Health Research SOP R02

STANDARD OPERATING PROCEDURE FOR DATA PROTECTION AND CONFIDENTIALITY IN RESEARCH

Author & Title	[redacted] Deputy Research and Development Manager BCUHB SOP Writing Group				
Responsible Dept / director:	[redacted] Associate Director, Research and Development Department				
Approved by:	BCUHB R&D Senior Managers – 07.02.2022 Information Governance – 29.12.2022 Clinical Effectiveness Group (CEG) – 18.01.2023				
Date approved:	18.01.2023				
Date activated (live):	06.03.2023				
Documents to be read alongside this document:	BCUHB Research Governance Framework Policy R&D01				
Date of next review:	18.01.2025				
Date EqIA completed:	18.08.2021				
First operational:	31.10.2013				
Previously reviewed:	13.10.14	13.12.16	18.05.20		
Changes made yes/no:	YES	YES	YES		

Disclaimer: Printed SOPs are considered uncontrolled. To ensure you are working with the current version always refer to the pdf version on the Betsi Research website.

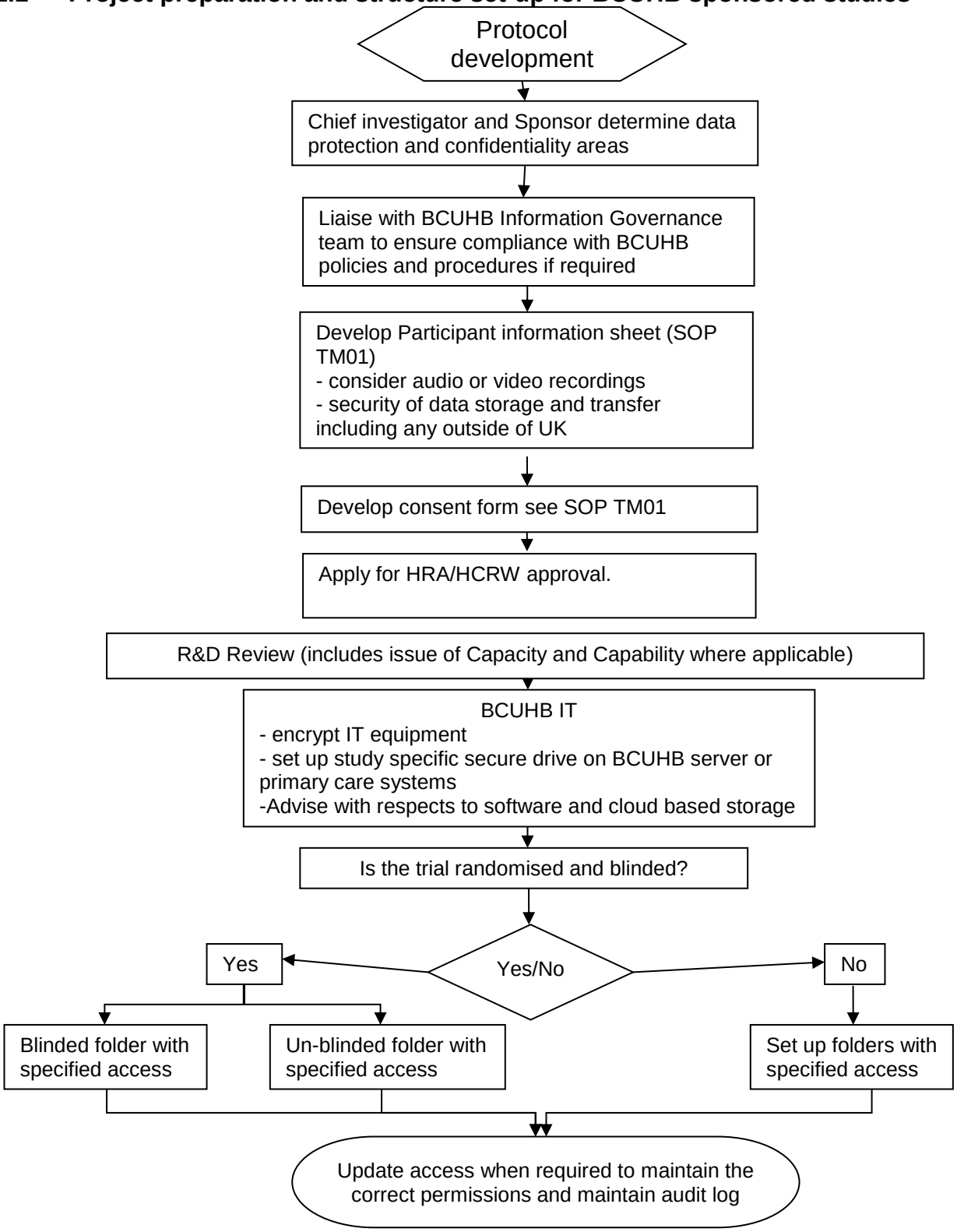
Document History

Version number	Effective date	Reason for change
1	31.10.13	Review - Minor change, format standardised
2	13.10.14	Name change Director BCUHB R & D, Reference to TM01 in flowchart included. Changed references from NISCHR to HCRW.
3	13.12.16	
4	18.05.20	Associate Director details added and all reference to Bangor University (BU) removed and links and references updated. Process charts reformatted.
5	01.03.23	Updated front sheet in line with BCUHB policies. Updated Flowchart 1 to remove references to University procedures and clarified processes. Added new appendix for FAQ about research and data protection, simplified appendix 2 with regards the seven DP principles.

