AI IN HEALTHCARE:
PRIVACY & ETHICS CONSIDERATIONS

Ivana Bartoletti
Head of Privacy, Data Protection and Ethics, Gemserv

Gemserv

Contents

- Privacy in the Digital age: main issues
- Ethics: definitions and background
- Privacy challenges in Health
- Ethics governance and framework
- Patient’s empowerment

Data in the Digital Age

PURPOSE

ACCURACY

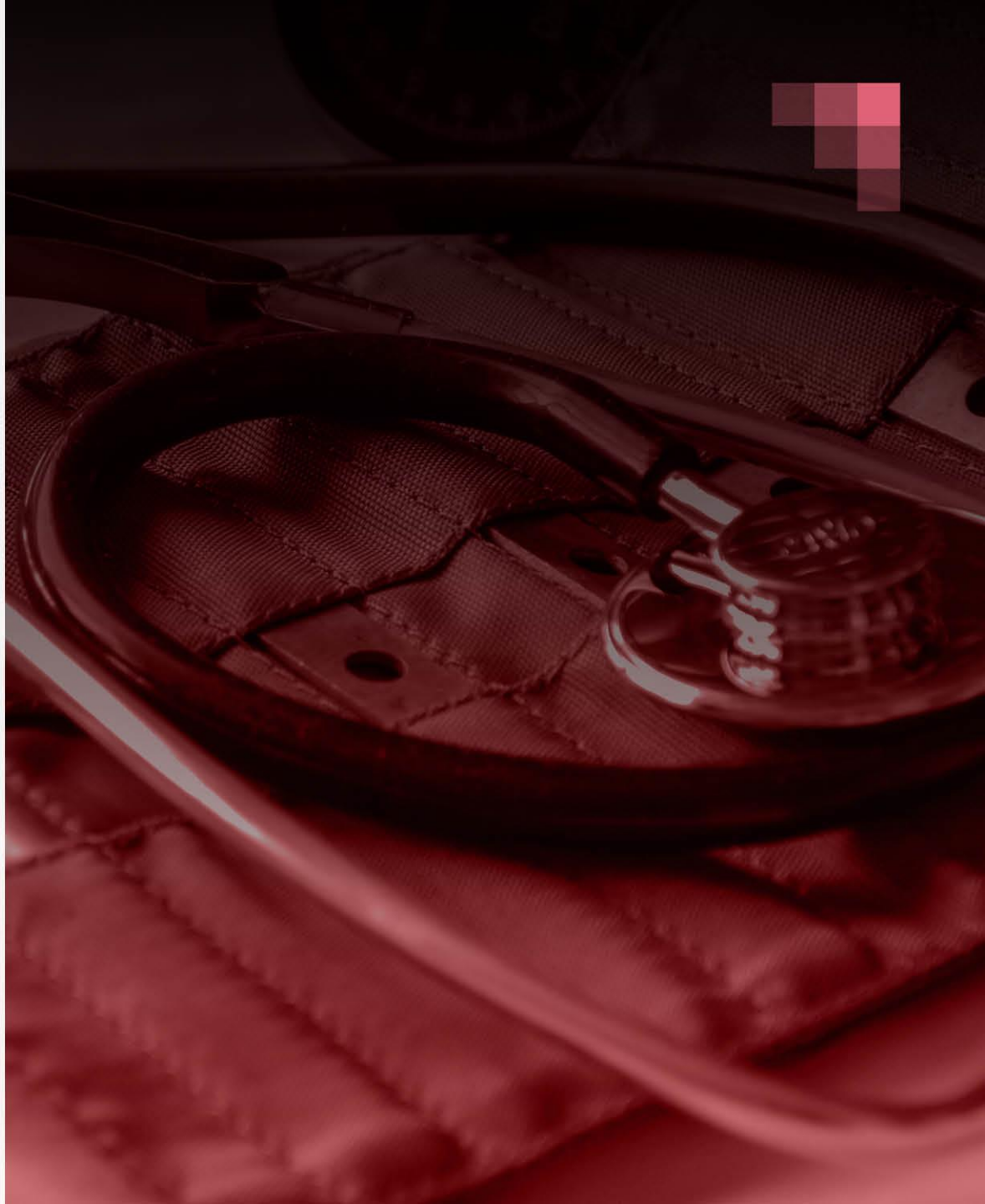
FAIRNESS

TRANSPARENCY

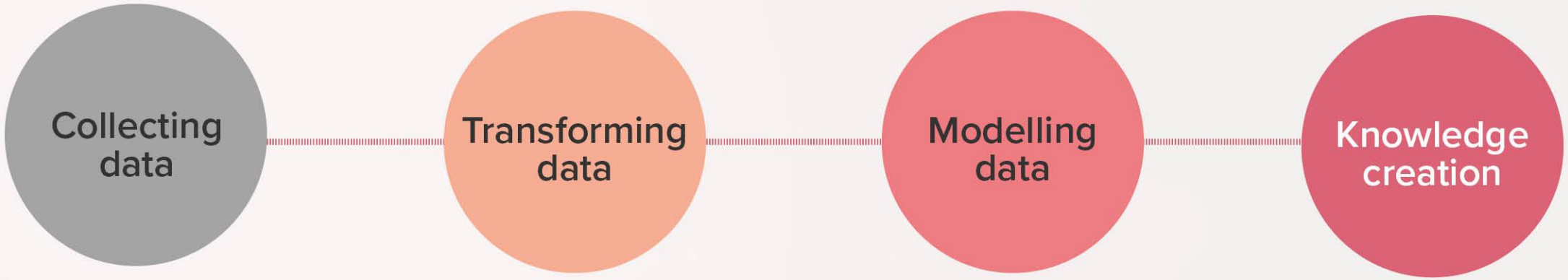
PERSISTENCE

Big Data Healthcare

- Misuse vs Missed use of data
- Consent vs Transparency
- The Big Data security lifecycle
  - Data security
  - Access control
  - Information security



Lifecycle



Key elements:

- Privacy / security by design
- Handle tech with tech
- Transparency & Accountability

WHAT IS ETHICS?

Recent Stories

San Francisco becomes first U.S. state to prohibit facial recognition by police forces

Image: Matt Popovich on Unsplash

Target Figured Out A Teen Girl Was Pregnant Before Her Father Did

Image: Tadas Sar on Unsplash

Google shuts down AI Ethics Board after criticised for appointment of anti-LGTBQ figure

Image: Pawel Czerwinski on Unsplash

COMPAS algorithm used in criminal justice found to biased against African-Americans

Image: Andre Hunter on Unsplash

Public concern and expectations

Behavioural Economics

An individual's desire for data privacy will depend on how they anticipate that data's effect on future economic outcomes.

Context and Setting

An individual's 'reasonable expectation' of privacy will differ depending on the context.

Transparency

Individuals may not be aware of how their personal data will be used, particularly when algorithms or "black box" decisions are used.

Variety of Solutions

Different system setups used in data analytics – including connected devices, AI systems and interfaces – may collect and combine data to different effects.

Existing regulation and standards

General Data Protection Regulation (GDPR) - In relation to data accuracy and security, is a central tenet of ensuring data processes remain accountable.

European Commission High Level Working Group on Artificial Intelligence – has released a Trustworthy AI assessment.

Other standards include:

- European Commission High Level Working Group ion
- The ISO is developing standard ISO/IEC JTC 1/SC 42 on Artificial Intelligence
- Institute of Electrical and Electronic Engineers (IEEE) released its Ethically Aligned Design framework

Existing standards and guidelines are targeting:

- Principles of Accountability, Responsibility, Transparency and Fairness
- Requires organisations to define values and purposes of analytics
- Conducting risk or impact assessments of the effects of AI decisions

Existing regulation and standards

Anti-discrimination law such as the Equality Act 2010 protects protects citizens from discrimination on the basis of basis of several grounds in the in the employment, commercial commercial and other contexts. contexts.

