University of Hertfordshire

CONFIDENTIALITY AND DATA PROTECTION OF PERSONAL DATA

Clinical Trials Support Network (CTSN)

Standard Operating Procedure for Confidentiality and Data Protection at the University of Hertfordshire

SOP Number: gSOP-026-01	**Effective Date:** 28th July 2022
Version Number: 1	**Review Date:** 2-3 years (or as required)

1.0 BACKGROUND

The Data Protection Act (2018) (DPA) and the UK General Data Protection Regulation (UK GDPR) sets the legal framework within which personal information can be processed. It applies to information that might identify any living person. The common law duty of confidentiality governs information given in confidence to a health professional (about a person alive or deceased) with the expectation it will be kept confidential.

The DPA defines six Data Protection Principles which all processors of personal information must abide by. The 6 principles are:

1. Processing shall be lawful, fair and transparent.
2. The purpose of processing shall be specified, explicit and legitimate.
3. Personal data processed shall be adequate, relevant and not excessive.
4. Personal data shall be accurate and kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary.
6. Personal data shall be processed in a secure manner.

The Research Governance Framework incorporates the stipulations of the DPA and stipulates the appropriate use and protection of participants' data in research settings by establishing secure systems to ensure the confidentiality of personal information.

2.0 PURPOSE

To outline the procedures to be followed and security measures to be taken when managing personal data collected for research purposes. Compliance with this SOP will ensure that all information collected during the research process is recorded, handled and stored in a way that maintains appropriate confidentiality but allows access and use as applicable, whilst satisfying the requirements of the DPA.

3.0 APPLICABLE TO

This applies to all staff involved in clinical research sponsored/co-sponsored by UH and/or adopted by the CTSN, including but not limited to: Chief Investigators (CI), Principal Investigators (PI), Research Fellows, Consultants, Statisticians, Clinical Trial Pharmacists, Research Managers, Research Nurses, Clinical Trial Practitioners, Allied Health Professionals, Trial Co-ordinators/Managers, Clinical Studies Officers, Data Managers, Research Assistants and Students who deal with personal identifiable data of any kind, at any time during the process of collection, handling, storing and analysis of research data.

4.0 RESPONSIBILITIES

The protection of research participants' data is the responsibility of the Sponsor, CI, PI and all members of the research team.

The CI is responsible for providing details of the collection, processing and storage of personal information and ensuring that they comply with the DPA.

The Data Protection Officer (DPO) is responsible for providing advice in relation to compliance with the data protection legislative framework and accountability requirements.

Specific data protection responsibilities may be delegated to the research team.

All UH staff must complete the mandatory UH GDPR training course and:

- must be aware of their legal and ethical duties in protecting personal data, and ensuring its confidentiality,
- are responsible for working within the DPA and relevant codes of practice,
- are responsible for ensuring that they are appropriately trained,
- are responsible for notifying their line manager of any changes to the way personal research data are processed or stored.

5.0 PROCEDURES

The UH UPR IM08 Data protection and privacy statement outlines the data protection principles that all UH staff are to comply with when processing personal data.

5.1. Data Controller and Data Processors

The DPA and the GDPR sets out the legal requirements and duties placed on data controllers (i.e., the University), and data processors (anyone the University uses to process data on our behalf).

Any processing of personal data must have a defined "Data controller"; the legal person, public authority, agency or other body which alone or jointly with others, determines the purposes and means of the processing of personal data. The roles of data controller and data processor should be clearly documented via agreements set up at the start of the project.

The University is required to register annually with the Information Commissioner as a Data Controller. The University's registration number is Z5759523.

5.2. Lawful basis for processing

The legal basis for processing personal data for research is determined by the type of organisation involved in that research. Where research is undertaken by the University (or an NHS organisation or Research Council) the legal basis for the processing of personal data is that processing is necessary for the performance of a public function and carried out in the public interest [Article 6(1)(f) GDPR].

