Framework for Data Governance and Ethical data use

Nicki Tiffin

University of Cape Town

nicki.tiffin@uct.ac.za

Why data governance?

- Health and genomic data are extremely sensitive
- Digital data are easy to copy and share

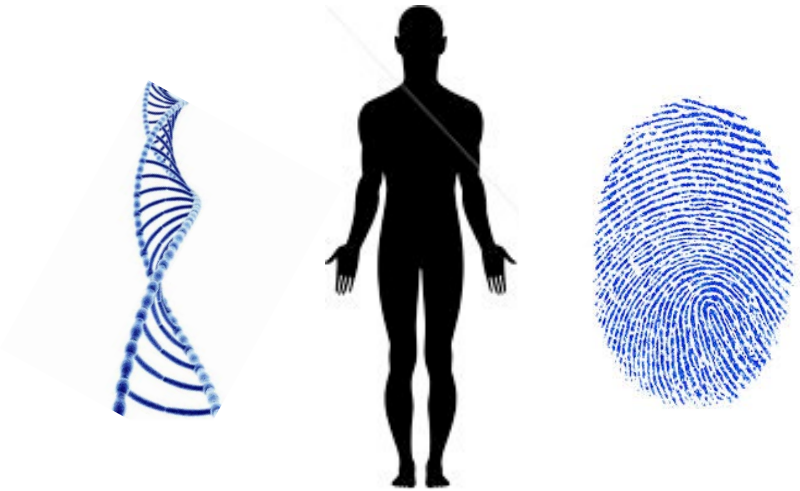
- No limit to number of copies
- No guaranteed way to delete copies

How do we ensure participant protection?

Genomic data are very sensitive

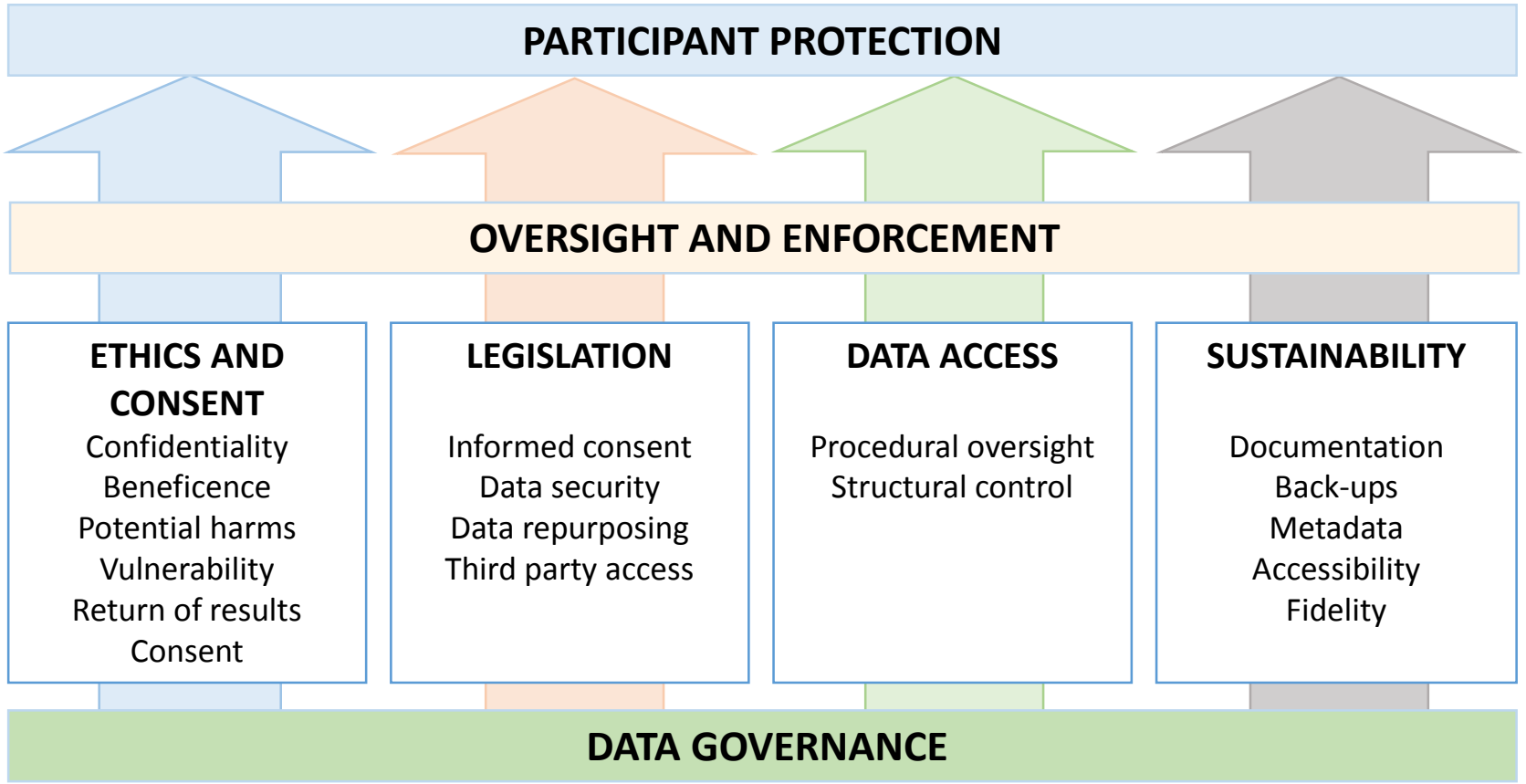
- Cannot be truly anonymised or de-identified
- (unlike clinical/biochemical data)

