Data Protection Guidance Document

This document provides guidance and definitions for researchers and JRMO Staff to supplement JRMO SOP 16a. Topics are listed in alphabetical order, if the topic you are searching for cannot be found then please email the GCP and Compliance Team via research.governace@qmul.ac.uk

Contents

1. Abbreviations

ATIMP	Advanced Therapy Investigational Medicinal Products
Barts Health	Barts Health NHS Trust
BCI	Barts Cancer Institute
CAG	Confidentiality Advisory Group
CTIMP	Clinical Trials of Investigational Medicinal Products
CTU	Clinical Trials Unit
DBST	Data Security and Protection Toolkit
DPA	Data Protection Act
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
FoIA	Freedom of Information Act
GDPR	General Data Protection Regulation
HRA	Health Research Authority
ICF	Informed Consent Form
ICT	Information and communications technology
IG	Information Governance
IRAS	Integrated Research Approval System
JRMO	Joint Research Management Office
MHRA	Medicines and Healthcare products Regulatory Agency
OID	Organisation Information Document
PID	Personal Identifiable Data
PIS	Participant Information Sheet
Queen Mary	Queen Mary University of London
REC	Research Ethics Committee
RIGG	Research Information Governance Group
SMD	School of Medicine and Dentistry

2. Personal data and types of anonymisation

Health Research Authority (HRA) definition of personal data: 'Personal data' means 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.

Whether a data set is personally identifiable or not is dependent on how many data points there are, what these are and the combination of data sets. For example, in most cases it would not be possible to identify someone from a date of birth or a postcode alone. But if a dataset contains both date of birth and postcode, it may be possible to identify individuals.

2.1 Pseudonymised data – Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific person without the use of additional information. Such additional information must be kept carefully separate from personal data. Note that personal data that has been pseudonymised – e.g., key-coded – should be considered identifiable and managed as such.

2.2 Anonymised data - Anonymisation is the complete and irreversible removal of any information that could lead to an individual being identified, either from the removed information itself or this information combined with other data. Data that have been anonymised are considered to be out of scope of data protection legislation. It is worth noting that the act of Anonymisation is processing personal data.

3. Background Data

Electronic data systems will often store more data than is first apparent. In addition to the foreground data that is directly entered by users, the system will generate and maintain background data. For example:

Metadata are data that provide information about other data – usually the foreground data entered by users. For example, the metadata for this sentence would include that it is in Arial font, font size 11, colour black, the name of the person who wrote it and the date and time that it was written.

An Audit Trial is used to track the changes that are made to data in a system. For every datum that is entered into the system, the audit trail will record who entered it, when it was entered and its value. If the datum is later changed, the audit trail will record this change but will not delete the original entry – both will be retained in the system.

4. Data Subject Access requests (also known as Subject access requests)

Individuals have a right to find out what data an organisation holds about them and obtain a copy of this. If it is a public organisation (such as a university or NHS Trust), members of the public should write to their Data Protection Officer (DPO). The DPO contact details for the organisation should be on the organisation's privacy notice.

The organisation must provide a copy of the data they hold about the individual as soon as possible, and within 1 month at most.

There are some situations when organisations are allowed to withhold information, for example if the information is about:

- The prevention, detection, or investigation of a crime.
- National security or the armed forces.
- The assessment or collection of tax.
- Judicial or ministerial appointments

An organisation does not have to say why they're withholding information.

The same applies to research data where research participants can request to see the data that Barts Health NHS Trust (Barts Health) or Queen Mary University of London (Queen Mary) holds about them. They should be directed to the appropriate team within the organisation. If you receive a Subject Access Request, please immediately inform the correct team.

5. Data Flow mapping

Data flow mapping helps identify all the information you hold and how it transfers from one location to another, such as from different Sites or vendors through to the study statistician. Simple steps could be:

- Document the scope and purposes of processing

Document every step of each process in your organisation, detailing who carries out each step and what assets are used.

- Add personal data to a data flow map of each process

Start your data flow map by recording what personal data enters into the scope of a given process.

- Add the supporting assets used to process personal data

Map the devices, applications or functions that are used to process personal data.

- Add data transfers to show the flow of data between assets

Mark how data flows between assets, detailing which data items are transferred and the methods used to do so.

- Review the process

View and print reports to share with stakeholders. Update the process map and details whenever changes are made to the process.