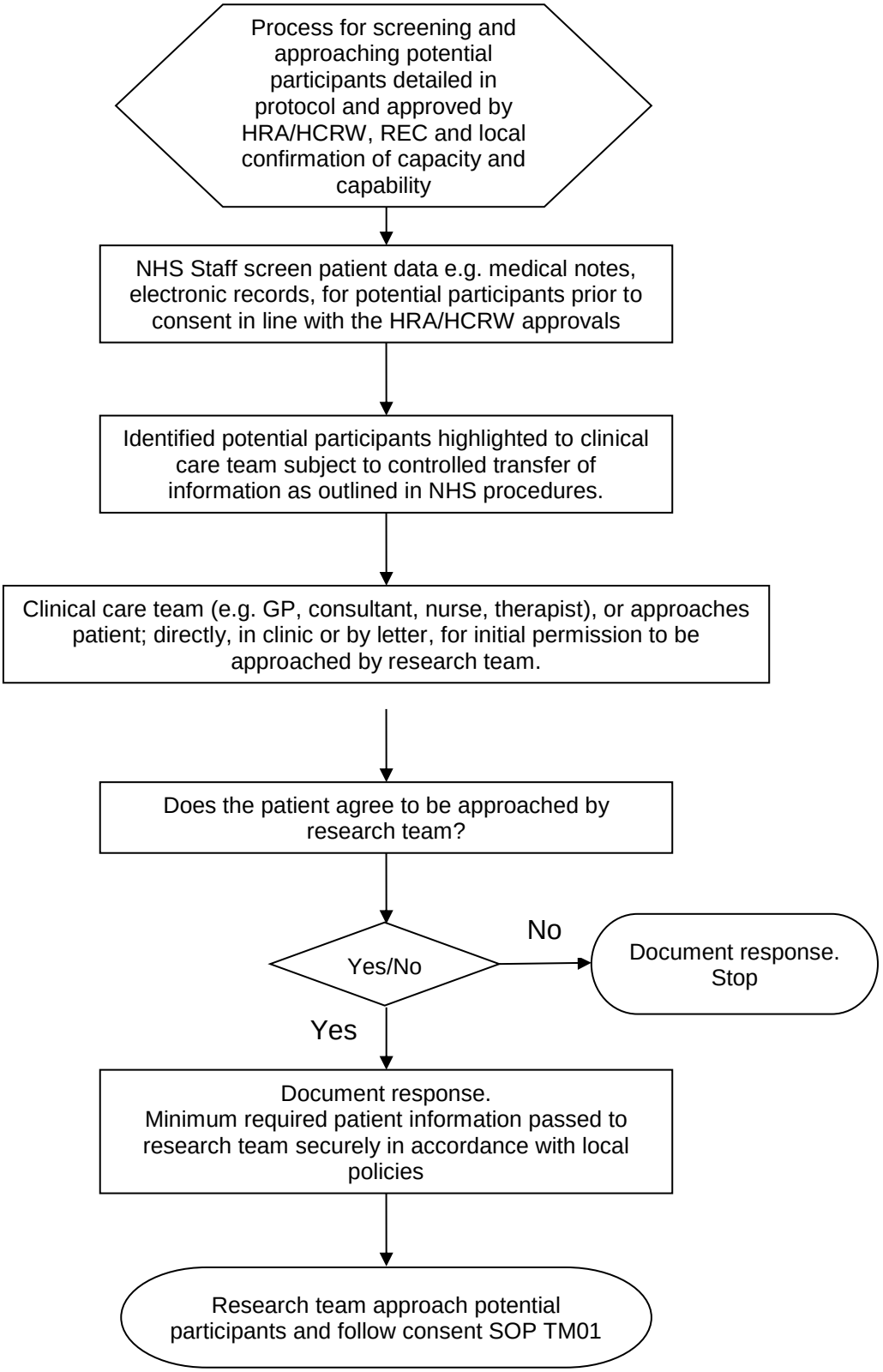
Table of contents

1. Flow Chart of Procedures

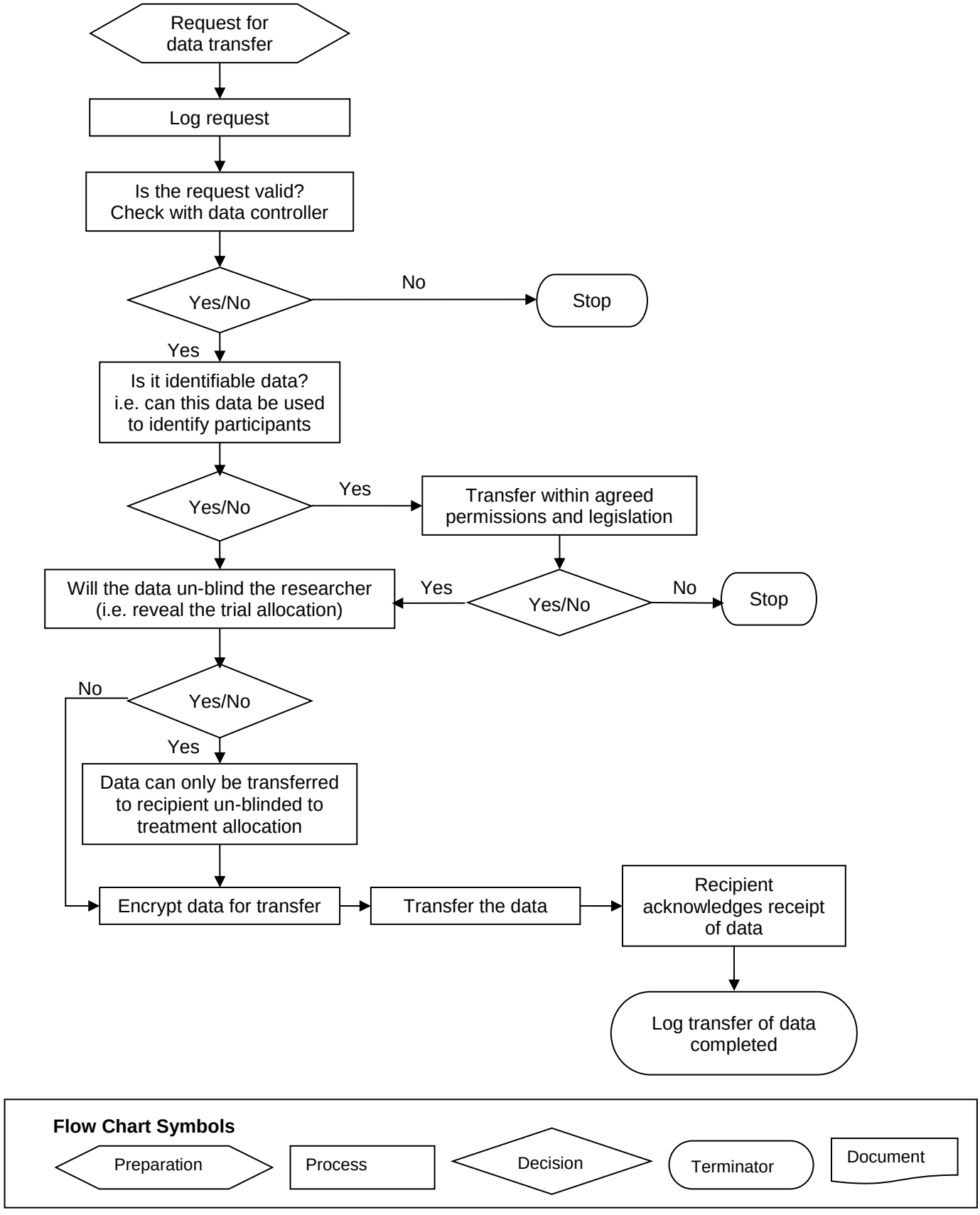
1.1 Project preparation and structure set-up for BCUHB sponsored studies



1.2 Screening for potential participants for research in NHS Settings for hosted and sponsored BCUHB studies



1.3 Data transfer



2. Purpose

The purpose of this SOP is to describe the systems and processes for managing personal data in the course of clinical research activities. Compliance with this SOP will ensure that all information collected during the research process is recorded, handled and stored in such a way that maintains appropriate confidentiality but allows access and use as applicable, whilst satisfying the requirements of UK GDPR the Data Protection Act (2018) and ICH topic E6 Guideline for Good Clinical Practice (See Appendix 1 for Frequency Asked Questions about data protection and research)

