# HANDOUT — Research with Health Data: Ethical issues, risk mitigation, and data management practices

**Giovanni Spitale, PhD – ITE Lab, IBME, University of Zurich**

giovanni.spitale@ibme.uzh.ch
EUTOPIA Health, Ljubljana, 20–21 Nov 2025

## Why Health-Data Ethics Matters

Health data enables breakthroughs in diagnosis, prediction, and public health.
But unlike other types of data, it encodes **identity, vulnerability, behaviour, history, and relationships.**

Ethical challenges arise because:

- **Data persists** long after the context of its collection.
- **Linkage** can reveal more than intended (e.g., inferring pregnancy, mental health, or risk behaviours).
- **Distribution of benefits** is uneven (those who contribute data rarely profit from products built with it).
- **Governance** involves actors with different incentives—industry, academia, governments.

**The central question:**
*How do we use data to heal without turning people into data points?*

## Governance Dilemmas

### Who governs the data?

Often multiple parties: hospitals, private vendors, governments.
Each has different values: public interest, profit, efficiency, political pressure.
**Risk:** ethical gaps fall into the cracks between institutions.

### Cross-border flows

Data moves through regimes with different legal protections (GDPR ↔ HIPAA).
**Risk:** when something goes wrong, it's unclear who is responsible.

## Public vs. private stewardship

Researchers rely increasingly on private infrastructures (cloud, AI models, biotech partnerships).
**Risk:** data subjects may not know who holds or processes their data, nor how to contest misuse.

# GDPR Essentials for Researchers

https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=en

**1. Personal data**
Any piece of information that *could* identify someone alone or in combination with others.

**2. Sensitive data**
Health, genetics, biometrics, political beliefs, religion, sexual life/orientation — everything with heightened risk.

**3. Research exemption**
Permits certain uses without consent **under strict safeguards** (art. 9), but does not erase ethical obligations.

**4. Transparency duty**
Participants have the right to know how data is used — except when that duty is *disproportionate* (e.g., 200,000 Telegram users).

**5. Data minimization**
Collect only what is needed, store only as long as needed.

**6. Accountability**
If something goes wrong, you must show that appropriate safeguards were in place.

# Case Illustration: Telegram vs Reddit

## Telegram Study (Ethical Use of Public Data)

https://doi.org/10.2196/34385

- Analyzed existing conversations.
- Full anonymization and pseudonymization.
- Destroyed raw data.
- Transparent methodology and limited access.
- Purpose: **observe**, not intervene.

## Reddit Experiment (Ethical Failure)

https://www.theatlantic.com/technology/archive/2025/05/reddit-ai-persuasion-experiment-ethics/682676/

- Bots impersonated real people.
- Engaged live with unaware users for months.
- No consent, no debriefing.
- Manipulated conversations to measure persuasion.
- Created emotional and reputational risks.

**Main lesson:**
Public data ≠ permission to manipulate people.

# Helpful Frameworks

## PHERCC Matrix

https://doi.org/10.1080/15265161.2023.2201191

**Core idea:** An ethical framework for planning, governing, and evaluating public-health communication during crises.

Evaluates communication according to:

- Public
- Evidence
- Communicator
- Channel
- Message
- Consequences

Highlights the ethical elements:

- openness
- transparency
- inclusivity
- understandability
- privacy

## WHO Ethics of Infodemic Management

https://www.who.int/publications/b/67856

https://doi.org/10.2196/56307

**Core idea:** IM must balance effectiveness with ethical integrity — transparency, fairness, and human-rights alignment are foundational.

Points to tensions such as:

- accuracy vs freedom of expression
- protection vs empowerment
- monitoring vs surveillance
- speed vs deliberation
- inclusion vs efficiency

Frameworks remind us that **ethics is layered, procedural, and translational**, not just substantive.

# Typical Ethical Dilemmas in Data Work

1. **Consent beyond limits**
   Reuse of old datasets when recontact is impossible.
2. **Illusion of anonymity**
   When linkage of two harmless datasets can reveal identities.
3. **Openness vs protection**
   Publishing data that includes individuals from stigmatized groups.
4. **Commercial partnerships**
   Tech companies gain access to health data under opaque agreements.
5. **Algorithmic triage**
   Models trained on unbalanced data produce discriminatory outcomes.

These are daily—not exceptional—scenarios.

