University of Sussex

Research Governance Standard Operating Procedure

The Management and Use of Research Participant Data for Secondary Research Purposes

SOP Reference:	**SOP/RGO/01**
Version Number:	**01**
Date:	**28/02/2014**
Effective Date:	**28/05/14**
Review by:	**28/05/16 (Two years from effective date)**
Author:	**Ms Isla-Kate Morris**
Author designation:	**Research Governance Officer, University of Sussex**

Version	Effective Date	Reason for Change
01	TBC	N/A

Disclaimer:

- When using this document ensure that the version you are using is the most up-to-date either by checking on the Research Governance webpages for any new versions or by contacting the author to confirm the current version
- Staff and students may print off this document for training and reference purposes but are responsible for regularly checking for the current version. Any print-off of this document will be classed as uncontrolled
- Out of date documents must not be relied upon.

Table of Contents

Purpose and Introduction

The UoS is committed to promoting and upholding the highest quality research and using the data resulting from this research to benefit the wider society, the public and the academic community. Collecting and making available data from research projects that have other potential research value must follow the procedures in this document.

This Standard Operating Procedure (SOP) intends to help you follow a standard protocol when setting up a database that intends to retain data from University of Sussex (UoS) research projects for future research purposes and to manage the database in a way that ensures high quality data, data management practices and respects the goodwill of research participants. This SOP aims to encourage best practice and does not expect to restrict

research activity. These stipulations are not in place to constrict publication of research based on such databases (non-identifiable) or collaboration.

It is intended for UoS staff acting as Database Manager and to provide guidance for using the database as an administrator, editor (including data entry) or researcher. It can be used for reference and for training. Students are welcome to use this as an example of best practice.

Definitions in the context of this SOP

Database: Database refers to data collected as part of a study, which are retained for future secondary research purposes with consent. For example, participants who have undergone a brain scan for one study by one researcher may consent to the scan and related information to be used by other researchers for subsequent separate studies, the scan and information can be stored in such a database. This SOP can be followed for data retained which is identifiable or anonymised. Annex A gives more detail about the difference in definition and requirements for identifiable data.

This SOP excludes databases of potential research participants e.g. contact details.

Database Manager: The Database Manager can be a named UoS staff member with managerial responsibility for the database and those data. The database manager will:

i. Maintain a list of authorised personnel and their level of data access privileges for the database
ii. Deal with participant enquiries and withdrawals (if relevant)
iii. Receives and considers applications from researchers to access those data.
iv. When receiving new data original data collection ethics approval to ensure this is permitted in study approvals and with participants knowledge
v. Maintain an up-to-date knowledge of responsibilities and obligations
vi. Responsible for training and induction of any individuals using the database
vii. Maintain a list of researchers with access to the database.

Research participants: Participants in this context can be healthy volunteers or NHS patients. In the context of NHS patient data, compliance with NHS Research Ethics and all other regulatory approvals will be mandatory for that research project and supersedes this guidance in the event of a conflict.

For identifiable participant data refer to Annex A

Data Protection

The Data Protection Act (1998) states that anyone who processes personal information[1] must comply with eight principles which ensure that personal information is:

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive

[1] Personal data is defined as any information relating to a living person and which can be identified as referring to him or her is included, whatever the format (electronic, paper, film, tape, text, still and moving image).

4. Accurate and up to date
5. Not kept for longer than is necessary
6. Processed in line with your rights
7. Secure
8. Not transferred to other countries without adequate protection

The University's information on the Data Protection Act can be found here: http://www.sussex.ac.uk/ogs/policies/information/dpa

The Data Protection principles are best practice standards to follow, however principles two and five are restrictive for such databases as the purposes are not limited and those data are retained for future research purposes.

Please refer to Annex A to see how requirements differ in the management of identifiable data.

Access and Security

Access to information or research data for secondary research should be on a strict need-to-know basis. Only individuals who have made a sufficiently robust application to the Database Manager to access information should have access granted and should only be permitted access to information required.

Everyone with access to this information should be made aware of their responsibilities before they begin using the database by the database manager. Individuals intending to have access to those data or to the database must be made fully aware of their responsibilities and obligations. This must be part of their training and induction to use the database by the database manager, or nominated individual, providing training and/or induction.

It is the database managers responsibility to monitor who has access and amend those permissions, as appropriate, to both encrypted files on a University system shared drive or database. Any staff members, including the database manager, or supervised students who may be leaving the University or where it is no longer appropriate for access to be allowed, access should be terminated.

Data are ordinarily only permitted to be used by staff and students of the University. Data sharing may be permitted on the condition that a data sharing agreement is in place or data sharing is explicit within an agreement or study protocol for a collaborative research project and on the condition that the consent and ethical approvals allow such sharing.