- "Anonymising" DNA sequence is like trying to anonymise a fingerprint
-



-Unique to an individual
-Unchanging

Data Governance Framework



H3ABioNet

1. Ethics and consent

- Ensuring confidentiality
- Beneficence: balancing benefits and potential harms
- Vulnerable populations
  - minors, low SES, poor access to health care
- Return of results, incidental findings

CONSENT: Tiered consent

- How do participants understand consent?
- primary purpose, secondary use, re-contact

- Oversight by Ethics Review Boards

Practical application
Vulnerable populations are identified and appropriate resources assigned.
Patient information describes in detail intended data use, storage and future destruction.
Tiered consent process is clearly delineated and each level of consent is stored.
Option to withdraw from study with data deletion is clearly outlined for participants.

2. Legislation

- National Legislation
- Protection of Privacy act
  - South Africa – POPI
  - EU - General Data Protection Regulation
- Health Act
- Protection of Minors Act

Practical application
Familiarity with relevant sections of local/regional legislation pertaining to personal/health data.
Identify data ownership, the responsible party for the data and key stakeholders, in collaboration with government structures.
Facilitate review by local regulators where necessary.
Comply with restrictions on moving data across borders, including identifying related issues with Cloud storage.

3. Data access controls

- Procedural oversight
  - Protocols for data requests, data access committees
  - Guidelines for data sharing
- Structural controls
  - Firewalls, login controls
  - Encryption, password protection
  - Separating sensitive data from identifying data

Practical application
Establish procedures for processing data access requests with protocols protecting against commodification, together with government stakeholders.
Install appropriate remote-delete software on devices in case of loss or theft.
Separately store and transport identifying and sensitive genomic and health data.
Store data in secure, firewall- and access-controlled locations, where possible within secure platform

4. Sustainability

- Documentation
  - Avoid person-centric knowledgebase
- Back-ups
  - Backup protocol, disaster recover plan
- Metadata
- Accessibility
- Fidelity and quality control

Practical application
Build an interoperable data structure so that data can be easily shared where appropriate.
Provide up-to-date documentation, consent information and codebooks for all datasets.
Establish a data backup plan for frequent back up to secure locations.
Implement a long term data storage and management plan that is not dependent on particular individuals or organizations.

Oversight and enforcement

Roles for:

- Legislative oversight (e.g. POPI regulator)
- Institutional oversight (e.g. Ethics review boards)
- Funders and donors oversight
- Program self-evaluation

Thank you