Sensitive personal data is a specific set of "special categories" that must be treated with extra security. This includes information pertaining to:

- Racial or ethnic origin,
- Political opinions,
- Religious or philosophical beliefs,
- Trade union membership,
- Genetic data, and
- Biometric data (where processed to uniquely identify someone),
- Data concerning health,
- Data concerning a person's sex life,
- Data concerning a person's sexual orientation.

It is best practice that sensitive personal data should be held separately from other personal data, although this may not always be possible.

To process sensitive data a lawful basis must be identified. In addition, one of the special conditions in Article 9 of the UK GDPR must be met. The condition for processing the special category data must be documented.

Where any research is carried out using special category or sensitive personal information, the University will ensure the processing is necessary for: archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, on the basis of EU or Member State law, and appropriate safeguards for the rights of data subjects will be established. [Article 9(2)(j)]. Other lawful basis may also be applicable.

5.3. Data Protection Risks and Safeguards

A Data Protection Impact Assessment (DPIA) is a process designed to help the University identify and minimise the data protection risks of a project.

The UK GDPR requires that the University must perform a DPIA for any project involving the processing of personal data that is likely to result in a high risk to individuals. It is good practice to carry out a DPIA for any project which requires the processing of personal and / or special category data.

A DPIA should always be undertaken in conjunction with the DPO who will advise whether one is necessary, and on the correct procedure for completing the DPIA.

'Safeguards' are measures to protect the rights and freedoms of individuals whose personal data you are processing. Under the GDPR there is a strong emphasis on implementing safeguards for research. In practical terms, this means giving careful consideration to:

- Only collecting personal data where it is necessary for the research purpose (known as 'data minimisation').
- Ensuring that data are pseudonymised or anonymised wherever possible and as early as possible.
- Ensuring appropriate arrangements are in place for security and storage of data, proportionate to the risks inherent in the nature of the data e.g., portable devices must be encrypted.

5.4. Access to personal data

Personal data will only be processed by CTSN staff when:

- a justified, lawful purpose for doing so is identified and clearly documented; or
- informed consent has been obtained from each data subject; and
- protective measures have been taken to allow access to personal data only to authorised individuals.

5.4.1 Non-NHS staff

Where research involves NHS patients, data or facilities, members of the study team may need to be covered by an appropriate Human Resource agreement with the NHS organisation hosting their research. The NHS Research Passport System provides guidance on whether researchers will require an honorary NHS contract or Letter of Access depending on the level of patient contact they are likely to have during the trial. This is in addition to any other Data Protection requirements (e.g., Caldicott Guardian approval). Staff working on NHS premises must be familiar with the local NHS Trust data protection policies and attend information governance training where it is available.

5.5. Study protocol

When planning the study the CI and research team must check that data protection issues are clearly described in the study protocol, and include:

- the data to be collected;
- how the data are to be collected;
- who will have access to the data;
- how and where the data are to be stored and for how long;
- how the data are to be transferred (if applicable);
- how the data are to be analysed.

5.6. Participant Information Sheet and Informed Consent Form

In addition to the above, and in order to comply with the UK GDPR and DPA, the Participant Information Sheet (PIS) and Informed Consent Form (ICF) should contain the following information:

- How the data will be used (research data collected will not be used for anything additional to what is specified at the time of consent).
- Details of the organisation(s) which will collect store and process data.
- Details of the type and form of any data transfer, and whether participants could be identified.
- Intended duration of record retention and that this would be confidential.

If data collected for research purposes are not anonymised, explicit consent from the data subject is required.

5.6.1 Informing the General Practitioner

When a participant's GP is informed that their patient has been recruited into a study the participant must be told that the GP will be informed and give their explicit consent. This information must therefore be included on the PIS and ICF.

5.6.2 Identification of potential participants from health records

If potential participants are to be identified through some form of health record this must be explicit in the protocol and PIS.