Research Governance and Ethics

Expedited ethical review

Before a new database can be set up, expedited ethical review will be required. Permission to begin development will be dependent on a favourable opinion from the Chair of an appropriate University Research Ethics Committee, the University's named Data Protection Officer and the Research Governance Officer. To clarify, this is not ethics approval for original data collection but for data retention for future research purposes.

Ethical review: Application process

To apply for expedited ethical review, complete the online ethical review application form on Sussex Direct>Research>Ethical Review. The application should be raised and submitted by a permanent member of staff, acting in the role of Database Manager. When the form is submitted to the appropriate Ethics Committee, an email must also be sent to the Research Governance Office (rgoffice@sussex.ac.uk) to notify them.

Informed consent from participants

Ethics approval for projects

For projects/studies appropriate ethics must be sought and given. This is separate from the expedited review the database requires for set-up.

The projects ethics application must explicitly state the intention to use the results for secondary purposes and must include the consent form and information sheet for that database and the date of when the database was provided with expedited ethical approval. Subsequently consent for both purposes will need to be sought from participants.

Consent form and Information sheet

All databases must have their own consent form and information sheet for UoS projects to use across the University (templates are available annexed in this document). Participants consenting to their data being retained and re-used will give consent to the secondary research purposes of the database while agreeing to participate in the project they have been recruited for. It is the responsibility of the researcher to make this explicit and clear for the participant using lay terms.

Data management

The following standard procedures and operational guidance on data entry, processing and validation will help to achieve the highest quality of data and record management and ensure data integrity.

Data entry and processing

It is recommended to implement and maintain:

- A secure system that prevents unauthorised access to the data
- A list of individuals who are authorised to make changes and enter data
- Documentation on data queries, corrections and audit trail/traceability of changes or edits made
- Adequate back-up of the data (including sufficient disaster recovery and business continuity plan)
- A list of the individuals who have requested access and the specifics of their request, including dates, relevant approvals, whether their request was accepted and when those data were provided to them
- Mechanisms to check and maintain the database regularly
- The timescale for retaining those data collected should reflect the anticipated value of those data in the future. It is recommended that when a database is seeking ethical review the applicant states how the data may be used in the future, the value of

retaining these data, and how appropriate storage, management and access will be organised in the future.

Data validation

Data validation identifies inconsistencies and missing errors to allow them to be corrected or clarified. It is recommended to conduct systematic and logical checks to ensure consistent reporting between relevant fields and that there are no implausible differences between fields e.g. male and pregnant. Post data entry checks should be performed to check for missing values and values outside of the pre-defined or expected range.

Ensuring data integrity

The following are recommended:

- Data coding when handling personally identifiable data (if appropriate), what coding systems or dictionaries are used, how are the coding systems documented and secured/protected, what checks are applied to coded items and what trail exists for coding edits
- Raising data queries and traceability of data corrections
- A method of data validation must be carried out including internal validation checks performed on it before use, a method for generation of error reports. If validation checks are not programmed validation is performed by manual review
- If individuals are able to enter data it is recommended that data entry screens are set-up to limit possible data entry errors, e.g. by not accepting dates outside a specific/expected range
- A method of audit trail must be set up in order to record when data is edited and by whom
- The database will require a method of authorisation of data on the database. Databases are secured with restricted permissions to authorised users only
- A list of authorised personnel and their level of data access privileges for each database should be recorded by the Database Manager.

Best practice

It is recommended to:

- Operate a clear desk policy, especially when hot-desking, working in an open plan environment or public access area
- Any identifiable information in hard copy or on other media should also be kept in locked storage
- Users must be issued with and use a unique username and a password that no one else knows
- Users must always lock their PC or laptop when leaving their desk for short periods, when leaving the desk for long periods it is recommended to log off
- If using an encrypted USB memory stick (see section on this) for short term data storage users must never leave their USB memory stick unattended at their work station, unless in a locked cupboard/drawer.

Withdrawal and periodic reminders to participants

Participants have a right to withdrawal of their data and they should be informed of how they can do this and when the cut-off point is e.g. prior to being anonymised. If appropriate, participants can receive periodic reminders, at a frequency as agreed in their consent and information sheet, within this correspondence the participant can be reminded of their right to withdraw consent and how to do this. For a large cohort or for data which is fully anonymised periodic reminders to participants may not be practical or necessary.

Disaster recovery

At UoS each school carries out an annual risk plan which covers disaster recovery, any databases should be included in this. The University's IT policies and systems are robust and there is a daily back up of data to the University server. Each database must develop back-up and disaster recovery plans including consideration to business continuity.