3. Scope

This procedure applies to health research, both CTIMPs and non-CTIMPs, Sponsored/hosted by BCUHB. Staff who deal with personal identifiable data of any kind (i.e. paper notes, electronic records etc.) at any time during the process of collection, handling, storing and analysis of research data must comply with this SOP and the requirements of the data protection act. Where researchers are not acting under the management of BCUHB, their own data protection procedures can be applied, however evidence of compliance will be required by the data controller. Please note the term “staff” as used in this document includes all those working within the Health Board including employees, bank, agency, locums, student etc.

4. Responsibilities

Role	Responsibilities
Sponsor	• Protection of research participants’ data • Specific data protection responsibilities may be delegated to the research clinical/site research team or clinical trial unit team
Chief Investigator (CI)	• Protection of research participants’ data • Specific data protection responsibilities may be delegated to the research clinical/site research team or clinical trial unit team
Principal Investigator (PI)	• Protection of research participants’ data • Specific data protection responsibilities may be delegated to the research clinical/site research team or clinical trial unit team
All members of the clinical research/site team and Clinical Trials Unit team	• Protection of research participants’ data
All staff	• Must be aware of their legal and ethical duties in protecting personal data, and ensuring its confidentiality • Are responsible for working within the Data Protection Act 2018 and relevant codes of practice • Are responsible for notifying relevant party in their organisation (e.g. line manager,Information Governance team) directly as appropriate of any changes to the way personal research data are

	processed or stored or any breaches in the confidentiality of the data
Information Governance Team and Caldicott Guardians	• In NHS based research, additional responsibility for data protection issues will lie with the NHS organisation Information Governance Team and Caldicott Guardians

5. Procedures

5.1 Data Custodian

When personal data are being processed a 'data owner' or data custodian should be identified (this would usually be the CI but may be delegated). The named data custodian can be found in the IRAS application. This person has the responsibility to ensure that the security and access arrangements for the personal data comply with the Data Protection Act (2018), and that all data processing and locally held personal data are registered with the host institution according to their employer's processes.

Every organisation that processes personal information must notify the Information Commissioner's Office (ICO), unless they are exempt. Notification is a statutory requirement and failure to notify is a criminal offence. The ICO publishes certain details in the Register of Data Controllers which should be checked to ensure the relevant organisation is registered.

5.2 Access to personal data

5.2.1 Identifying potential participants for clinical research

National guidance allows clinical support staff to work within clinical/site research teams to access clinical data for the purposes of identifying potential participants for research projects. This approach must be clearly defined in the protocol. This data is held within the clinical/site research team and is used to facilitate designated clinical staff to approach potential participants i.e. the health professional responsible for the patients' care makes the first approach to the patient. Clinical staff should document any consent given by participants for their personal details to be passed to third parties such as clinical trial unit research teams. Non-NHS staff are not permitted to access clinical data before consent is obtained from potential participants.

5.2.2 Personal Data should only be processed when:

- a justified purpose for doing so is clearly documented. Within the NHS, data collected as part of clinical care can be used to provide clinical care, auditing and internal service evaluation purposes.
- informed consent has been obtained from each data subject* prior to accessing personal data, and
- protective measures have been taken to restrict access to personal data only to authorised individuals

* Or, where anonymised information (data where any links to the identity of a living individual have been permanently removed) is not sufficient and participant consent is not practicable, approval has been obtained from the Health Research Authority (HRA) Confidentiality Advisory Group (CAG) under section 251 of the National Health Service Act 2006.

5.2.3 Non NHS research staff and handling of recruited participant data

Where research involves NHS patients, data or facilities, members of the study research team may need to be covered by an appropriate Human Resource agreement with the NHS organisation hosting their research. The NHS Research Passport System Resource Pack provides guidance whether researchers will require an Honorary NHS contract or Letter of Access depending on the level of patient contact or access to patient data that 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 organisation data protection policies and attend mandatory information governance training.

5.2.4 Privacy Notices

In some situations, the HRA/HCRW approved document set may contain a Privacy notice or similar information (e.g. data collection of routine data for research purposes without patient consent). Any approved instructions must be followed (such as displaying “opt out” information in patient areas). Any available privacy notices must be highlighted to the research governance team and made available on the BCU Website under the privacy notices for research section.