5.6.3. Transfer outside the European Economic Area (EEA)

There are certain limited circumstances in which we may share personal data with third parties outside the EEA. Written consent to transfer data outside of the EEA should be sought during the informed consent process.

Any transfer of personal data outside the EEA will be subject to appropriate safeguards, such as contractual arrangements which comply with UK GDPR provisions regarding such transfers.

5.7. Security Measures

5.7.1. Anonymised and pseudonymised data

Anonymising data is a process that balances producing safe data with reduced utility of the data, recognising that whether data are anonymised or not, is a function of both the data and the data environment. Fully anonymising the data so that the risk of disclosing information referring to individuals is negligible is required in order for the data to be exempt from the DPA.

Pseudonymisation is a form of de-identification, in which information remains personal data. The legal distinction between anonymized and pseudonymised data is its categorisation as personal data. Pseudonymous data still allows for some form of re-identification (even indirect and remote), while anonymous data cannot be reidentified. Therefore, pseudonymised data cannot be considered to be outside the DPA, however, such data may still be shared subject to appropriate safeguards as laid out in this policy.

Anonymised individual patient data can be shared without specific consent, as the DPA does not cover anonymised data. However, participants should be told if researchers intend to keep the data participants provide for use beyond a specific research study and if data may be shared anonymously with others in the future. It is recommended that the following statement is included in the consent form and the patient information leaflet for research studies, if appropriate.

“I understand that the information collected about me will be used to support other research in the future and may be shared anonymously with other researchers.”

In most research studies it is not always possible to completely anonymise data as source data verification is required, and data must be ‘pseudonymised’. When data are pseudonymised, one master list with the identifier/ codes and the participants’ details is kept separately in order to link the patients to their data (and should be kept in a locked cabinet/office/password protected file); no copies of this list should be made. The study monitor will usually access the master list at site, or there may be a master list in the CTSN for trial specific purposes, or blinding codes may be kept for access etc.

For studies in which source data verification is not required, it will be possible to keep completely anonymised data (e.g., epidemiological research). In these cases, the DPA does not apply.

5.7.2. Paper based data

All data not received in an anonymised form must be collected with the permission of study participants, stored securely (e.g., password protected, in a locked cabinet etc.), and retained only for as long as is necessary. It should be clear in the protocol, PIS and ICF that personal data with the potential to identify research participants will be kept separate from the study data and CRFs, with the exception of essential study documents required to be kept as part of the Trial Master File and Study Site

File e.g., signed ICFs. Access to this data will be restricted to members of the research team, unless authorised by the Investigator, a member of the research team or the Caldicott Guardian.

5.7.3. Electronic data

Files containing electronic data must be password protected and stored on a secure University network (not a hard or 'C' drive) and security of the data protected. Workstations should be locked if the user is leaving the computer unattended.

Where electronic files containing personal data are saved in folders on a shared network, access should be restricted to authorised individuals who have been allocated a password to allow access to the data. Logins and passwords should never be shared, even with team members or line managers, as this is a breach of the Computer Misuse Act (1990)[16].

If handling electronic files with direct identifiers, such as names and addresses, the following should be observed:

a) Files containing direct identifiers should be separated from other trial data and saved in a folder with access only to individuals who strictly need to see it for the purposes of managing the trial.
b) Files containing direct identifiers should remain in only one location in a secure area of the server and not be copied and saved elsewhere.
c) Files containing direct identifiers should not be transferred via e-mail or by other means, except with the explicit consent of the participants.

Personal identifiable data must not be stored on home computers, personal laptops, memory sticks, CDs, handheld devices, digital cameras or other imaging equipment, even if they are password protected.
All personal data (whether pseudonymised or anonymised) should be centrally backed up on a secure server.

5.7.4. Transfer of data

All data sharing requests and data transfers should be approved by the Trial Management Group. They must be logged and accompanied by a Data Sharing Agreement which has been signed by the member of the CTSN transferring the data, and then returned to the CTSN and countersigned by the recipient.

