

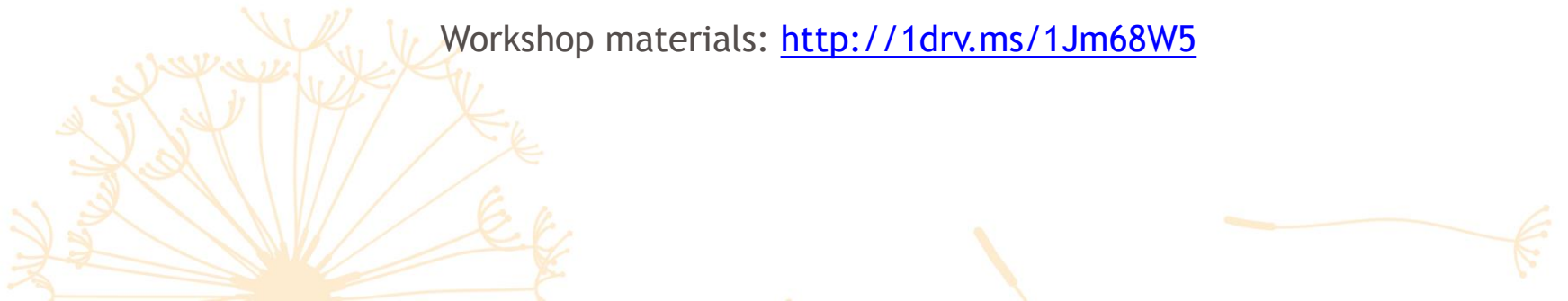


Facilitate Open Science Training for European Research

RESEARCH DATA MANAGEMENT AND OPEN DATA

6-7 October 2015
University of Manchester, UK

Workshop materials: <http://1drv.ms/1Jm68W5>



LEGAL AND ETHICAL ISSUES IN DATA SHARING

Libby Bishop, UK Data Service



UK Data Service



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



Ethical and legal issues in data sharing

- Benefits of sharing data
- Legal and ethical issues to consider
- Best practices to enable sharing
- Research Ethics Committees(RECs)

Sharing Data - Debate!

- Groups of 5-6 on left-hand side of the room: generate AS MANY reasons as you can for why researchers *should* share their data.
 - What are the benefits of sharing data?
 - Who does sharing data benefit?
 - How does it benefit them?
- Groups of 5-6 on right-hand side of room: generate AS MANY reasons as you can for why researchers should not share their data.
 - What are some of the downsides of sharing data?
 - What are some of the impediments to sharing data?
 - What are some of the concerns associated with sharing data?
- Take about 6-8 minutes.
- Then we'll come back together and debate the issue!



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

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 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

FOSTER

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, or private content *can* be shared

- 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.

Consent, and alternatives

- If strictly interpreted, then may require explicit, specific consent; written - exemptions?
- Broad consent - Genome Project, biobanks. Accepted in UK, but not across Europe (e.g., Germany)
- Dynamic consent - maintain contact, seek content for any new use “substantially” different from original
- Alternative legitimate basis
 - Administrative Data Research Network
 - Access review committees - medical, Understanding Society
 - Citizen panels
- Proposed EU General Data Protection *Regulation*

Sensitive data can be shared - *ethically*

- Timescapes Qual Longit data
 - sensitive data; 95%+ consent
- Foot and mouth disease in N. Cumbria
 - highly sensitive community information
 - 40/54 interviews; 42/54 diaries; audio restricted
- Bio-bank data—enduring consent
 - no time limits; open reuse
 - 99% consent rate (2500+ patients) – Wales Cancer Bank
- Conflict Archive on the Internet
- Witness to Guantanamo

<http://ukdataservice.ac.uk/manage-data/plan/checklist.aspx>

Managing access to data - UKDA

Open

- available for download/online access under open licence without any registration

Safeguarded

- available for download/online access to registered users who have agreed to an End User Licence; some special conditions

Controlled

- available for remote or safe room access to authorised, authenticated, and trained users whose research proposals have been approved

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