5.3 Study protocol

When planning the study the CI and clinical/site 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
- how the data are to be stored
- how the data are to be transferred (if applicable)
- how the data are to be analysed
- retention period for data

For Sponsored studies consideration must be given to use of new technologies such as Apps, or any new data sharing arrangements that may be required to undertake the research. In such cases it will be necessary for the Sponsor to seek advice for IG and conduct a study or system specific Data Protection Impact Assessment (DPIA). Guidance as to how to complete these is available on the intranet and also access to standard data sharing agreements.
Please note that DPIAs for the processing of personal data that is undertaken for the purposes of research are the responsibility of the Sponsor. Participating NHS organisations are not responsible for the DPIA of the processing activities that they will undertake on behalf of research sponsors. They are responsible for ensuring that they process data only in accordance with appropriate technical and organisational measures and ensuring they follow the research protocol.

5.4 Participant Information Sheet and Informed Consent form

In addition to the above, and in order to comply with the Data Protection Act (2018) 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

- Where particularly sensitive data is required e.g. medical records, specifically who will be accessing this
- Details of the type and form of any data transfer and storage, and whether participants could be identified e.g. the use of video / audio recording devices
- 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 (or their designated representative) is required.

On the ICF every statement which requires consent should be separate, with space next to each statement for the participant's initials see SOP TM01.

Participant information sheets will contain GDPR transparency wording and the HRA has provided standard text which can be adapted by Sponsors for this purpose. The standard text links to an online information sheet provided by the HRA entitled "Patient Information and Health Care Research" (See links). This leaflet should be available to ALL research participants in paper format should it be required and is available from the R&D Department in Welsh.

5.4.1 Informing the General Practitioner

When a participant's GP is to be informed that their patient has been recruited into a study, the participant or participant representative must be told that the GP will be informed and give their explicit consent, unless there are concerns regarding mental health issues (e.g. potential suicide) where immediate action may be required. This information must therefore be included on the PIS and ICF.

5.4.2 Transfer outside the European Economic Area

Written consent to transfer identifiable data outside of the EEA should be sought from the participant during the informed consent process and the rationale for doing so should be clear in the Participant Information Sheet. Please refer to the Data Protection Act (2018) as it states that personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

5.4.3 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. Access to these health records must only be undertaken by professionals with a legitimate right of access to these records, usually as part of the participant's direct care team. If retrospective access to records is required by individuals without a legitimate right of access, CAG approval will need to be sought from the Health Research Authority. The Wellcome Trust briefing 'Towards consensus for best practice' provides guidance on the use of GP records for research.

5.4.4 Pseudo-anonymous and anonymous data

In most research studies it is not always possible to completely anonymise data as source data verification is required. In such cases data must be 'pseudo-anonymised', and local procedures should be applied. When data are pseudo-anonymised, one master list with the identifier/code and the participants' details is kept separately in order to link the participant to their data. This should be kept in a locked cabinet and office, or as password protected files on a secure data server; no uncontrolled copies of this list should be made. Pseudo-anonymised data qualifies

as personal data under the Data Protection Act (2018). Study monitors may need to access this master list but cannot take copies of it. If researchers involved in data analysis, such as clinical trial unit staff, cannot access the master file list the dataset can be considered anonymous, and does not need to be treated as personal data. For instance, if the database linking participants personal details to their study number is stored on secure NHS servers accessible only by site clinical staff, then pseudo-anonymised data transferred to research staff at other sites can be considered anonymous. 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 Data Protection Act (2018) does not apply, as anonymised data is not considered to be personal data.

5.5 Paper based data

All paper based data not received in an anonymised form must be collected with the permission of study participants, stored securely in a locked cabinet, locked away if unattended and retained for only as long as is necessary to extract the data for analysis. 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 clinical trial unit research team, unless authorised by the Investigator, a member of the clinical/site research team or the Caldicott Guardian. The data will be retained for the minimum length of time possible, following which it will be confidentially destroyed.

5.6 Storage of electronic data

Files containing electronic data must be password protected and stored on a secure network (not a ‘C’ drive or local drive) and security of the data protected. Workstations should be locked (consult IT if assistance needed) if the user is leaving the computer unattended. Please refer to the Information Management &Technology security procedures.

If 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 clinical/site research team members or line managers, as this is a breach of the Computer Misuse Act (1990) and local IM&T Security Policy. Access to the shared drive/network should be removed for any leavers/movers that no longer require access to the information.

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

- 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.
- Files containing direct identifiers should remain in only one location in a secure area of the server and not be copied and saved elsewhere.
- Files containing direct identifiers should not be transferred via email or by other means, except with the explicit consent of the participants (e.g. Letters to their GP).

