4. MANAGEMENT OF PERSONAL DATA:

Data Protection, Information Security, Secondary Use of Data, Anonymisation, Confidentiality, Sharing Personal Data, Data Retention

Author: Ellen Paterson and Rachael Mold
Date: 9th August 2017 (Version 1)

DATA PROTECTION

Researchers’ use of personal data must comply with the Data Protection Act 1998 (DPA) and, from May 2018, The General Data Protection Regulations.

- Data protection legislation is complex but well established in the UK and EU. In the UK, compliance with the law is regulated by the Information Commissioner, whose website is the primary source for comprehensive but easy to digest guidance. Jisc have also produced data protection guidance specifically for researchers.
- The University portal contains both data protection guidance and the UEA data protection policy.
- Researchers should ensure that any information given to research participants (e.g. in information sheets or similar) is sufficient to satisfy the fair processing requirements. The Information Commissioner’s ‘privacy notice’ guidance outlines the information that must be provided at point of data collection.
- Researchers who rely on participant consent for handling personal data must be able to satisfy the conditions for consent.
- The DPA contains limited exemptions, including a narrowly-defined exemption for research data, and for data processed for the purposes of Journalism, Literature and Art.
- Many other countries have privacy laws, but these may not be considered to give equivalent protection to data subjects. Researchers should therefore seek advice if their activities will involve transfer or storage (including cloud storage) of personal data outside the EEA.

INFORMATION SECURITY

Information security is a critical component of data protection, but is not limited to the protection of personal data. Ensuring adequate information security is important for all types of research, and will in many cases be a prerequisite for obtaining third party datasets. Provisions for data security at the end of a project should be made clear in the Data Management Plan.

For advice on information security, contact infosec@uea.ac.uk.

SECONDARY USE OF DATA

When obtaining personal data from third parties, care should be taken to ensure those parties are entitled to share that information, and are doing so in accordance with the data subjects’ legal rights. You should consider whether you will need to obtain consent from the data subjects, and what information about the research should be or has been made available to them. The UEA Research Ethics Policy does require review for secondary use of data even if the provider of the data does not request it. This is to ensure appropriate anonymization and consent arrangements are in place.

Access to health service data is now managed by NHS Digital via the Data Access Request System (DARS) http://content.digital.nhs.uk/dars. You will need to work with the team in the Research and Innovation Services (RIN) via your Project Officer to complete the Health and Social Care Information Centre
application form available from this link and cross reference to existing agreements UEA has about use of health service data sets for research. RIN has a couple of examples of applications made previously via this route. RIN will refer to the UEA Information Security team as needed.

Further guidance on using secondary data in research is available at:

The Research Ethics Guidebook - a resource for social scientists http://www.ethicsguidebook.ac.uk/secondary-analysis-106

ANONYMISATION
• Wherever possible data should be collected, stored or handled in anonymous form. If that is not possible, personal data should be pseudonymised\(^1\) and/or processing kept to a minimum.
• The ICO has published an Anonymisation Code of Practice: https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf
• The UK Anonymisation Network (UKAN) provide information and support for practitioners to discuss issues relating to anonymization: http://ukanon.net/
• UKAN have also published the Anonymisation decision-making framework ebook: http://ukanon.net/wp-content/uploads/2015/05/The-Anonymisation-Decision-making-Framework.pdf

CONFIDENTIALITY
A researcher may not disclose the identity of a person nor disclose any information that could identify that person without having obtained, prior to the person’s participation, the person’s consent in writing. If it is necessary to identify participants explicitly, then the researchers should explain why this is the case and how confidentiality will be protected.

Researchers should be aware of the risks to anonymity, confidentiality and privacy posed by all kinds of personal information storage and processing which directly identify a person, e.g. electronic and paper-based files and communications. Measures to prevent accidental breaches of confidentiality should be taken, and in cases where confidentiality is threatened, relevant records should be securely destroyed.

Research involving NHS data must comply with the requirements of NHS Information Governance: https://www.england.nhs.uk/ourwork/tsd/ig/

SHARING PERSONAL DATA WITH OTHERS, INCLUDING TRANSCRIPTION SERVICES
• UEA, as a data controller, is legally required to have formal written agreements with all third parties who handle personal data on its behalf (data processors). This includes companies or individuals offering a transcription service. UEA has a standard Data Processor Agreement template that can be used for this purpose.

\(^1\) Defined by Article 4 of the GDPR as meaning ‘the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person’
• Researchers may also need to share personal data with other data controllers (e.g. collaborative projects with other HEIs). From May 2018, joint controllers will need to have agreements or protocols in place, which set out their respective obligations for data protection compliance. The researcher must maintain records of all such agreements, to enable the University to comply with the forthcoming changes to data protection law. Contact dataprotection@uea.ac.uk for advice.

DATA RETENTION
• The DPA requires that personal data must be kept no longer than necessary, but also recognises that some research data may, in specific circumstances, need to be kept indefinitely. There is therefore a lack of consistency as to how long research data involving identifiable individuals should be retained, although it is likely that external funding bodies may impose their own retention periods.
• The University has published guidance on research data management.
• Individual UEA departments also maintain records retention schedules, which outline how long they will store information.
• For healthcare studies where UEA is the Sponsor, the retention requirements are detailed in SOP 900: Storage and Retention of Research Documents (available from the NNUH website under research).