6. Data Protection Impact Assessments

All research seeking sponsorship by Barts Health or Queen Mary must submit a Data protection Impact Assessment (DPIA) screening form to the relevant organisations team (see SOP 11a_Sponsorship of MHRA regulated studies (Process for Researchers)) requested to complete a full DPIA prior to sponsorship being granted.

A DPIA is a process to help organisations identify and minimise the data protection risks of a project.

DPIA must be completed for processing that is likely to result in a high risk to individuals.

This includes some specified types of processing.

It is also good practice to complete a DPIA for any other major study which requires the processing of personal data.

The DPIA will:

- Describe the nature, scope, context, and purposes of the processing.
- Assess necessity, proportionality, and compliance measures.
- Identify and assess risks to individuals; and
- Identify any additional measures to mitigate those risks.

At Barts Health and Queen Mary, the Barts Health Information Governance (IG) team and Queen Mary Records & Information Compliance Manager lead on this process with the study team.

7. Data Security and Protection Toolkit

The Data Security and Protection Toolkit (DBST (previously called the IG toolkit)) is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards.

All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

Some Organisations (NHS DIGITAL) will require evidence of toolkit status prior to information of data being transferred or shared.

Barts Health is registered as a primary user, whilst several sections of Queen Mary School of Medicine and Dentistry (SMD) are registered as secondary users. For further details: Barts Health – contact the Barts Health IG department for Queen Mary - contact the SMD Research IG group.

7.1 Transfer of data and associated data

When exporting a curated dataset from a database it is important to make sure that the audit trail and metadata do not include any undesired data. For example, while all Personal Identifiable Data (PID) may have been removed from the foreground data, the audit trail or metadata may still contain PID. In a blinded study, background data transferred to blinded study team members must not include any information that could unblind them.

Where data is stored electronically, it is important to be aware of the background data stored within the system and whether this will be included in the transfer.

Imaging scans are normally de-identified prior to transfer for central review. It is important to make sure that the method of anonymization removes all identifiable information from the DICOM tags attached to the imaging file, as well as from the images themselves. (See DICOM section)

Conversely, there are times when it is important to make sure that the full audit trail and metadata are included in a data transfer. Examples of this include when transferring the full dataset from one database to another, or when providing the dataset for regulatory inspection.

Please refer to JRMO 38a Use of Computerised equipment in clinical research and SOP 38b Electronic data management systems for MHRA-regulated studies for details of how transfer system details should be documented and approved.

* Please ensure sites are aware of the need to de-identify at feasibility to so time and cost can be included.

DICOM Tags are information and metadata attached to medical imaging files such as CT scans, MRI scans or x-rays which provide additional information about the scan. Most systems used to transfer imaging scans to disk or transmit them over the internet will transfer the DICOM tags along with the images. If background data contains identifiable information or unblinded information, then access to it must be controlled.

When data must be completely deleted (e.g., removal of erroneously recorded PID) it is important to make sure that the data is removed from the audit trail as well.

At Barts Health please contact salma.abdullahi3@nhs.net to discuss this for the type of images you are using and how you wish to transfer them, there will be a cost associated.

8. Encryption of portable devices

Encryption is a mathematical function using a secret value—the key—which encodes data so that only users with access to that key can read the information.

Encrypting data whilst it is being stored (e.g., on a laptop, mobile, USB or back-up media, databases, and file servers) provides effective protection against unauthorised or unlawful processing. It is especially effective to protect data against unauthorised access if the device storing the encrypted data is lost or stolen. However, it is important that strong passwords are used for the protection to be effective.

Contact the applicable Information and communications technology (ICT) or Information Governance department at Barts Health or Queen Mary for guidance on encrypting data and information.

9. External access to source data

The researcher is responsible for ensuring any access to Barts Health or Queen Mary source data is clearly defined in the study paperwork and would need to be assessed as part of capability and capacity review. Full justification as to why this source data is being accessed should be provided. The participants should be aware and consent to this, as appropriate.

The Joint Research Management Office (JRMO) team may need to be involved to ensure the site agreement /Organisation Information Document (OID) fully covers this activity or an appropriate data sharing/ transfer agreement is in place.

It may be necessary to discuss with Barts Health or Queen Mary IG teams if novel agreements or transfer systems are to be used and they can always be consulted as required.

10. Freedom of Information requests

The Freedom of Information Act (FOIA) and Freedom of Information (Scotland) Act (FOISA) aims to promote greater openness about the way public authorities operate and gives members of the public a right to access information held by public authorities.