Participants’ identifiable data must not be stored on home computers, personal

laptops, USB sticks or other removable media. Unencrypted work laptops, portable hard drives, digital cameras or other imaging equipment even if they are password protected should not be used. Encrypted work issued laptops, hard drives and imaging equipment may be used to temporarily store personal data, but such data should be backed up to a secure server at the earliest opportunity and the portable data erased.

All personal data (pseudo-anonymised or anonymised) should be centrally backed up on a secure server.

5.7 Transfer of data

All transfers of study specific data sets should be approved by the Trial Management group and must be logged in an appropriate manner.

5.7.1 By post

Personal information being sent or received by post should be in a sealed envelope marked private and confidential, it must be clearly and fully addressed to indicate who the recipient is (it could be a number of people), and should also include sender details. If there is a large amount of personal information to be sent it should be sent by recorded or special delivery to enable tracking. Audio or video recordings of consultations or interviews should be labelled with unique study identifiers and sent by registered post or secure courier. The transfer and receipt of paper based data should be documented to ensure a clear audit trail is maintained.

5.7.2 Electronic data on CD or USB stick

If it is necessary to transfer data using CD or USB stick, the data sent on CD/USB stick should be password protected and encrypted (e.g. trucrypt), and sent by recorded or special delivery. (Please speak to relevant IT people if you need advice or need to encrypt any data). Check local information security policies (e.g. BCUHB Information Security Policy requires that all USB sticks are encrypted)
A robust system logging the receipt of sent items must be in place either for a CD/USB stick coming into the organisation or leaving the organisation – for example, by registered mail or secure courier, requiring signature on delivery. As with electronic data, the data on the CD/USB stick should be encrypted and password protected (e.g. trucrypt).
Upon receipt of the electronic data the USB stick should be reformatted to erase all data or the CD destroyed.

Please refer to local policies and procedures for further information regarding the encryption of data and management of removable media.

5.7.3 By e-mail

Identifiable data must not be transferred by e-mail unless the e-mail has been encrypted, or all of the data is in an encrypted attachment. BCUHB e-mail is not encrypted by default. It is, however, possible to send queries/information to sites provided that no identifiable data is included and participants can only be identified by a unique study number. Under no circumstances should any identifiable data be used in the subject heading of the email.

Where data is to be transferred by e-mail, records of the transfer (purpose, date, time data provided, and format) should be kept in the study documentation in order to provide a clear audit trail.

Other facilities e.g. the secure file sharing portal are also available to enable secure transfers of data. Further guidance can be sought from the IT department of BCUHB.

The electronic transfer of data should only be done with the research participant's explicit consent and over secure channels. Data that are transferred over the Internet must be encrypted and password protected to maintain security. The encryption key must be sent by a different method. The mechanism for transferring data must allow secure transfer of data either via a client software application or via the World Wide Web. Evidence of secure transfer methods will be required by the data controller. Identifiable information that is not encrypted must not be sent via email.

5.7.4 NHS e-mail

- Emails between addresses ending in @wales.nhs.uk should be secure, however password protection is recommended.
- NHS net to NHS net e-mail (which ends with nhs.net) is secure as it stays behind the firewall
- Any mail coming to or going to an @nhs.uk account is not secure as it goes through public servers.

The sender should limit identifiable information to a minimum, and consider the need to send by e-mail. Care needs to be taken with the addresses and/or number of recipients, and the likelihood of it being forwarded. A confidentiality statement should be included in the email.

5.8 Breach of confidentiality

A breach of confidentiality relating to a research study (e.g. a fax containing hospital notes with a visible name attached, or an email with a data file containing identifiable details) may be reported to a member of staff from an internal or external source. In such situations, the member of staff should contact the person who sent the data and make them aware of the breach of confidentiality. The records received should be either promptly deleted or any identifying details thoroughly erased (ensuring details on paper are not still visible by holding the paper to light for example). Reference should be made to confidentiality agreements of the relevant organisations.

All suspected breaches should be investigated, documented in the study file and reported to the sponsor as appropriate.

For research involving BCUHB all suspected breaches should be reported to the Information Governance team immediately and recorded on Datix, either directly or via your line manager as we may have to report externally to the ICO.

5.9 Data Security

5.9.1 General Principles

It is important that access is limited to the minimum required number of authorised people who need access when they need access i.e. on a need to know basis, and that access is revoked promptly when it is no longer needed.

5.9.2 Blinded data

At the start of a trial two active directory groups will be created, one for blinded access and one for un-blinded access.

All documents relating to a trial should be stored on a shared drive on an organisation's server with access restricted to members of the group(s) related to the trial by means of username and password.

Each project should have a unique folder; within this folder there will be two folders, blind and un-blinded. When adding a document or data to the project it should be determined as to whether it should be added to the blinded or un-blinded folder.