Identifiable data must not be transferred by unencrypted e-mail, CD or USB. University e-mail is not encrypted by default. All personal information should be transferred by use of the University's secure file transfer system, Exchange File.

It is, however, possible to send queries/information to sites provided that no identifiable data is included, and patients can only be identified by a unique study number.

5.8. Re-using personal data for a different purpose & sharing with third parties

If a researcher wishes to re-use personal data that were collected for a particular purpose (e.g., a specific research project) for a new purpose (e.g., a new research project), and the data subject was not informed of this as part of the original informed consent procedures, then the researcher would be required to contact the data subject to inform them of this BEFORE the new processing commenced. If the data from the original project had already been fully anonymised before use in the second project, it would no longer constitute personal data and would therefore no longer be subject to data protection legislation and the data subject would not need to be contacted about the re-use of their data.

Where personal data is to be used by a researcher, but they have NOT obtained the data directly from the data subject, the original data controller supplying the data must have informed the data subject of relevant information relating to this new processing.

In some circumstances, where personal data has NOT been obtained directly from the data subject, then the requirement to provide information to the data subject does not apply. This is where:

- Data has been pseudonymised and the new research activity is conducted without using identifiable data; AND
- The provision of information would be impossible or involve a disproportionate effort (taking into consideration the number of participants, the age of the data, etc.); OR
- The provision of information would render impossible or seriously impair the objectives of the research.

Such a decision should be documented as part of the ethics review procedure, and appropriate safeguards should be in put place.

5.9. Processes for dealing with data breaches

5.9.1. Defining and identifying a data breach

The GDPR defines a breach as “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed” by the University or one of its subsidiary companies.

Some examples of data breaches are; personal information of data subject(s) sent to the wrong person, loss of portable device containing personal information such as laptop, USB memory stick (regardless of whether encrypted or password protected).

All breaches or suspected breaches, regardless of severity, must be reported immediately to the Data Protection Officer (“DPO”) once the staff member becomes

aware of it using the procedure detailed in UH UPR IM008 Appendix V Data Breach Procedure.

5.9.2. Reporting procedure:

Staff should contact the DPO by email at dataprotection@herts.ac.uk, marked as urgent, with the subject line “DATA PROTECTION BREACH”.

When reporting the breach, the member of staff should, where possible, provide the DPO with the following information:

- Data Subjects affected (categories and number of individuals affected).
- Information categories concerned e.g., names, email address, bank details etc.
- How the breach occurred.
- When the breach occurred.
- When staff member became aware of the breach.

The DPO will decide in consultation with senior management if the breach is severe enough to require reporting to the ICO and, if applicable the data subjects affected.

5.10. Archiving

Source documents, and trial-related electronic and other data must be stored safely and in accordance with the requirements of the DPA, for a minimum of five years or as stipulated by the Sponsor’s requirements, and the applicable regulations. (gSOP-17 Archiving Essential Documents).

6.0 RELATED DOCUMENTS

- UH UPR IM08 Data protection and privacy statement
- Data Protection Impact Assessment (DPIA)
- UH UPR IM08 Appendix 5 – Data Breach Procedure
- gSOP-04 Informed Consent
- Data Sharing Agreement
- gSOP-17 Archiving Essential Documents

7.0 APPENDICES

8.0 VERSION HISTORY/REVISIONS

Version Number	Effective Date	Reason for Change

9. AUTHORSHIP & APPROVAL

Author

Signature  **Date 16 June 2022**

Pro-Vice Chancellor (Research and Enterprise) Approval

Signature  **Date 16 June 2022**
Professor J M Senior

10. AGREEMENT (MOVE ON TO A SPERATE SHEET BEFORE PRINTING)

Please detach and retain within <u>your training files</u>

I have read and understood the contents and requirements of this SOP (ref gSOP-026-01) and accept to follow University of Hertfordshire policies implementing it.

Recipient

Signature: ……Date: ……..

Name & Position: ……