

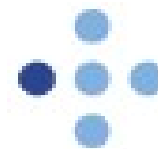
Ethics of Data Collection and Management

Daniela Elena Costea

Professor in Tumour Pathology
Experimental Pathology Research Group
University of Bergen, Norway



Centre for
Cancer Biomarkers
Norwegian Centre of Excellence – University of Bergen



HELSE BERGEN
Haukeland Universitetssykehus

Learning Outcomes

By the end of this session, you should have knowledge on:

- Ensuring integrity in data collection
- Responsible data management practices
- Data security principles
- Address data sharing and breach response
- Foster transparency and accountability

Learning Methods

- Educational Video
- Discussion Forum
- Case Study Exercise
- Reading Material

Learning Outcomes

By the end of this session, you should have knowledge on:

- Ensuring integrity in data collection
- Responsible data management practices
- Data security principles
- Address data sharing and breach response
- Foster transparency and accountability

Integrity in Data Collection

Key Ethical Principles:

- Informed Consent
- Confidentiality and Privacy
- Accuracy and Honesty
- Avoiding Bias
- Transparency
- Ethical Review
- Handling Sensitive Data
- Responsibility to Participants

Informed Consent & Confidentiality

Informed Consent:

- Purpose and procedures explained
- Right to withdraw anytime

Confidentiality:

- Anonymization techniques
- Secure data storage

Ensuring Accuracy & Avoiding Bias

Accuracy and Honesty:

- Avoid fabrication or selective reporting

Avoiding Bias:

- Use validated instruments
- Objective sampling techniques

Integrity in Data Collection

Key Ethical Principles:

- Informed Consent
- Confidentiality and Privacy
- Accuracy and Honesty
- Avoiding Bias
- Transparency
- Ethical Review
- Handling Sensitive Data
- Responsibility to Participants

Learning Outcomes

By the end of this session, you should have knowledge on:

- Ensuring integrity in data collection
- **Responsible data management practices**
- Data security principles
- Address data sharing and breach response
- Foster transparency and accountability

Responsible Data Management Practices

- Data Planning:
- Data Collection
- Data Storage
- Data Documentation
- Data Sharing and Access
- Data Integrity and Quality

Responsible Data Management Practices

Data Planning:

- Develop a Data Management Plan (DMP)

Data Storage:

- Secure, backed-up locations (e.g., cloud storage)
- Encryption and access control

Data Documentation & Sharing

Documentation:

- Maintain metadata and logs

Data Sharing:

- Ethical guidelines and anonymization
- Use repositories with persistent identifiers

Responsible Data Management Practices

- Data Planning:
- Data Collection
- Data Storage
- Data Documentation
- Data Sharing and Access
- Data Integrity and Quality

Learning Outcomes

By the end of this session, you should have knowledge on:

- Ensuring integrity in data collection
- Responsible data management practices
- **Data security principles**
- Address data sharing and breach response
- Foster transparency and accountability

Data Security

Confidentiality:

- Use encryption, anonymization techniques and secure systems

Integrity:

- Regular audits and integrity checks

Compliance:

- Legal and ethical standards
 - General Data Protection Regulation (GDPR)** in Europe
 - Sudan currently does not have a comprehensive data protection law similar to the **GDPR** or the frameworks seen in countries like South Africa or Kenya.

Mitigating Harm

Transparency and Accountability

Long Term Stewardship

Learning Outcomes

By the end of this session, you should have knowledge on:

- Ensuring integrity in data collection
- Responsible data management practices
- Data security principles
- Address data sharing and breach response
- Foster transparency and accountability

Ethical Data Sharing

Informed Consent for Sharing:

- Explicit consent for identifiable data

Confidentiality in Sharing:

- Anonymization and limited access

Fair Use and Equity:

- Promote equitable access

Data Integrity and Quality:

- Ethical responsibility for accuracy / providing detailed metadata

Data Breach Response

Key Steps:

- Prompt notification (affected participants and authorities)
- Mitigate harm (steps to prevent further unauthorized access and address any immediate risks to participants)
- Transparency and accountability
- Restoration and recovery (work with cyberexperts)
- Ethical Reflection and Improvement

Learning Outcomes

By the end of this session, you should have knowledge on:

- Ensuring integrity in data collection
- Responsible data management practices
- Data security principles
- Address data sharing and breach response
- Foster transparency and accountability

Transparency & Accountability

Transparency:

- Open methodologies
- Disclosures of conflicts of interest
- Data availability

Accountability:

- Ethical oversight and integrity
- Reporting misconduct

Case Study Exercise

Scenario: A data breach exposes sensitive participant information.

Discussion Questions:

- What steps should the research team take immediately?
- How can similar breaches be prevented in the future?

Summary

- Upholding ethical principles ensures trustworthiness and credibility.
- Integrating transparency, accountability, and robust security safeguards strengthens research outcomes.
- Ethical data practices are foundational to responsible research.

Thank You!