5.9.3 User control

Access to un-blinded data should be controlled through formal request and logging procedures. Approval for access to un-blinded data should be documented in the trial delegation log. For emergency unblinding if there is a safety issue, see SOP S01 Urgent Safety Measures in Research.

5.10 External Data Control

Where it necessary to pass data to external parties e.g. collaborating universities, the request should be logged. The person delegated via the delegation log should approve the transfer of data. When the data is sent it will also be copied to the project folder. Data will be transferred in accordance with section 5.7.

5.11 Password generation and storage

Wherever possible strong passwords should be generated randomly using a password generator e.g. PWGen, and should include a combination of letters, numbers and symbols. Please refer to local procedures for advice on password or pass phrase creation.

It is a requirement that passwords for any shared accounts are stored in a secure manner. This should be shredded as soon as possible. If a password is suspected to have been compromised then it must be changed immediately.

5.12. Deceased Records

In some situations, access to deceased records may be required for research purposes. The Data Protection Legislation applies to living individuals. Especially for any Sponsored research, the Caldicott Guardian must be consulted, as the Caldicott Principles apply to the use of confidential information within the NHS, including from the deceased.

6. Archiving

Source documents, and trial-related electronic and other data must be stored safely and in accordance with the requirement of the Data Protection Act (2018), the clinical trials regulations, the UK Policy Framework for Health and Social Care Research or as stipulated by the Sponsor's requirements (See SOP TM12 Archiving in research) and IG02 -Corporate Records Management procedure. Destruction of records is undertaken according to TM12 and Information Governance confidential waste advice.

7. Training

Training activities will be in accordance with training SOPs T01 Research Quality System Training and T02 Trial Specific Training.

8. Acronyms and Glossary of Terms

Anonymous	Data for which it is impossible to identify the participant from the information alone, or by combining it with any other information held.
Caldicott Guardian	A Caldicott Guardian is a senior person with overall responsibility for protecting the confidentiality of participants and service-user information, and enabling appropriate information-sharing. The Guardian plays a key role in ensuring that the NHS, Councils with Social Services responsibilities and partner organisations satisfy the highest practicable standards for handling patient identifiable information.
CD	Compact Disk
Coded data	Identifiable personal data in which the details that could identify someone are concealed in a code, but which can readily be decoded by those using the personal data. Such coded data are not anonymised data.
Confidential information	Information obtained by a person on the understanding that they will not disclose it to others, or obtained in circumstances where it is expected that they will not disclose it. The law assumes that whenever people give personal information to health professionals/members of a clinical/site research team caring for them, it is classed as confidential as long as it remains personally identifiable. Also covers information disclosure under confidentiality agreements (e.g. Non-Disclosure Agreements).
CAG	Confidentiality Advisory Group
CRF	Case Report Form
CTIMP	Clinical Trial of an Investigational Medicinal Product
Data	Data includes anything from paper and electronic records, to images and sound. Some examples are: trial reports, case report forms, faxed documents, emails and attachments, trial databases, photographs and x-rays.
Data subject	An individual who is the subject of personal data.
EEA	European Economic Area
GP	General Practitioner
HCRW	Health and Care Research Wales
ICF	Informed Consent Form
Personal data	Data which relate to a living individual who can be identified directly or indirectly from those data, or from those data in combination with other accessible information. This includes names, addresses, NHSD numbers, dates of birth, and online identifiers, as well as combinations of data specific to physical, physiological, genetic, mental, economic, cultural or social identity,

	which together might identify an individual (e.g. a dataset containing hospital, gender, age, dates).
PIS	Participant Information Sheet
Processing data	Processing data includes anything from obtaining, recording or holding the data to carrying out any operation on the data, such as altering, using, combining, disclosing or deleting it.
Pseudo-anonymised data	Study participants are given an identifier by which they are known in a system (e.g. Case Record Form, computer database), which is typically a number but may also be an identifier. One master list with the identifier and participants' details must be kept separately in order to link the participant to their data. This is held at the site under the control of the PI. Under the Data Protection Act, pseudo-anonymised data is still classed as personal data.
Sensitive processing of personal data	Section 35(8) of the Data Protection Act (2018) states that "sensitive processing" of data means: a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual; c) the processing of data concerning health; d) the processing of data concerning an individual's sex life or sexual orientation.
SOP	Standard Operating Procedure
Transfer of data	In this SOP, transfer of data means the transmission of data from sender to a recipient or the removal of data from one location to another.
Uncontrolled copy	Is any document that does not meet the criteria of a controlled copy. A controlled copy is always at the correct/latest version. When a change is made, it is retrieved and replaced in an authorised manner.
USB Stick	Universal Serial Bus memory stick or flash drive, a portable data storage device.

