DIVISION OF RESEARCH AND INNOVATION

Joint Research and Development Office

Document Number: GOSH/ICH/SOP/R&D/024	Version Number: 7
Title: **DATA PROTECTION**	
Effective Date:	*Same as implement by Date*

	Name	Position
Authored by:	Dr Thomas Lewis	Research Governance Manager
Approved by:	Dr Vanshree Patel	Head of Governance, Clinical Trials and Contracts

1. Scope

This SOP is applicable to all the research studies sponsored by Great Ormond Street Hospital/Institute of Child Health, and other external sponsors. If a research study involves the use of 'personal data' then it falls under the scope of the General Data Protection Regulation 2016(GDPR). It is the responsibility of the Principal Investigator (PI) to ensure that all data is collected, stored and analysed in accordance with the GDPR.

The legal basis for this operating procedure is the UK policy framework for health and social care research V3.3 07/11/17, the GDPR, the Data Protection Act 2018 and The Health Records Act 1990.

2. Purpose

This document is for use by the Joint R&D Office for GOSH/ICH and details the method used by the Joint R&D Office to ensure that researchers are aware of, and comply with, the GDPR. This SOP also covers the handling of different types of data within GOSH/ICH.

3. Definitions/Abbreviations

The GDPR lays down principles of good information handling which is designed to ensure that personal data is used in a way that is fair and transparent to individuals and protects their rights. The GDPR applies to personal data, which is defined as:

Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The GDPR does not apply to information about deceased individuals, but you may still owe a duty of confidentiality after death.

It is expected that all staff comply with the legal requirements of the Trust and University policies, procedures and guidelines, as outlined in section 5.7. All researchers must ensure that processing of personal or sensitive data takes place only when there is a clear purpose for doing so. Individuals must be informed, and agree to, of the uses to which their data will be put (i.e. the collection, use and distribution of their personal data). Confidentiality must be maintained in the use of personal data and the identity of individuals must be protected. It must be remembered that individuals have the right to prevent the use of their data. All data must be stored both properly and securely.

For GOSH/ICH the health and care research should serve the public interest as the lawful basis for processing personal data, therefore GOSH/ICH needs to demonstrate that the research performed/led by the organisation serves the interests of society as a while. This can be done by following the UK policy framework for health and social care research V3.3 07/11/17.

The Health Research Authority (HRA) NHS approval for research includes a review of data protection in compliance with the GDPR. For research that does not require HRA approval but requires NHS Research Ethical review the Trust, under its research governance review, should be assured that necessary data protection steps have been taken and appropriately

assessed in line with the associated Trust Information Governance policies (available via GOSHWeb Intranet services and in section 7). The UCL Information Governance policies should also be referred to as appropriate (available in section 7).

4. Responsibilities

The Deputy Director of Research & Innovation is responsible for ensuring that researchers comply with the GDPR. This responsibility has been delegated to the Head of Governance, Clinical Trials and Contracts.

It is expected that all research and researchers will comply with all the legal requirements and University and Trust policies, procedures and guidelines.

5. Procedure

5.1 Health Research Authority (HRA) approval projects

Those projects approved through the HRA approval process (and subsequent GOSH confirmation of participation in the research) have their own IG research governance arrangements and therefore will not fall under the scope of this SOP. It is recommended however that for those studies undergoing a GOSH/ICH sponsorship review for HRA approval, the Caldicott Guardian or the Trust's Information Governance Manager (in the Caldicott Guardian's absence) should be contacted for any data protection assessment if necessary. For new clinical studies participant information sheets relevant transparency information is required to be added as per the HRA guidance and assistance will be provided for researchers though the governance sponsorship review process.

Health research already takes place within a context of established arrangements for sponsor oversight and for use of personal data, which should include documented risk assessments through the IRAS application. As part of the sponsor oversight, consideration should be given to the above risks. This means that it is not necessary for the sponsor to undertake a separate privacy impact assessment process for every research project. Furthermore, due to the arrangements for study-wide review across the NHS (through HRA

Approval and equivalent coordinated approaches), NHS sites should not undertake separate privacy impact assessments for each project. The study-wide review will highlight any considerations to be included in the local decisions about capacity and capability.

