Research Data Management

Guidance on the Retention of Research Records and Data

Version 4.0 March 2023

University of Bristol

Research Data Service

Image: By Black and White, Wikipedia , CC-BY-SA-3.0

University of BRISTOL

INTRODUCTION

This guidance deals with research records and data specifically relating to human participants, their tissue, and/or human data. This includes administrative documentation such as procedures, consent forms, protocols, approvals and reports, and also aspects of research data produced during the course of a project, including primary and derived datasets, instrument readings, databases, samples and images. Collectively, this information can provide evidence of research integrity and strengthen the validity of research findings, as well as demonstrate compliance with legislative requirements.

1. Why manage the retention of research records and data?

Projects involving human participants and their tissue/data by nature generate information which is sensitive and often governed by formal legislation. As a result, there are often additional requirements with regards to the collection and retention of this information. These can be imposed by external funders, regulatory bodies, collaborating organisations, and specific acts/legislation. Effective management of the retention of research records and data will ensure you meet these requirements.

2. Who is responsible for managing research records and data?

Researchers, especially those working with human participants, their tissue and/or data have a responsibility to keep clear and accurate research records, giving due consideration to the requirements of anonymity and confidentiality. In as far as it is possible, this should include any documentation required to facilitate the reconstruction of a study and support a complete retrospective audit, if necessary.

The person with ultimate responsibility for managing the research records and data is the Chief Investigator, herein also known as the Data Steward. If the Data Steward subsequently leaves the University or is absent for a prolonged period of time, their line manager will, in the first instance, assume the responsibilities of Data Steward.

3. How long should research records and data be kept?

It is important to protect the integrity and auditability of your research. Each research project is unique and judgement is required to determine how long records and data should be kept. Researchers must determine the retention requirements for their research records and data on a project-by-project basis, or at least for clearly defined categories of projects, taking account of:

- The legal and regulatory framework for particular types of research;
- The terms and conditions imposed by external research sponsors/funders/potential publishers;
- The commercial, political or ethical sensitivity of particular types of research, or any research for particular external sponsors; and
- The University's Records Retention Schedule, section 4.3.[1]

[1] University Secretary's Office, Records Retention Schedule (IGP-04)

Research carried out for the NHS or under contract for a commercial organisation is subject to that body's own archiving, data protection and retention policies. Researchers should be aware of the archiving policies of other organisations involved in their research.

Before a project starts, the Data Steward should compile a Records Retention Schedule/Archiving Plan, listing all records that will be produced during the project and how long these will be retained for. The Records Retention Schedule/Archiving Plan should be produced in conjunction with a Data Management Plan, which will outline how research data will be generated, managed and remain accessible. Many funders now require Data Management Plans as part of the application process. The University's Research Data Service (http://data.bris.ac.uk) can offer further advice in producing Data Management Plans.

Actual retention periods should be informed by both the research funder's policy, and the aims and objectives of each study. Valuable research data and associated metadata should normally be retained for a minimum of ten years after a study has concluded. Records from studies with major health, clinical, social, environmental or heritage importance, novel intervention, or studies which are ongoing or controversial, should be retained for at least 20 years after completion of the study.

4. Keeping information secure

Due to the often sensitive and confidential nature of the information created and managed during research projects involving human participants, it is imperative that appropriate security measures are in place, both during and on completion of the research, and that all staff are aware of the need to keep information secure. Storage should be "fit for purpose" and provide adequate space, security, access control and environmental conditions. All participant-identifiable information, whether paper or electronic, must be stored with adequate security measures and only stored for as long as absolutely necessary (further information on the Data Protection Act is included in section 7.3 of this document).

The following should also be noted:

- A custodian should be designated for any archived information;
- Records and data should be stored in line with funder, sponsor, and University policies;
- Records and data should be stored in a way that permits a complete retrospective audit if necessary;
- Records and data should be safely stored, with appropriate contingency plans e.g. extra copies, in a format that is viable in the future;
- Records and data, particularly personal data, should be treated in confidence, i.e. kept securely with no unauthorised access;
- Should the research team cease to exist, or the research lead moves to another organisation, the expectation is that the responsibility for their information passes to the University that hosted their research activity;
- Research hosted within the NHS should comply with the data retention policy of the host Trust, provided that the minimum requirements of this guidance are adhered to.