Human rights law such as the European Convention on Human Rights (ECHR) provides for the protection of human rights, including the right to privacy and non-discrimination.

Consumer law can be used to protect consumers from unfair services – e.g. dynamic pricing as a result of decisions informed by analytics or algorithms.

Microsoft provide six principles to guide the development of ethical AI:

Fairness

AI systems should treat everyone in a fair and balanced manner and not affect similarly situated groups in different ways. Developers need to understand how bias can be introduced into AI systems and how it can affect AI-based recommendations. Racism and sexism can also creep into societal data used to train AI systems, so it's important that those designing AI systems reflect the diversity of the world for which it's designed and have the relevant subject matter expertise.

Reliability

Users need to trust that AI systems will perform reliably within a clear set of parameters and respond safely to unanticipated situations. This will require the involvement of domain experts in the design process, systematic evaluation of the data and models, a process for documenting and auditing performance, determination of how and when an AI system seeks human input, and a robust feedback mechanism.

Privacy and Security

Not unlike other digital technologies, AI systems need to protect the privacy and security of the data or users will not share the data needed to train the AI. Techniques and policies are needed to protect privacy while facilitating access to the data that AI systems require to operate effectively.

Inclusiveness

AI can be a powerful tool for increasing access to information, education, employment, government services, and social and economic opportunities. But to benefit everyone, AI technologies must understand the context, needs, and expectations of the people who use them, and address potential barriers that could unintentionally exclude people.

Transparency

When AI systems help make decisions that impact people's lives, it's particularly important that people understand how those decisions were made. Contextual information about how an AI system works and interacts with data will make it easier to identify and raise awareness of potential bias, errors, and unintended outcomes.

Accountability

Those who design and deploy AI systems must be accountable for how their systems operate and should periodically check whether their accountability norms are being adhered to and if they are working effectively.

Key points

Privacy:

- Limits to privacy as we know it?
- Does privacy as we know it stand in health?
- Consent vs transparency
- Public & private

Terminology:

- The misleading narrative of empowerment
- Digital companions?