It should be noted that those projects with HRA approval that also involve storage of identifiable or pseudo-anonymised data at ICH may require UCL data protection registration as per section 5.2.

5.2. Procedure

1. All relevant projects undergoing research governance review (outside the HRA approval process and subsequent GOSH confirmation of participation) within the Joint R&D Office will be passed to the Research Management and Governance Officer (RM&G Officer), Research Governance Manager (RG Manager) or the Head of Governance, Clinical Trials and Contracts. The R&MG Officer, RG Manager or Head of Governance, Clinical Trials and Contracts will check the IRAS Application Form (if applicable), UCL REC application form (if applicable) or any other relevant documentation to ascertain whether the project involves the use of personal data and whether it is pseudo-anonymised or anonymised.

2. If the project solely uses data which is fully anonymised then this does not fall under the GDPR and there is no need for data protection registration. Anonymised means that the recipient of the data cannot trace the data to an individual. Pseudo-anonymised refers to data that has been given a unique identifier code in order to break any link to the data subject. Such data should be stored separately from the identifiable information. These types of studies are normally classed as using personal data under the GDPR and therefore would need to be registered for data protection purposes.

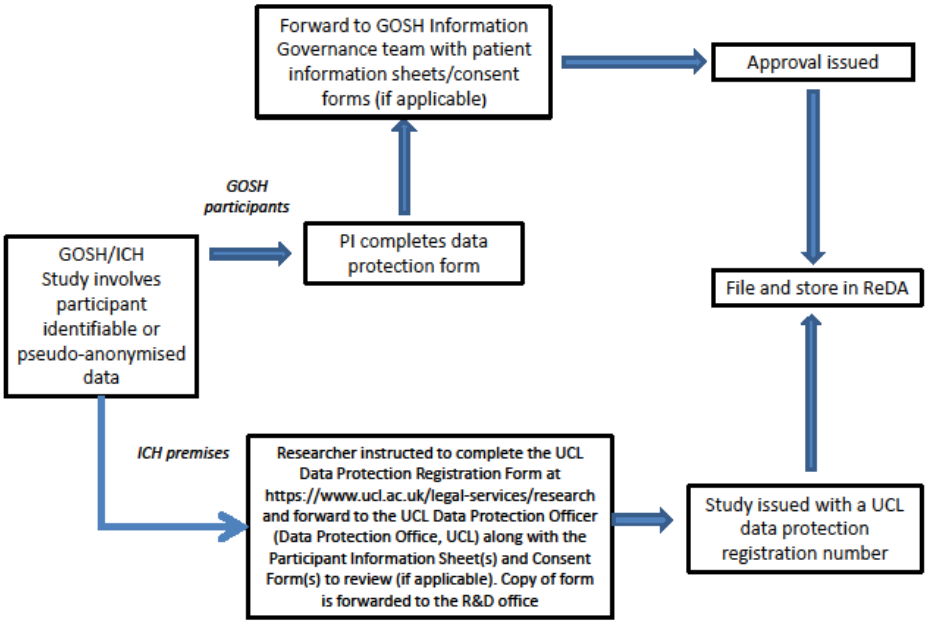
3. If the project uses identifiable or pseudo-anonymised data at GOSH then the PI will be requested to complete a R&D 'Data Protection Registration Form' and return it to the R&MG Officer, RG Manager or Head of Governance, Clinical Trials and Contracts. This form asks questions about what identifiable data will be collected, how it will be stored, how long it will be kept for, and whether any data will be transferred overseas. Examples of uses of data are given in section 5.7. Returned forms will be reviewed by the R&MG Officer, RG Manager or Head of Governance, Clinical Trials and Contracts to identify whether identifiable or pseudo-anonymised data is being stored in GOSH, or another organisation. The forms are stored in Section 5 (Local Study Documents) on ReDA.