The University has an Information Security Policy (http://www.bristol.ac.uk/infosec/policies/) that both complies with stringent legal requirements and provides the necessary assurance that information held and processed by the University is treated with the highest appropriate standards to keep it safe.

4.1. Paper records

Paper records must be kept in locked cabinets and in locked offices or storage rooms, if unattended. Access to cabinets, offices and storage rooms must be restricted to authorised personnel only.

Transferring information into an electronic form is permitted as long as the following conditions are met:

- The study is not going to be submitted to regulatory authorities;
- The study does not involve the administration of medicinal substances or any intervention which could represent a risk to the subjects' health;
- The main papers relating to the relevant study have been published at least 12 months earlier and no substantive queries have been raised.

Once the information has been transferred into an electronic form, the paper records can be destroyed in an appropriate manner, either using a cross-cut shredder or by using the University's confidential waste service. Prior to scanning and destroying any records, the following must be documented and stored in the project master file:

- An accurate description of how any data was transcribed from the paper format to the electronic database and the quality assurance steps that were taken to ensure the accuracy of the transcription;
- The process for scanning the paper records and the quality assurance steps that were taken to ensure the scanned image is of sufficient quality that it represents an accurate and useful copy of the original. The process must be robust and secure to uphold the integrity of the scanned image, e.g. it should not be possible for an unauthorised person to modify an image, and any authorised changes must be recorded in an audit trail or change log;
- Where the electronic data is stored and the retention period or criteria;
- The proposed destruction process; how, when and by whom.

The resulting electronic records should be kept as described below.

4.2. Electronic records and data

Appropriate technical procedures should be established to ensure that instances of unauthorised access, loss, or misuse of records and data do not occur. These procedures should apply to both on and off-campus activity and especially if staff work from home. During the course of your project the following good practice should be adhered to:

- Computer screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons;
- Ensure that your PC is locked whenever you are away from your desk;

- Passwords should never be shared with other members of staff and should be changed on a regular basis (and always when a member of staff leaves the project);
- Each study database should be password protected, with its own unique password, with access to the password restricted to authorised personnel only;
- Where identifiable data is not a requirement of the research project, then the data should be retained in an anonymised format;
- All records and data should be archived in a durable form that cannot be subsequently amended or tampered with;
- Records and data should be held on secure networks – the University of Bristol has its own Research Data Storage Facility[2] (RDSF) which provides secure, long-term storage for research data. Suitable storage is also available in some schools/departments.

In cases where it is necessary to remove research records or data from the University, appropriate security measures must be taken to protect the data from unauthorised disclosure or loss. "Strictly Confidential" data in electronic form must be strongly encrypted prior to removal. Particular care needs to be taken when information assets are in transit. University supplied mobile devices must always be fully encrypted. Secret data must never be removed, except with the explicit written permission of the data owner.

5. Consent

Where the research involves human participants, it is vital that proper informed consent is obtained from individuals. Consent should generally be in writing and constitute a part of the research records and data for scrutiny; a lack of proper informed consent may raise concerns over the validity of the research results. Any consent should be obtained in accordance with professional standards and guidelines in the field of research, and should contain information on storage, retention, data sharing and anonymising of data. For more information on consent forms and archiving see: https://www.ukdataservice.ac.uk/manage-data/legal-ethical/consent-data-sharing.aspx.

A number of funders and publishers now require researchers to make their anonymised primary research data available for sharing with the research community. This needs to be fully reflected in patient information sheets in order to comply. There will always be exceptions to this requirement, particularly when the research involves very small cohorts for participant recruitment, highly sensitive research, and commercially sensitive research. The ethics review process will advise on this aspect of research.

Signed paper consent forms or other non-digital records may contain identifying information and should be stored separately from data files, although an anonymous ID system can help link the two sets of materials together if required (e.g. for re-contacting purposes).

[2] http://www.bristol.ac.uk/acrc/research-data-storage-facility/

Consent forms may be digitised for ease of storage, as described in section 4.1. Whether in paper or digital format, consent forms must be retained as long as other research records and study data exist. This requirement applies even if study data has been anonymised.

6. Record Destruction

Some research records and data associated with human participants and their tissue and/or data will need to be destroyed at the end of a given retention period, in order to comply with funder and legislative requirements, or simply as part of good records management practice. Your Records Retention Schedule/Archiving Plan will have identified which items are suitable for destruction after a given period. It will be appropriate to review the records with a department/study unit every five years to see if they still need to be retained given the current research and policy environment and events that have happened subsequent to the end of the research.

