

@privacyforum

www.worldprivacyforum.org

## Resources and Additional Information

### Privacy by Design:

- Privacy by Design was developed by Ann Cavoukian in the 1990s. It has 7 components.

- *Privacy by Design* extends to a “Trilogy” of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and networked infrastructure.

- The objectives of *Privacy by Design* — ensuring privacy and gaining personal control over one’s information and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the following 7 Foundational Principles

### 1. *Proactive* not Reactive; *Preventative* not Remedial

The *Privacy by Design* (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events *before* they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to *prevent* them from occurring. In short, *Privacy by Design* comes before-the-fact, not after.

### 2. Privacy as the *Default Setting*

We can all be certain of one thing — the default rules! *Privacy by Design* seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, *by default.*

### 3. Privacy *Embedded* into Design

*Privacy by Design* is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

### 4. Full Functionality — *Positive-Sum*, not Zero-Sum

*Privacy by Design* seeks to accommodate all legitimate interests and objectives in a positive-sum “win-win” manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. *Privacy by Design* avoids the pretense of false dichotomies, such as privacy *vs.* security, demonstrating that it *is* possible to have both.

### 5. End-to-End Security — *Full Lifecycle Protection*

*Privacy by Design,* having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, *Privacy by Design* ensures cradle to grave, secure lifecycle management of information, end-to-end.

### 6. *Visibility* and *Transparency* — Keep it *Open*

*Privacy by Design* seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

### 7. *Respect* for User Privacy — Keep it *User-Centric*

Above all, *Privacy by Design* requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

See: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

## A Privacy by Design implementation in the 2024 digital health context can include:

The planning, design, goals, utilization, and ongoing evaluation of digital health data and ecosystems need to be **intentional**, with all steps carefully planned well in advance of any project or use.

Privacy Enhancing Technologies (PETs) have matured: tools such as differential privacy and synthetic data have improved and should be considered and evaluated for digital health projects from the earliest planning stages.

Best practices, standards, (including data formatting standards) and country-level practices are key.

Planning, action, evaluation, and revision is an **ongoing process** from the beginning to the end of any public health project.

## Key Best Practices for Public Health Data Analysis:

Data analytics is a core part of public health data flows and ecosystems. It has been important in COVID-19 to predict trends, assess needs, and anticipate problems.

This is where governance regarding **Artificial Intelligence** and **Machine Learning** come in. It is a rare health data project that does not utilize AI in some way, even if just using a regression analysis. This is where you will need to implement ethical AI principles and learn to apply best practices to public health data ecosystems and apps.

## *Principles of Trustworthy AI*

There is a great art in implementing AI principles. It will require policy experts in this area, and it will require AI experts. There are many tradeoffs in AI, some of which relate to privacy.  Much depends on the system and the data inputs.

At a principles level, these are well-accepted principles/best practices:

- Human-centered values
- Fairness
- Accuracy
- Transparency
- Explainability of outcomes
- Robustness, security, and safety
- Accountability
- and…
- Ensuring outcomes in the form of scores have minimum / maximum scores and interpretation guidelines
- Ensuring algorithms are properly fit and up to date
- Ensuring “outliers” (people) have redress if denied a service or goods based on an AI analysis

See: OECD https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

***Not everything needs be a formal law to be effective: there is room for additional governance tools such as codes of conduct, sandboxes to test system, and more:***

- Codes of Conduct and Best Practices for handling public health data are very important to agree upon in this situation
- All stakeholders need to be involved
- Respect for privacy and respect for public health
- Much can be done with data aggregation, with research uses and access control and audits, logs
- Improving public health data standardization and formats globally is an important goal. We have learned many lessons from the beginning of the pandemic until now. There is renewed importance of creating better standards for public health data.