4. If the study involves identifiable or pseudo-anonymised GOSH participant data then approval is required from the GOSH Information Governance team. The R&MG Officer, RG Manager or Head of Governance, Clinical Trials and Contracts will forward the completed R&D 'Data Protection Registration Form' along with the Participant Information Sheet(s) and Consent Form(s) for review (if applicable) to the GOSH Caldicott Guardian or the GOSH Information Governance Officer (in the Caldicott Guardian's absence). In addition any other relevant information should be forwarded to the GOSH Information Governance team. Initial contact to the GOSH Information Governance team should come from the R&MG Officer, RG Manager or Head of Governance, Clinical Trials and Contracts. On occasion it may be necessary for the Principle Investigator or research team to clarify these queries with the GOSH Information Governance team.

5. If it is identified that identifiable or pseudo-anonymised data will be stored on ICH (UCL) computers then the R&MG Officer, RG Manager or Head of Governance, Clinical Trials and Contracts will instruct the researcher to complete the UCL Data Protection Registration Form at https://www.ucl.ac.uk/legal-services/research and forward to the UCL Data Protection Officer (Data Protection Office, UCL) along with the Participant Information Sheet(s) and Consent Form(s) to review (if applicable). The researcher will also be instructed to forward the completed UCL Data Protection

Registration Form to the R&D office for their records. Once reviewed by UCL a Data Protection Registration Number will be issued to the PI, In which this will be entered by the R&MG Officer, RG Manager or Head of Governance, Clinical Trials and Contracts into ReDA under the management tab in the 'data protection registration number' box. The Data Protection Form and confirmation of the Data Protection Registration Number should be stored in the relevant folder on ReDA.

6. Some PIs contact the Joint R&D Office about Data Protection issues before they have submitted their R&D Registration Form. In these cases the R&MG Officer, RG Manager or Head of Governance, Clinical Trials and Contracts will discuss with them about how to treat their data in accordance with the GDPR liaising with the relevant IG teams if necessary.



5.3. Processes for ensuring data protection compliance

The GDPR imposes stringent security obligations on data controllers. Personal data must be kept secure, in proportion to their sensitivity. UCL/GOSH is obliged to take appropriate measures to safeguard against the unauthorised or unlawful processing of personal data and against accidental loss, destruction of, or damage to, personal data. It must also ensure the reliability of staff who, have access to personal data and ensure that they are made aware of the requirements of the GDPR.

To ensure that arrangements are in accordance with GDPR, Caldicott Principles and NHS Organisation confidentiality policies the protocol and IRAS form (Questions A36-45 and A52), and other relevant study documentation such as the patient information sheet (PIS) and consent forms should be reviewed. The Head of Governance, Clinical Trials and Contracts and Research Management & Governance team will assess that the process of utilising data and personal information is consistent in all information provided for the R&D submission e.g. if data is to be transferred outside the UK or European Economic Area (EEA) then this should be stated in the Patient Information Sheet and the consent forms. All researchers must be careful when contemplating the transfer of research data overseas. In most cases, the safe option will be to ensure that data subjects give explicit consent for overseas transfer during data collection.

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR. Transfers may be made where the Commission has decided that a third country, a territory or one or more specific sectors in the third country, or an international organisation ensures an adequate level of protection.

In some situations a data sharing agreement may be required between sponsor and site. In this case the relevant organisational Information Governance/contract teams should be contacted to confirm this.

Will personal information only be accessed by those with a right to access?

The clinical care team should be the only ones to have access to patient data if consent has not been obtained. If it is unclear whether a relevant person is a member of the clinical care team the R&MG Officer or Head of Governance, Clinical Trials and Contracts should gain confirmation of this from the clinical or speciality lead. If consent has been obtained data should be shared in accordance with the protocol, HRA approval (and Research Ethics Committee (REC) approval if applicable) and Participant Information Sheet and Participant Consent Form.

Are the local data security, arrangements for the anonymisation or pseudo-anonymisation of local records, access to data and storage of data during and at the end of the study robust?