Research records and data must be destroyed in a robust and secure way:

- Paper can be destroyed using either a cross-cut shredder or by using the University's confidential waste service;
- Hard drives and other electronic media must be destroyed using a University approved method for hardware disposal.

A record of the destruction should be kept including what was destroyed, when it was destroyed, and who did it. More information and advice on hardware and data disposal is available from https://uob.sharepoint.com/sites/itservices/SitePages/disposal.aspx.

7. Statutory considerations

7.1. Clinical Trials of Investigational Medicinal Products (CTIMPs)

Record retention for CTIMPs should be undertaken according to UK law. Further details concerning governance of clinical trials are available at www.gov.uk/government/organisations/medicines-and-healthcare-products-regulatory-agency.

A Trial Master File should be set up at the beginning of a trial and maintained throughout the trial in accordance with Good Clinical Practice. There is more specific and detailed guidance at www.ct-toolkit.ac.uk which outlines which records are essential to be archived and how these documents should be stored, for what duration, lines of responsibility and how and when they should be destroyed.

A data manager and/or data monitoring committee should be appointed for CTIMP studies and should take into account the regulations, this guidance, and whether the trial data will be used for the licensing of any medicinal product. All of these factors will influence the record retention schedule for the study.

The Research Governance Team in the Division of Research, Enterprise and Innovation can help you plan a pathway through the complex regulatory landscape to ensure all the necessary requirements are in place before the study starts. See http://bristol.ac.uk/red/research-governance/ for more information.

7.2. Human Tissue Act

There are some special considerations when storing Human Tissue or data relating to human tissue for future research use:

- Consent for long-term storage and future research use should have been obtained, wherever practicable. Where consent has not been obtained, only anonymised data should be retained;
- NHS Research Ethics Committee (REC) approval for storage and future uses should be obtained;
- A dedicated custodian should control storage and use;
- Data and tissue samples should be held securely;
- Tissue samples should be stored according to quality requirements, i.e. frozen at the correct temperature, with machines robustly monitored, and storage locations known;
- Electronic information should remain accessible and usable;
- A summary of key data items or types of samples should be made available to the research community;
- Access should be governed appropriately.

If planning to store human tissue samples in England, Wales or Northern Ireland, beyond the life of an NHS REC approved research project and before a new project begins, an HTA licence will be required. A summary of HTA licensing requirements and advice is available from www.bristol.ac.uk/red/research-governance/human-tissue/.

7.3. Data Protection Act

When storing any kind of personal data, the principles of the Data Protection Act 2018 must be met. There is a separate University policy on Data Protection (www.bristol.ac.uk/secretary/data-protection/). Personal and sensitive information can be securely retained by anonymising or coding data and storing identifiers separately. Where consent has not been obtained to retain personal information or personal information is not required by the proposed study, only pseudonymised or anonymised information should be stored. Your requirements should be monitored throughout your study to ensure that you are only collecting required information.

7.4. Freedom of Information Act

Most requests for information are informal and part of routine 'business as usual' and need not be treated as FOI requests. If you would normally agree to share the records and data, you should continue to do so, paying due care and attention to normal research considerations, e.g. ethics, privacy and confidentiality. However, research data can be the subject of a formal Freedom of Information request. You should consult the University's Information Rights Officer (freedom-information@bristol.ac.uk) if any of the following apply:

- The request is specifically identified as an 'FoI Request'
- You believe there are legal or ethical reasons why the data shouldn't be supplied
- You don't want to supply the data for any other reason

Explain the request, and the reasons why you don't want to or cannot supply the information and the Information Rights Officer will work with you to help resolve the request.

8. Further Reading and References

UoB Research Data Management	http://data.bris.ac.uk
UK Data Archive	https://www.ukdataservice.ac.uk/manage-data/legal-ethical.aspx
Study Closure and Archiving: Archive Data/Tissues	https://www.ukri.org/councils/mrc/facilities-and-resources/find-an-mrc-facility-or-resource/mrc-regulatory-support-centre/using-human-samples-in-research/
Clinical Trials of Investigational Medicinal Products	http://www.ct-toolkit.ac.uk/
Data Protection Guidance	http://www.bristol.ac.uk/secretary/data-protection/
UoB Institutional Policy on Open Access to Research Publications	https://www.bristol.ac.uk/media-library/sites/library/documents/open-access/uobpolicy.pdf