If you receive a FOI request, please contact the relevant organisations FOI Contact: Queen Mary foi-enquiries@qmul.ac.uk and Barts Health: foi.bartshealth@nhs.net

11. HRA transparency wording

HRA transparency wording is standard text placed within participant information sheets in order to comply with the transparency requirements of General Data Protection Regulation (GDPR).

The HRA expects those with a study that was in progress on 25 May 2018 to have changed their wording. There is no requirement for those who have adopted to use the original wording published in May 2018 to further amend their text unless they wish to do so (in which case it will be regarded as a non-notifiable amendment as previously and does not need to be submitted to HRA). The wording provided on the HRA website (https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/templates/transparency-wording-for-all-sponsors/) is therefore for new studies and will help to avoid being asked to make changes to participant information during approval.

12. National opt out

The national data opt-out was first introduced on 25 May 2018, enabling patients to opt out from the use of their data for research or planning purposes, in line with the recommendations of the National Data Guardian in her Review of Data Security, Consent and Opt-Outs.

Patients can view or change their national data opt-out choice at any time. For details can be found via https://digital.nhs.uk/services/national-data-opt-out.

All health and care organisations are required to be compliant with the national data opt-out policy. The NHS national opt out only applies to research studies that use SECTION 251 exemption (Confidentiality Advisory Group (CAG) approval) and the Barts Health IG team have been working with study teams across Barts Health to ensure they are ready when the NHS opt out comes into force.

Please contact Barts Health IG team bartshealth.infogov@nhs.net for details of local implementation.

13. NIGB and Social Care approval (now defunct).

An independent statutory body that was responsible for Section 251 of the NHS Act 2006 in England and Wales; and reviewed applications for use of identifiable data where consent was not practicable. From April 2013 this function transferred to the HRA, the CAG now performs this function.

14. Queen Mary SMD safe haven

Barts Cancer Institute (BCI) are currently undertaking a review and refresh of their IT Infrastructure with the aim of providing a Data Safe Haven for the SMD. The Data Safe Haven Network will support:

- New server and storage infrastructure at Charterhouse Square and an off-site Datacentre
- New dark fibre links between Charterhouse Square and the off-site Datacentre
- New client workstations at a number of Queen Mary campuses

The Data Safe Haven is Queen Mary SMD's technical solution for storing, transferring, and analysing research information that contains patient identifiable or other highly confidential data.

The Data Safe Haven must comply with NHS Digital's Data Security and Protection Toolkit, which is aligned to the GDPR, Data Protection Act (DPA) 2018 and ISO 27001:2013 Information Security Standard.

Once the Data Safe Haven is complete it will be expected to be able to store, transfer and analyse any and all data that the SMD is responsible for safeguarding which will include patient identifiable and other highly confidential data.

Governance of the Data Safe Haven will be managed through Research Information Governance Group (RIGG), SMD IG Leads and the Queen Mary Records & Information Compliance Manager.

15. Recruitment and consent process

It is important to consider the recruitment and consent process when planning your study.

Will informed consent be received? If yes, then ensure relevant sections within Integrated Research Approval System (IRAS) form (A27-A34) are completed appropriately detailing methods of recruitment and consent process.

If consent will not be received, then a clear explanation required as to why this is the case and CAG Application form will need to be completed (Section 251). Please refer to CAG website and guidance (Associated document 2 Barts health CAG (Section 251) application form guidance and associated document 3 Queen Mary CAG (Section 251) application form guidance).

16. Role of data controller and data processors

"Data controller" means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are or are to be processed. In the area of research, this is usually the Sponsor. The data controller should be an organisation not an individual.

"Data processor", in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller. The data processor can be a third party external to the organisation e.g., a site or Clinical Trials Unit (CTU).

"Processing", in relation to information or data means obtaining, recording, or holding the information or data or carrying out any operation or set of operations on the personal data, including:

- Organisation, adaptation or alteration of the information or data,
- Retrieval, consultation or use of the information or data,
- Disclosure of the information or data by transmission, dissemination or otherwise making available,
- Alignment, combination, blocking, erasure or destruction of the information or data

17. Role of Data Protection Officer

The GDPR introduces a duty for Public organisations to appoint a DPO.

DPOs monitor internal compliance, inform, and advise on data protection obligations, provide advice regarding DPIAs and act as a contact point for data subjects and the supervisory authority.

The DPO must be independent (has no conflicts of interest in the organisation), an expert in data protection, adequately resourced, and report to the highest management level.

A DPO can be an existing employee or externally appointed.