Data stored and transferred should be encrypted with identifiers/keys kept in a separate secure location. The use of shared drives should be encouraged to ensure data is backed up, however, it is important to ensure access to these drives is controlled and monitored. It is rarely necessary to store electronic personal data on portable devices such as laptops, USB flash drives, portable hard drives, CDs, DVDs, or any computer not owned by UCL/GOSH. Similarly, manual personal data should not be regularly removed from UCL/GOSH premises. In the case of electronic data, to minimise the risk of loss or disclosure, a secure remote connection to UCL/GOSH should be used wherever possible.

Manual personal data and portable electronic devices should be stored in locked units, and they should not be left on desks overnight or in view of third parties. All portable electronic devices should be encrypted.

Sections A36-45 of the IRAS form and the Data Protection Registration form address how confidentiality is maintained throughout the study. The UCL REC application form (if applicable) or any other relevant documentation may also be reviewed. These questions and answers should be assessed to see whether they meet the requirements for R&D approval.

Where a project warrants the use of patient identifiable information without consent under Section 251 of the NHS Act 2006 (Formally Section 60, Health and Social Care Act 2001) researchers must provide evidence of exemption from the Confidentiality Advisory Group (CAG).

For GOSH and ICH researchers it should be encouraged to use the GOSH Digital Research Environment (DRE) for data analysis and/or utilising anonymised clinical data from EPIC for research. The use of the DRE should be included in the IRAS form, protocol and participant documentation. Researchers should be directed to DREProjects@gosh.nhs.uk for further information.

Those researchers using identifiable data at ICH should be directed towards the use of the Data Safe Haven (DSH), which provides a technical service for storing, handling and analysing identifiable data. The use of the DSH should be included in the IRAS form, protocol and participant documentation. Researchers can be directed to the relevant DSH webpage on the UCL website for further information.

All studies audited by the Joint Research and Development Office (as per SOP GOSH/ICH/13/RG30) require a data protection element (including determining how and where data is stored) which will be recorded in the final audit report. This is to ensure this data is captured and to understand how much data is being stored on GOSH and ICH devices. Any concerns should be reported to the Head of Governance, Clinical Trials and Contracts and the relevant GOSH/ICH IG team.

5.4. Breaches and Misconduct

All data holding organisations are registered with the Information Commissions Office under the GDPR, and neglectful or intentional abuse of personal information may result in the organisation, and the individual concerned, being prosecuted.

Any identified breaches of data protection or misconduct in the use of the agreed data should be reported to the Information Governance Manager for the Trust (if concerning Trust patients, staff or information), and/or the Data Protection Officer for UCL (if concerning ICH related activity). Details of which can be found on respective organisation websites and the R&D office.

If the incident is defined as any event or circumstance that could have or did lead to unintended or unexpected harm, loss or damage to GOSH then this needs to be reported on the Trust Datix system within 24 hours of the incident.

5.5. Records

Completed Data Protection Forms are filed electronically on ReDA in the Joint R&D Office, and are kept indefinitely.

The long term storage of study related documents which may include identifiable information should be done in accordance with the agreed arrangements with the study sponsor and complies with the relevant Trust and UCL policies.

For UCL, when all essential documents are ready to archive, the UCL Records Office can be contacted by email records.office@ucl.ac.uk to arrange on-going secure storage of the research records unless specific alternative arrangements have been made with the department, funder, or R&D office.

5.6. Data protection holdings survey

UCL carries out an annual Data Protection Holdings Survey.
The purpose of this survey is to determine whether or not the Institute has the appropriate procedures in place in regard to data protection and whether it has changed the way it collects, uses and stores personal and sensitive personal data. UCL will contact the Institute

Manager in writing who will request the Data and Information Administrator to collect the information from each Unit.