Key points

Transparency:

- Explainability of algorithms: defining the trade offs
- Machine – human cooperation
- The human in the loop
- Bias & data accuracy

Inferred data:

- Definitions
- Limits to use of inferred data: what is reasonable?

Governance Frameworks

The following principles should be followed in the delivery of data analytics systems, including AI solutions:

Organisations should ensure data governance such as by:

- Appointing an Ethics Board responsible for oversight.
- Embedding collaboration between data scientists/developers and operational management.

Data Stewards

Appropriate ‘data stewards’ should be assigned with responsibility for relevant processes in the deployment of AI systems – including for the sourcing of data, for the development or procurement of data processing systems, and for their use in business operations

Governance Frameworks

The following principles should be followed in the delivery of data analytics systems, including AI solutions:

Risk Management

Organisations should consider a 'three lines of defence' model for managing risks around new systems, i.e.:

1. First line – Operational departments (responsible for specific applications of systems) and developers
2. Ethics committees – with specialists, designers and technologist
3. Independent assurance/audits

Product Taxonomy

Organisations should consider deploying a taxonomy of products and solutions to:

- Outline what the features and uses of particular systems are
- Identify the benefits and risks of those solutions
- Assign responsibility and actions for their development and deployment

Third Parties

With regard to onboarding third parties, organizations must:

- Carry out due diligence of third parties, including hosting systems and bought-in data sets.
- Ensure that liability is apportioned with third parties.

Transparency Mechanisms

Organisations should ensure that citizens and users are made clear about how data analytics and AI systems will collect and use their data.

- Publishing a Code of Conduct, outlining the organisation's commitment to fair and unbiased AI and to protecting privacy.

- Use transparency notices to inform individuals of how their personal data with be used and their rights.

What to include?

You should provide information such as:

- Where the data is sourced from
- What is collected
- The purposes of the system
- Which organisations information is shared with
- What their rights are

Algorithmic Impact Assessments

Where new artificial intelligence (AI) systems and solutions are deployed, several standards identify that organisations should risk-assess the possible effects of their deployment.

Algorithmic Impact Assessments should look towards identifying:

1. **Reliability or accuracy of data** used to develop and/or train AI systems
2. **Data minimisation** and legality of using/ collecting certain categories of data
3. **Fairness of profiling** or categorising any groups of individuals
4. **Biased or uneven effects** of any outputs/ decisions made by AI systems
5. **Compatibility** of the system with data subject rights to access, deletion, etc.

Algorithmic Impact Assessments (AIAs)

Algorithmic Impact Assessments take the form of an audit or gap analysis that allows an organisation to determine whether they comply with legal, industry and ethical requirements and norms.

Algorithmic Impact Assessments

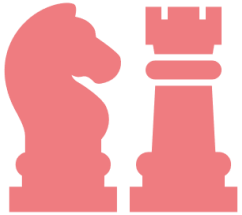
Where new artificial intelligence (AI) systems and solutions are deployed, several standards identify that organisations should risk-assess the possible effects of their deployment.

Organisations should consider:

- ❑ Potential for bias and the meaning of ‘fairness’
- ❑ Using external agencies to test systems
- ❑ Using audit trails on databases and systems
- ❑ Compliance with industry Certification Schemes

Training and Testing

- ❑ When training and testing AI systems, organisations should:
- ❑ Introduce procedures for checking for accuracy and data cleansing.
- ❑ Evaluate the impact of data analytics and profiling on groups of individuals.



Human Autonomy

Data analytics systems, particularly AI systems, should act as a complement rather than replacing human intuition:

The following principles should be core to systems:

- ❑ The purpose or use of the system should functionally be limited to suggesting/scoring/ranking rather than deciding;
- ❑ The ability for a user (e.g. member of staff) to overrule and/or amend system decisions should be enabled
- ❑ The ability to audit decisions (e.g. to see if a particular loan was approved by the system, and why) should always be possible

COMPLEMENTARY

HUMAN AGENCY

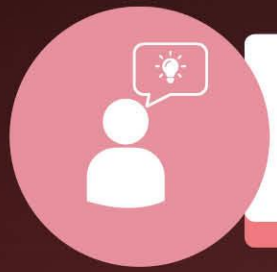
AUDIT

SUMMARY

Benefits of Data Ethics Governance

Data Ethics Governance can ensure that:

Designing is with rather than for patients / medics



Provides transparency and fairness - defines what fairness is

Takes into account socio-economic consequences and investigates intended and unintended consequences

Assigns responsibility, monitoring and provides full accountability

Any Questions?

THANK YOU FOR LISTENING

Ivana Bartoletti
Head of Privacy, Data Protection and Ethics

dataprotection@gemserv.com

Gemserv

INVESTORS IN PEOPLE | Gold Until 2020

bsi. ISO/IEC 27001 Information Security Management

GlobalGROUP ISO 14001 UKAS MANAGEMENT SYSTEMS 0039

LLOYD'S REGISTER LRQA ISO 9001 UKAS MANAGEMENT SYSTEMS 001

CYBER ESSENTIALS PLUS