# Core Ethical Principles in Health Data

## Autonomy

https://global.oup.com/academic/product/principles-of-biomedical-ethics-9780190640873

People should understand and control how their data is used.
**Why it's hard:**

- Consents are often broad, vague, or outdated.
- Secondary uses (linkage, algorithmic inference, data reuse) go far beyond what participants originally envisioned.
- Re-contacting participants may be impossible.

**Practical strategies:**

- Provide short, layered explanations instead of long forms.

- Offer "revisitable" choices (dynamic consent).
- Explain *risks of reuse*, not only purposes.

## Justice

https://global.oup.com/academic/product/principles-of-biomedical-ethics-9780190640873

Fairness in who bears risks and who reaps benefits.
**Common issues:**

- Biased datasets (overrepresentation of majority groups → skewed algorithms).
- Unequal data infrastructures (Global South contributes, Global North profits).
- Exclusion from governance: communities rarely help decide what "fair" means.

**Practical strategies:**

- Audit datasets for representation.
- Share results and benefits with contributing communities ("data reciprocity").
- Include community voices in rules, not only as participants.

## Beneficence & Non-maleficence

https://global.oup.com/academic/product/principles-of-biomedical-ethics-9780190640873

Use data to advance health while avoiding harm.
**Invisible harms include:**

- Stigmatization (e.g., linking data with mental health or substance abuse datasets).
- Exclusion (algorithms performing poorly for specific groups).
- Data breaches (family members learning sensitive information).
- "Function creep": data used beyond its original purpose.

**Practical strategies:**

- Map foreseeable downstream uses and risks.
- Re-assess risks after major changes (new linkage, new tech partner, new model).
- Limit retention to what is strictly necessary.

## Privacy

https://doi.org/10.2196/56307

https://doi.org/10.1080/15265161.2023.2201191

https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/

More than confidentiality: the right to **contextual integrity** (Nissenbaum).
**Where it breaks:**

- Re-identification from innocuous data points.
- Group harms (e.g., genetic data exposing entire families or communities).

- Surveillance-by-accident (e.g., continuous app tracking).

**Practical strategies:**

- Combine technical safeguards (encryption, differential privacy) with organizational ones (access control, training).
- Treat privacy as ongoing stewardship, not a one-off compliance checkpoint.

## Trust

https://doi.org/10.2196/56307

https://doi.org/10.1080/15265161.2023.2201191

Built slowly, lost quickly.
**What erodes trust:**

- Sudden changes in data use ("we updated our privacy policy").
- Commercial partnerships without transparency.
- Overpromising and underdelivering on anonymization.

**Practical strategies:**

- Communicate uncertainty honestly.
- Document decisions and trade-offs.
- Show who is accountable — and how participants can complain or appeal.

# Building Ethical Data Systems

## Privacy-by-design

- Minimize collection
- Pseudonymize early
- Delete raw data promptly
- Limit access strictly

## Transparency-by-design

- Create audit trails
- Use dashboards/visuals to explain data flows
- Provide clear user-facing explanations (not legal jargon)

## Accountability mechanisms

- Clear data ownership
- Named individuals for oversight
- Regular audits and ethical checkpoints

## Participatory governance

- Involve patients and affected communities in designing consent, access rules, benefit sharing.
- Close the loop: report back what you learned.

## Proportional openness

https://doi.org/10.1007/s11948-024-00502-3

- Open science is not a religion — it is a tool.
- Evaluate harm before release.
- When full openness is risky, create safe alternatives (e.g., secure enclaves).

# Five Dimensions for Ethical Data Design ("Ten P Questions")

## Purpose

- Is the purpose legitimate, proportionate, and clearly articulated?
- Would participants agree if told explicitly?

## People

- Who will benefit?
- Who could be harmed — directly or by inference?
- Whose voice is missing?

## Process

- How are consent, oversight, and revision handled?
- Are responsibilities distributed or ambiguous?
- Are safeguards maintained over time, not just at launch?

## Power

- Who sets the rules for fairness, openness, and benefit-sharing?
- Can communities challenge decisions?
- Is there an appeal mechanism?

## Provenance

- Where does data come from?
- How does it transform?

- Who touches it along the way?
- Can these steps be documented and justified?

# Reflection Exercise: Your Data, Your Ethics

Take two minutes and ask:

- Which ethical tension defines your project most clearly?
- Are your safeguards legalistic (minimum compliance) or ethical (aimed at real-world protection)?
- Who participates in ethical decisions — and who should?
- If someone asked “why should we trust your data practices?” — what would your one-sentence answer be?