Methods for sharing data from the database to an individual researcher or research team

Providing the database is set up and used in such a way that complies with this SOP and the relevant study approvals, the method of how to share the data from the database to individual researchers can be agreed on a case by case basis for that database. These are some recommended methods in which data can be shared with individual researchers to limit errors and prevent security breaches;

- A researcher can apply to the database manager to access data. The access request must be specific and justified to those data and information required for the study or project. Those data provided to the researcher must apply the third Data Protection principle[2].
- The recommended method for data sharing with University staff and students who have successfully applied to access specific data for specified purposes will receive those data through an encrypted folder on a shared drive (e.g. password protected) within the University IT system
- Where a data sharing agreement has been agreed between the University and another party either within a standalone agreement or within a collaborative agreement or study protocol, the method of data sharing will be agreed between the parties to assure the integrity and security of those data
- Small portable media devices (e.g. memory sticks, external hard drives, personal computers, smartphones or laptops) should not be used as a primary store for data for long periods of time by a researcher and should always be encrypted if used for short periods of time
- It is recommended that a very limited number of individuals are able to enter data, file and store the data from other projects and retrieve data requested from individual researchers
- The number of individuals with access should be limited and a written record of those individuals with access must be maintained by the database manager or administrator.

Training requirements

New users of the database should be trained as appropriate to that database, appropriate to their authorisation level and to how they will be expected to interact with it. As part of an individual's induction to use the database the database manager, or nominated individual, must provide training. If the individual will be expected to enter or edit data then the database manager must perform quality control checks on data entry performance to ensure competency.

[2] Those data provided must be "adequate, relevant and not excessive".

Acknowledgements

- Data Protection Act 1998
- BSMS Tissue Bank: SOP Human Tissue Act Research, Recording of Sample Data onto FreezerPro SOP/HTA/007 v.1.0 1/11/2010 (accessed 18/10/13)
- CISC Clinical Operations Policy / Procedure Data Protection Policy V1.2 01/12/12 (accessed 21/10/13)
- Cardiff University SOP for Data Management CU/08/S20/4.0 (accessed 24/10/13)
- Imperial College London JRCO SOP on Data Management JRCO/SOP/020 v6.0 (accessed 24/10/13)
- The BrainShare project: Consent form and information sheet (accessed 05/11/13)
- Research Governance, University of Bristol
- Research Governance, University of Cardiff
- The Royal College of Radiologists Academic Committee

Annex A

Identifiable data

The Data Protection principles are best practice standards to follow, however principles two and five are restrictive for such databases as the purposes are not limited and those data are retained for future research purposes.

Identifiable data should only be accessible to a study's Principal Investigator and only accessible to the research team when justifiable.

Any data to be submitted to a database for secondary purposes for use by anyone outside of the study research team must be on the condition that appropriate consent was given by participants to retain those data and the unspecified, future use of those data was included in the ethics approval.

Confidential Data

Personal Identifiable Information is the responsibility of all individual employees professionally, ethically and legally.

Confidential waste must not be used as scrap paper for messages, notes etc. Identifiable paperwork must be shredded as soon as the paperwork is no longer required or has been scanned for electronic records

Sensitive Personal Data is defined as information relating to race, racial or ethnic origin; political opinion; religious belief or other beliefs of a similar nature; physical or mental health or condition; trade union membership; sexuality or sexual life; and offences (including alleged offences) and any criminal history, which if released may or may not put the participant at risk of harm or distress.

Personal data is defined as any information relating to a living person and which can be identified as referring to him or her is included regardless of the format; electronic, paper, film, tape, text, still and moving image.

- Name
- Address
- Full Post code
- NHS number
- Email address
- Date of Birth (Not age of individual)
- Driving license number
- Telephone number(s)
- Local patient identifier (if NHS)
- National insurance number

It is important to consider what information, which may not be considered identifiable may be traceable to that individual e.g. a rare medical condition and locality in which they are reside.

When seeking expedited ethical review the applicant(s) must include details of the types of data anticipated to be retained and how they intend to manage handling of personal or sensitive personal data.

Annex B and C: Templates to use for gaining informed consent

Annex B: Template consent form

This is intended to be used to seek informed consent for data/information to be retained for secondary research purposes by the University of Sussex. ***Please insert and/or delete as appropriate for your database***

<INSERT DATABASE TITLE>

CONSENT FORM

I confirm that I have read and understood the information sheet entitled <INSERT DATABASE TITLE>. I understand that my <DATA/SCAN/OTHER> being retained for future unspecified research purposes is voluntary. I understand that joining this database is **not** a requirement to participate in the current research project I have been recruited to.

I understand that I am free to withdraw at <ANY TIME/AT ANY TIME BEFORE THIS CUT-OFF DATE>, without giving any reason and that the process to request withdrawal has been explained to me. I have been given the database manager contact details in order to request withdrawal and understand it is separate from the current research project I am participating in. I understand that if I withdraw from the database, my personally identifiable data will be removed and I will no longer be contacted for future participation in research by <INSERT DATABASE TITLE>.

