Ethical and legal issues in managing and sharing research data from people/organisations

Louise Corti
UK Data Service
University of Essex

Essex Big Data and Analysis Summer School
University of Essex
24-26 August 2015

UK Data Service

How to archive, share, re-use research data from ‘human participants’ within ethical and legal boundaries

UK Data Service

Research with people as participants

- Research data may contain personal data that allows living individuals to be identified
  - Data protection / privacy legislation
  - Inform participants how personal data will be used, stored etc.
  - Store securely, avoid disclosure
  - Need consent from participant to share such data

- Research data may contain confidential information - information given in confidence, agreed to be kept confidential (secret) between two parties
  - E.g. information on business, income, health, political opinion,…
  - Legal duty of confidentiality
  - Ethical: do no harm
  - Need consent from participant to share such data

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
  - 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 do

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

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
  - 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 a General Data Protection Regulation in 2015
  - Directly binding on all member states (not via national legislation)
  - Key changes possible in: consent; rights of data subjects; international data transfer; sanctions;

    reuse for research

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)

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

Data sharing and research ethics committees

- REC/IRBs are responsible for safeguarding participants from harm, ensuring ethical research, protecting home institutions
- Not always fully informed about data sharing requirements
- Perceived tensions between data sharing and protection
- 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

Questions

Contact details

datasharing@ukdataservice.ac.uk
http://ukdataservice.ac.uk/manage-data.aspx