The data protection public register can be searched for UCL's entry registration number: **Z6364106** on line at **https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/**

5.7. Guidance on general handling of personal data

Examples of uses of data:

- Access to medical records by those outside the direct healthcare team
- Electronic transfer by magnetic or optical media, email or computer networks
- Sharing of personal data with other organisations
- Export of personal data outside the EEA
- Use of personal addresses, postcodes, faxes, emails or telephone numbers
- Publication of direct quotations from respondents
- Publication of data that might allow identification of individuals
- Use of audio/visual recording devices
- Retention of data
- Storage of personal data on any of the following:

1. Manual files including X rays
2. NHS computers
3. Home or other personal computers
4. University computers

5. Private company computers
6. Laptop computers

Activity	*Guidance*
Access to medical records by those outside the direct healthcare team	This should only be undertaken with consent or Section 251 support.
Electronic transfer of data by magnetic or optical media, email or computer networks	Where personal data is transferred electronically, data must be encrypted during transfer.
Sharing of data with other organisations	Except where such disclosure has consent or approval under Section 251, only anonymised data should be shared. Where data has been effectively pseudonymised it should only be shared on the basis that the recipient cannot disclose pseudonymised data to third parties and is not permitted to link the data with other data which might render the information more identifiable.
Export of data outside the EEA	In general, patient level data should not be transferred outside of the European Economic Area (EEA). This is because other countries do not have the same legal framework or protections for patient data. Even where this is the case, it is difficult to manage and monitor the use of data to ensure it is safeguarded appropriately and is not misused.
Use of personal addresses, postcodes, faxes, emails or telephone numbers	It should be remembered that such personal contact details can be sensitive information, either because individuals are concerned about identity theft or because of domestic violence etc.

Publication of direct quotations from respondents	Should be anonymised
Publication of data that might allow identification of individuals	In general, publication of case histories should be effectively anonymised. Where identification is possible it is essential that this is only undertaken with consent.
Storage of personal data on manual files (including X-rays)	Paper and other manual files should be appropriately filed and stored securely.
Storage on NHS computers	Appropriate access controls need to be in place to ensure that access to confidential research information is restricted to those who need access.
Storage on home or other personal computers	Under no circumstances should patients" or research participants" personal data be stored on a home or other personal computer.
Storage on university computers	Appropriate access controls need to be in place to ensure that access to confidential research information is restricted to those who need access. Any personal information stored on UCL computers should be stored on the UCL Data Safe Haven (details in section 7).
Storage on private company computers	Appropriate access controls need to be in place to ensure that access to confidential research information is restricted to those who need access.
Storage on laptop computers	Use of laptops and other portable devices is to be avoided. Where it is necessary for them to be used, data must be encrypted and the data uploaded onto a secure server or desktop as soon as possible and the data removed from the portable device as soon as possible and using appropriate data destruction software.

Retention of data	Data should only be kept for the length of time specified by the research retention guidelines. Data should not be kept indefinitely. Data must be deleted securely.

6. Related Documents

GOSH confidentiality policy

GOSH information security policy

GOSH encryption policy

GOSH e-mail use policy

GOSH internet policy

GOSH Use of camera and photographic equipment policy

GOSH records retention policy. Refer to pages 42-4

UCL data protection policy

UCL data retention schedule

UCL guidance for storage of sensitive data

UCL ADS general encryption guidance

MRC good research practice

MRC personal information in medical research

7. References

1) UK Policy Framework for Health and Social Care Research V3.3 07/11/2017

https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/uk-policy-framework-health-social-care-research/

2) Health Research Authority guidance on the GDPR

https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/

3) Health Research Authority (HRA) approval for research

https://www.hra.nhs.uk/approvals-amendments/what-approvals-do-i-need/hra-approval/

4) Confidentiality NHS Code of Practice 2003
https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice

5) Sending personal Data outside the EEA

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/

6) University College London GDPR guidance

https://www.ucl.ac.uk/legal-services/ucl-general-data-protection-regulation-gdpr

7) University College London data protection guidance/policies

https://www.ucl.ac.uk/legal-services/policies

8) UCL Data Safe Haven

https://www.ucl.ac.uk/isd/services/file-storage-sharing/data-safe-haven-dsh

9) HRA Data Privacy Impact Assessments guidance

https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/what-law-says/data-privacy-impact-assessments/

8. Appendices (If applicable)

*all these documents are available electronically