I consent for my <INSERT AS APPROPRIATE <E.G. SCAN/DATA/INFORMATION> to be used for further research to be <INSERT EXAMPLES OF HOW RESEARCHERS ANTICIPATE USING THEIR DATA/SCAN/INFORMATION>. Y/N

Signed by participant……

Participant name……

Date……..dd/mm/yyyy

I understand that I will **not** be contacted in advance about the use of my <INSERT AS APPROPRIATE <SCAN/DATA/INFORMATION> for future projects and <OPTIONAL INSERT IF THEIR ANONYMOUS DEMOGRAPHIC INFORMATION OR DETAILS OF THEIR E.G. GENDER WILL BE MADE AVAILABLE TO THE RESEARCHERS ALONGSIDE THEIR DATA>. Y/N

I am willing to be contacted to take part in further research in which my existing <SCAN/DATA/INFORMATION> can be used again. Y/N

Signed by participant……

Participant name……

Date……..dd/mm/yyyy

If you have any questions, concerns or would like to withdraw your information from the database please contact <INSERT FULL CONTACT DETAILS OF DATABASE MANAGER>

Signed by researcher present…….

Researchers name……

Date……..dd/mm/yyyy

If you have any other questions or concerns please contact the University of Sussex Research Governance Officer:

Tel: 01273872748

E: rgoffice@sussex.ac.uk

Annex C: Template Information sheet

Please insert and/or delete information as appropriate for your database

<INSERT DATABASE TITLE>

<INSERT VERSION NUMBER>

<INSERT DATE>

<INSERT CONTACT DETAILS IN FULL>

<INSERT DATE OF EXPEDITED ETHICAL APPROVAL GIVEN>

Dear Participant,

As well as participating in the current research project, you are being invited to join a database for research.

Before you decide, it is important for you to understand what the database is and its function. Please take time to read the following information carefully. We would like to emphasise that joining the database is optional and is **not** a requirement to participate in the current research project you have been recruited to.

What is <INSERT DATABASE TITLE>?

<EXPLAIN IN LAY LANGUAGE WHAT YOUR DATABASE IS AND WHY AND HOW RESEARCHERS ARE ABLE TO USE THE DATA. WHAT ARE THE BENEFITS OF THIS FUTURE RESEARCH; WILL IT BENEFIT THE SCIENTIFIC COMMUNITY, HOW WILL IT IMPACT ON WIDER SOCIETY.>

<WHAT WILL HAPPEN TO MY DATA?>

<EXPLAIN IN LAY LANGUAGE THAT YOUR DATA/SCAN/INFORMATION WILL NOT BE USED FOR ANY OTHER PURPOSES UNLESS YOU EXPLICITLY AGREE TO THIS ON THE CONSENT FORM.> Agreement to allow other researchers to use your data for future research purposes is optional and does not affect your participation in the current study in any way.

<HOW AND HOW OFTEN WILL PARTICIPANTS BE CONTACTED (IF AT ALL)>. There is no obligation to participate in future studies if you are contacted, all studies have to go through the University's ethics system and be given ethics approval.

This database has ethical approval and is maintained and managed to University of Sussex standards.

<EXPLAIN IF THERE ARE ANY CIRCUMSTANCES IN WHICH THE DATA WOULD BE LINKED TO INDIVIDUAL CHARACTERISTICS HELD ON A SECURE DATABASE. EXPLAIN HOW A PARTICIPANT CAN REQUEST THAT THEIR DETAILS AND/OR DATA CAN BE REMOVED AT ANY POINT AND WITHOUT GIVING ANY REASON UNLESS THERE IS A CUT-OFF POINT.> You are not obliged to take part in any of the additional studies and you will be given separate information sheets and consent forms relating to these.

<WHAT IF I CHANGE MY MIND?>

If you change your mind and would like to withdraw from the <INSERT DATABASE TITLE>, please contact <INSERT THE DATABASE MANAGER AND THEIR CONTACT DETAILS>. All of your identifiable data and contact details will be withdrawn from the database and you will no longer be contacted with invitations for upcoming experiments or projects.

Thank you for taking the time to read this information sheet.

Please ask the researcher if you have any more questions.

<INSERT CURRENT RESEARCH PROJECT TITLE>

<INSERT VERSION NUMBER>

<INSERT DATE>

<INSERT CONTACT DETAILS IN FULL>

If you have any questions, concerns or would like to withdraw your information from the database please contact <INSERT FULL CONTACT DETAILS OF DATABASE MANAGER>

If you have any other questions these can be directed to the University of Sussex Research Governance Officer Tel: 01273872748 or E: rgoffice@sussex.ac.uk.