Ethics and Data Sharing

Michael Martin

Chair, Humanities and Social Sciences Delegated Ethical Research Committee
Chair, Science and Medical Delegated Ethical Research Committee
Australian National University
It can be ethical to share data

• Allowing data to be used “for future research” by other researchers is supported by the National Statement on Ethical Conduct in Human Research

• “Allowing” means “making provision for” and “facilitating”
Ethics is about

- Identifying risks
- Informing about risks
- Balancing risk vs benefit
- Gaining consent keeping the above in mind
- Working to mitigate these risks even once consent is gained
- Seeking to minimise ongoing risks
Best Practice

• Seek consent for re-use
• Any future use should – if possible – check for ongoing consent (not always possible)
• Is the data sensitive (i.e. might harm be done if it were made known in its existing form)? If so, de-sensitize
• Never give sensitive data away without express consent
But what if it is sensitive?

- Ask first – if explicit consent for future use has been sought and acquired, then it’s easy
- If the data is sensitive then it can be confidentialised so that the sensitivity is removed
- Sometimes you cannot go back and get consent – but even then it is critical that the identity of the respondent is NOT linked
Confidentialising

• Is more than just removing names
• For example, if you know my address it will be easy to find out who I am
• And that’s just the start…

• Direct identifiers include name, initials, address, telephone number, e-mail, photos, audio, among others
How much do you need to know about me to know who I am?

• Searchable or relatively “public” information will identify me – even if my name is unknown.

• Other, less public information – indirect identifiers might identify me if I collect them together and “build a case”

• e.g. Statistician, 6’5” tall, born in Toowoomba = Michael Martin…
Sensitive Data

• Carries inherent risk unless it is managed and protected properly
• Even with management, risks remain (third-party identification, small populations, even “guesses”)
• Later use of data – with or without express consent – raises risk further.
Confidentialising Data

• Reduces risk to the participant
• Usually doesn’t damage the usefulness of the data
• May not be simple, and sloppy or incomplete confidentialisation may lead to “jigsaw attacks” – piecing together identity
To be ethical

- **Be aware** of what participants were told about data re-use – if they were told it would NOT be re-used, then it CANNOT be re-used as that was a condition of consent.
- **Be aware** of what they were told about how data would be accessed, stored and deleted. It is not OK to keep it, remove names and re-use it IF you told participants you would destroy it!
- If you don’t have this information, at least ask!!
BUT it *would* be ethical if

- The original data was gathered but nothing explicit was said about re-use (i.e. nothing explicitly allowing it, but nothing explicitly precluding it either)

THEN

- Data can be safely shared provided it is
  - confidentialised; AND
  - there is no reasonable risk of harm from the use of confidentialised data.
Small populations present issues

• Indigenous populations
• Rare conditions
• Unusual or memorable features

• All raise the stakes and can make confidentialisation difficult to impossible
• E.g. ABS even deliberately changes data to reduce this problem
Main Message

• Always think about the effect on participants
• Do “worst case” analyses and plan accordingly
• Plan to share or re-use data by building it into processes before data collection – i.e. seek consent!
This work is licensed under a Creative Commons Attribution 3.0 Australia License

NCRIS
National Research Infrastructure for Australia
An Australian Government Initiative

ANDS is supported by the Australian Government through the National Collaborative Research Infrastructure Strategy (NCRIS).