9. Documents to read alongside this procedure

- BCUHB Research Governance Framework Policy R&D01
- BCUHB Code of Conduct (Disciplinary rules and standards of behaviour) WP6BCUHB Confidentiality Code of Conduct IG13
- NHS Wales Information Governance Policy
- NHS Wales Email Use Policy
- NHS Wales Internet Use Policy
- BCUHB Notification of Information Security Breach Procedure IG24
- BCUHB Email procedure IG08
- BCUHB Procedure for Information Management and Technology (IM&T) Security IG14

- UK Policy Framework for Health and Social Care Research (2017)
- Wellcome Trust Briefing 'Towards Consensus for Best Practice. Use of patient records from general practice for research.' June 2009

10. References and SOP Links

- SOP T01 Research Quality System Training
- SOP T02 Trial Specific Training
- SOP TM12 Archiving in Research
- SOP S01 Urgent Safety Measures in Research
- The Data Protection Act (2018) https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
- The Computer Misuse Act (1990) https://www.legislation.gov.uk/ukpga/1990/18/contents
- Health Research authority GDPR Guidance:
  - https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/
- Information Commissioners Office Guidance on research Provisions within UK GDPR and DPA 2018
  - https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/research-provisions/
- HRA standard information leaflet for research participants:
  - https://www.hra.nhs.uk/information-about-patients/
- UK Research and Innovation : GDPR and research an overview for researchers:
  - https://www.ukri.org/about-us/policies-standards-and-data/gdpr-and-research-an-overview-for-researchers/
- Welcome Trust "Towards Consensus for Best Practice"
  - https://wellcomecollection.org/works/hmdp4ua7
- Coldicott Guardian Principles:
  - https://www.ukcgc.uk/caldicott-guardians-manual

11. Appendices

Appendix 1:

The UK GDPR and Data Protection Act 2018: FAQ for Research

Appendix 2:

Data Protection Principles Summary

Appendix 1:

The UK GDPR and Data Protection Act 2018: FAQ for Research

The UK General Data Protection Regulation sits alongside the Data Protection Act 2018 to for the primary data protection law in the UK. These laws contain provisions for processing personal data for research purposes.

- What is personal data?
  Personal data is data that relates to living people from which they can be directly or indirectly identified. Directly identifiable data means identifiable from the data itself and indirectly identified being from the combination of the data or other available data, Data that has been pseudonymised (with identifiers separated), may still be personal data depending on how hard it is to reconnect the identifiers with the data set.

- What is meant by “Processing?”
  In relation to personal data, processing means any operation or set of operations which is performed on personal data (or sets of personal data) which includes collection, recording , organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction.
  Note that the process of anonymising data counts as “processing”,

- What is a data controller?
  A person, public authority, agency, or other cody which alone or jointly with others determines the purposes and means of processing of personal data. In research this is usually the Research Sponsor and they are accountable to the ICO. However there may be more than one controller and please seek advice from R&D for queries in relation to this.

- What is a data processor?
  A person, public authority, agency or other body which processes personal data on behalf of a controller. In research this is usually the research site.

- What is the lawful basis for research?
  The UK laws demand that data processing is lawful, fair and transparent. There are 6 lawful basis for processing personal data. For research the lawful basis is usually public interest as set out in Article 6 of UK GDPR:

  e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

  Consent is another lawful basis for processing personal data, however note the ICO states that consent should only be considered when no other lawful basis applies and therefore not likely to be the lawful basis used for research. This is not to be confused with the requirement of Good Clinical practice, the Declaration of Helsinki, and other legal reasons in which seeking informed consent to participate in research where this is appropriate and possible is a requirement.

Processing of personal data will be explained in the HRA/HCRW approved information sheets and should be part of the informed consent discussions.

- What does being fair and transparent mean for my research?
  This includes respecting participants rights and ensuring that personal data is used in line with their expectations as explained in the research information sheets or study specific privacy notices.

- What about transfer of personal data outside of the EU?
  Individuals risk losing the protection of the UK data protection laws if their personal data is transferred outside the EU. The UK GDPR restricts the transfer of personal data to a separate organisation located outside of the UK, unless the rights of the individual in respect to their personal data are protected in another way , or one of a limited number of exceptions applies. See the ICO website for more information.

Appendix 2

Part 3, Chapter 2 of the Data protection Act (2018) – Principles Summary

See article 5 of UK GDPR

Seven Key Principles:

Personal data shall be:

"(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')

And

"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."