In some cases, several organisations can appoint a single DPO between them.

DPOs can help demonstrate compliance and are part of the enhanced focus on accountability.

The DPO for Queen Mary is Jonathan Morgan and the DPO for Barts Health is Sarah Palmer Edwards

18. Role of Caldicott Guardian

A Caldicott Guardian is a senior person within a health or social care organisation who makes sure that the personal information about those who use its services is used legally, ethically, and appropriately, and that confidentiality is maintained. Caldicott Guardians should be able to provide leadership and informed guidance on complex matters involving confidentiality and information sharing.

The Caldicott Guardian should play a key role in ensuring that their organisation satisfies the highest practical standards for handling person-identifiable information. Their main concern is information relating to patients, service users and their care, but the need for confidentiality extends to other individuals, including their relatives, staff, and others. Organisations typically store, manage, and share personal information relating to staff, and the same standards should be applied to this as to the confidentiality of patient information.

The Caldicott Guardian within Barts Health is Anita Anghi (contact through bartshealth.infogov@nhs.net).

Queen Mary does not officially need to have an appointed Caldicott Guardian as it is not a health or social care organisation, but to assist with DSBT applications and governance Coleen Colechin nominally acts as the Queen Mary Caldicott Guardian.

19. Safe transfer of data by email

Wherever possible, PID should be sent and received using nhs.net accounts. Transferring data between two nhs.net accounts is secure but using other email services (including qmul.ac.uk) to either send or receive the data is not.

If PID must be sent or received from another email address, it must be stored in an encrypted password protected file. Microsoft Office files can be encrypted by clicking *File* > *Info* > *Protect Document* > *Encrypt with Password*. A strong password should be used by avoiding common words and phrases, using a combination of upper and lower case letters, numbers, and symbols and by making the password as long as is practical. The password must be communicated to the receiver separately, ideally using a different method of communication (e.g., telephone), in order to reduce the risk of the password being intercepted.

20. Storage and use of data after the end of the study

It is vital that participant information sheets and informed consent forms clearly and accurately describe how participant data will be managed. All participant information sheets must confirm that data will be held for the duration of the retention period (30 years for Advanced Therapy Investigational Medicinal Products (ATIMPs), 25 years for Clinical Trials of Investigational Medicinal Products (CTIMPs) and other interventional research, 5 years for observational research) and must include GDPR transparency wording or privacy notice.

Researchers should consider the future use of research data when designing their study and seek consent from participants for future use of data. This can include entering the data in a research database.

Once a study has completed, research data must be archived for the duration of the retention period. Please see JRMO Standard Operating Procedure (SOP) 20: Archiving for more information on the archiving process.

The Queen Mary retention schedule is available on:
http://www.arcs.qmul.ac.uk/governance/information-governance/records-management/records-retention-schedule/

Barts Health retention policy is available on We share.

21. Transfer of data outside of the UK & EEA

NHS Research Ethics Committee (REC) applications, participant information sheets and informed consent forms must clearly state if PID will be sent to third parties and how the data will be managed once it is received. A contract defining the use of the data must be in place between the study sponsor and the receiving party before any PID is transferred. In Medicines and Healthcare products Regulatory Agency (MHRA) regulated studies, the third party must undergo sponsor vendor assessment.

The minimum amount of PID should be transferred to third parties. Data must be encrypted during the transfer.

Further information on transfer of data outside of the UK and EEA can be found through the following link **https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/#ib5**

NB This section will be affected by the arrangements put in place from Brexit, please Speak to JRMO.

22. Use of personal devices

PID relating to trial participants must not be stored on personal mobile phones, on other personal devices or in personal paper records.

Where researchers need to access PID remotely this must be done using an approved solution such as a managed laptop or a virtual private network provided by the organisation's IT department. If unsure whether a solution is acceptable, please contact the organisation's information governance department.

Specifically, Barts Health has a suite of guidance documents for the trust regarding permissible activity – these are located on We share.

23. Use of trial data for further research studies or audits

Data collected within one study cannot be retained and used for any other purpose. When setting up a study consideration should be given to the possibility of using data for future research or be part of open access sharing.

Should either of these be required the study it should be made clear in the protocol, declared in the Participant Information Sheet (PIS)/Informed Consent Form (ICF) and specific consent sought.

If added after approvals participants should be asked to re-consent unless CAG approval is sought.

Whatever the participant consents to with regards to their data (destroyed after study, kept for future studies) is what must happen to the data.