Ethical and legal issues in data sharing - overview

Research Data Management Support Services
UK Data Service
University of Essex

April 2014
Ethical and legal issues in data sharing

- Legal and ethical aspects
- Informed consent for data sharing
- Anonymising data (separate session)
- Controlling access to data
- Working with Research Ethics Committees (RECs) and Institutional Review Boards (IRBs)
Ethical arguments for archiving data

- Store and protect data securely
- Not burden over-researched, vulnerable groups
- Make best use of hard-to-obtain data, e.g. elites, socially excluded, over-researched
- Extend voices of participants
- Provide greater research transparency
- Enable fullest ethical use of rich data

In each, ethical duties to participants, peers and public may be present
Duty of confidentiality and data sharing

- Duty of confidentiality exists in common law and may apply to research data
- If participant consents to share data, then sharing does not breach confidentiality
- Public interest can override duty of confidentiality
  - may need to give up data for court subpoena or to police
  - Bbst practice is to avoid vague or general promises in consent forms
Data Protection Act, 1998

- Personal data:
  - relates to living individual
  - individual can be identified from those data or from those data and other information
  - include any expression of opinion about the individual

- Requirements for handling personal data
  - processed fairly and lawfully
  - obtained and processed for a specified purpose
  - adequate, relevant and not excessive for the purpose
  - accurate
  - processed in accordance with the rights of data subjects, e.g. informed about how data will be used, stored, processed, transferred, destroyed,
  - kept secure and no kept longer than necessary
  - not transferred abroad without adequate protection

- Personal data can be disclosed only with consent
Data protection act and research

- Exceptions for personal data collected as part of research:
  - can be retained indefinitely, if needed
  - can be used for other purposes in some circumstances
  - people should still be informed
- If data are anonymised (personal identifiers removed) then DP laws will not apply as these no longer constitute ‘personal data’
Sensitive data

Data regarding an individual's race or ethnic origin, political opinion, religious beliefs, trade union membership, physical or mental health, sex life, criminal proceedings or convictions (DPA, 1998)

• Can only be processed for research purposes if:
  • explicit consent (ideally in writing) has been obtained; or
  • medical research by a health professional or equivalent with duty of confidentiality; or
  • analysis of racial/ethnic origins for purpose of equal opportunities monitoring; or
  • in substantial public interest and not causing substantial damage and distress
Best practice for legal compliance

• Investigate early which laws apply to your data
• Do not collect personal or sensitive data if not essential to your research
• Seek advice from your research office
• Plan early in research
• If you must deal with personal or sensitive data
  • inform participants about how their data will be used
  • remember: not all research data are personal (e.g. anonymised data are not personal)
Options for sharing confidential data

- Obtain **informed consent**, also for data sharing and preservation / curation
- **Protect identities** e.g. anonymisation, not collecting personal data
- **Regulate access** where needed (all or part of data) e.g. by group, use, time period
- **Securely store** personal or sensitive data
Consent needed across the data life cycle

- Engagement in the research process
  - decide who approves final versions of transcripts

- Dissemination in presentations, publications, the web
  - decide who approves research outputs

- Data sharing and archiving
  - consider future uses of data

Always dependent on the research context – special cases for covert research, verbal consent, etc.
Managing access to data

- Essential when anonymisation is ineffective or damaging
  - Visual or audio data or disclosive microdata
- UK Data Archive Access Policy has three tiers:
  - Open - no registration, but may be licenced, e.g., CC
  - Safeguarded – not personal, but disclosure risk if linked
    - Registration required, e.g., End User Licence
    - Special agreements (depositor permission; approved researcher)
    - Embargo for fixed time period
  - Controlled - may be identifiable
    - Only available to accredited users
    - May be accessed via physical or virtual secure environment
- Same study may be released with different conditions
  - Data with varied levels of aggregation
Data sharing and research ethics committees

• REC/IRBs are responsible for safeguarding participants from harm and ensuring ethical research and protecting home institutions, but are not always informed about sharing.

• There can be perceived tensions between data sharing and protection.

• We try to ensure that REC/IRBs understand that:
  • anonymised data are not subject to data protection laws
  • most funders require or encourage data to be shared
  • most research data can be shared
  • procedures (consent, anonymisation, regulating access) are available to enable ethical sharing
  • data archives ensure ethical re-use of research data, protection of participants and safeguarding of personal data.
Contacts

Collections Development team
UK Data Service
University of Essex

datasharing@ukdataservice.ac.uk