Ethical and legal aspects of managing and sharing sensitive data

Veerle Van den Eynden
UK Data Service
University of Essex

Creating Shareable Research Data: Managing and Archiving Social Science Research Data
28th and 29th November 2017

UK Data Service

Ethical arguments *for* archiving data

- 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

In each, ethical duties to participants, peers and public may be present

Ethical obligations and data sharing

- Research with human participants usually requires ethical review (Research Ethics Committee)
- Uphold scientific standards
- Comply with relevant laws
- Avoid social and personal harm
- Data archives such as UK Data Archive facilitate ethical re-use of research data, protection of participants and safeguarding of personal data
  - data anonymisation
  - regulate data access
  - data sharing is NOT violation of data privacy or research ethics

Legal Compliance

Duty of confidentiality and data sharing

- Duty of confidentiality exists in UK 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
  - Best practice is to avoid vague or general promises in consent forms

Data Protection Act 1998

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

- Only disclose personal data if consent given to do so, and if legally required to do so

Handling personal data:

- processed fairly and lawfully
- obtained and processed for specified purpose
- adequate, relevant and not excessive for purpose
- accurate
- not kept longer than necessary
- processed in accordance with the rights of data subjects
  - e.g. right to be informed how data will be used, stored, processed, transferred, destroyed
  - e.g. right to access info and data held
- kept secure
- not transferred abroad without adequate protection

DPA 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
  - for anonymised data (personal identifiers removed) DP laws will not apply as these no longer constitute ‘personal data’

- EU Data Protection Directive will be replaced by the General Data Protection Regulation on May 25th 2018
  - directly binding on all member states (not via national legislation) – includes the UK
  - key changes possible in: consent; rights of data subjects; international data transfer; sanctions; reuse for research

DPA ‘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 you 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)

Strategy for sharing confidential data

1. Obtain informed consent, also for data sharing and preservation or curation
2. Protect identities e.g. anonymisation, not collecting personal data
3. Regulate access where needed (all or part of data) e.g. by group, use or time period
4. Securely store personal or sensitive data