QUALITY MANAGEMENT SOP

SOP Number: BTC-SOP-QM-002

SOP Version: 3.0

Click here to record your training for this SOP

	NAME	TITLE
Author	Rachael Heys	Quality Assurance Manager
Reviewer	Melanie Lewcock	Head of Bristol Trials Centre Strategy
Authoriser	Melanie Lewcock	Head of Bristol Trials Strategy

Release Date:	26/02/2024	**Implementation Date:**	26/03/2024

Review Due:	26/03/2026

Implementation plan

This Standard Operating Procedure (SOP) should be implemented within two weeks from the 'Release Date' to allow for staff training.

Note to User:

It is your responsibility to ensure you are using the latest approved version of this SOP. Please note that versions may be superseded before their initial review date.

THIS IS AN UNCONTROLLED VERSION WHEN PRINTED.

If you are reading this document in printed form, please check that the version number and date match the most recent SOP's details. Current versions of all Bristol Trials Centre (BTC) SOPs and accompanying documents are available on the BTC Teams.

Table of Contents

1. PURPOSE

Good Clinical Practice (GCP) requires the implementation and maintenance of quality assurance and quality control systems to ensure that studies are conducted, and data generated recorded and reported, in compliance with the protocol, GCP, and the applicable regulatory requirements.

The **Quality Management System (QMS)** at the BTC comprises the tools, processes and procedures for ensuring that the Centre's functions are performed to the highest standards and the research studies conform to all relevant ethical and regulatory requirements and satisfy contractual obligations.

Quality management documents consist of **Standard Operating Procedures** and **Process Documents** which are documents supporting the SOPs and working practices (templates, forms, instructions, etc).

The purpose of this SOP is to describe the quality management system and how it is managed to ensure that the BTC meets expectations and promotes best practice, and the process for planning, conducting, reporting and following up quality checks and audits to ensure that any selected processes are compliant with applicable requirements and all audit activities are conducted with a consistent approach.

2. SCOPE

This SOP applies to all BTC staff actively involved in research within the BTC; it covers all activities pertinent to the development, implementation and maintenance of the QMS at BTC, and all processes and activities pertinent to quality checks and internal audit at the BTC.

It does not cover any monitoring or auditing performed by Sponsors in order to meet their responsibilities.

The Chief Investigators (CI) must be made aware of this SOP and as a minimum, be signposted to the SOP by BTC.

NB: Throughout this document the terms 'research', 'study, 'research project', and 'trial' will be used interchangeably to denote those projects which fall under the remit of the UK Policy Framework for Health and Social Care Research 2017, unless a clear distinction is made.

3. DEFINITIONS, ACRONYMS AND ABBREVIATIONS

Quality Assurance (QA): Planned, systematic actions and processes established to ensure delivery of research in compliance with applicable regulatory requirements and GCP.

Quality Control (QC): The real-time, ongoing operational techniques and activities undertaken within the quality assurance system to verify that the requirements for quality of the study-related activities have been met.

Quality Management (QM): The overall system, including structures and responsibilities, which provides the framework for all quality management activities (including QA and QC), used to facilitate compliance with quality standards, identify areas in need of corrective action and enable quality improvement.

NB: For all other definitions, acronyms and common abbreviations refer to the BTC-RES-TM-001 Definitions and Acronyms document available on the BTC Intranet.

4. RESPONSIBILITIES

Any delegation of these responsibilities should be clearly documented.

4.1 Bristol Trials Centre

It is the responsibility of the BTC to:

- Ensure that all research activities are fulfilled in a professional manner, consistent with the requirements and expectations of Sponsors, GCP principles, UK Policy Framework for Health & Social Care Research and any applicable regulations, to ensure the rights, safety and well-being of participants and the scientific integrity of work undertaken.
- Ensure that members of staff are aware of the requirements of the QMS and their responsibilities in terms of its implementation and maintenance.
- Promote risk-based quality management by putting in place processes to identify, assess, control and review risks associated with the research studies it undertakes during their lifecycle.
- Introduce proportionate adaptation of conventional practices regarding the management, monitoring and conduct of the studies.

4.2 Quality Assurance manager or delegate

It is the responsibility of the QA manager (or delegate) to:

- Lead the implementation and further development of BTC QMS.
- Organise training associated with the implementation and maintaining of QMS.
- Review processes and procedures to ensure quality is maintained across all stages of research.
- Ensure that quality management documents are available for areas of work relevant to the core functions of the BTC. Centrally manage the distribution and control of the BTC SOPs.
- Ensure that staff receive appropriate SOP training, and such training is recorded according to instructions given at the time of SOP release.
- Review SOPs and provide input regarding clarity, suitability and assignment of roles and responsibilities and assess documents associated with SOPs (e.g. working instructions, templates) to ensure their ability to promote compliance.
- Ensure that processes are in place to identify non-compliances and inefficiencies as well as examples of commendable processes or tools, providing assurance that processes meet (or will meet) requirements as per applicable regulations, contractual arrangements and GCP.
- Conduct or coordinate quality checks and internal audits (scheduled or triggered (for cause)) on studies or internal processes, and request remedial actions and make suggestions for process improvements; communicate findings to appropriate study staff and senior management respectively.

- Provide support to study teams in the preparation for inspections and audits, determining the adequate documentation applicable for specific studies to support the inspection or audit.

4.3 SOP Author or delegate

It is the responsibility of the SOP author (or delegate) to:

- Generate, finalise, and release the SOP in accordance with the BTC-SOP-QM-001.
- Ensure that the SOP remains fit for purpose.
- Ensure that the SOP is reviewed and amended as required.
- Provide relevant training and education materials to ensure that staff are aware of their responsibilities in relation to SOP content and management.

4.4 SOP user

It is the responsibility of the SOP user to:

- Ensure compliance with this document.
- Become familiar with the QMS pertinent to their role and duties performed within the BTC.
- Read relevant quality management documents and any updates in a timely manner, undertake any relevant training and record training according to applicable SOPs.
- Review procedures during use of the SOP and inform the author of any changes required.

5. SPECIFIC PROCEDURES

5.1 Documentation

5.1.1 Quality Management documents

Quality Management documents are non-study specific documents designed and implemented to ensure that BTC staff can fulfil their obligations and responsibilities, in accordance with applicable regulatory requirements, GCP and contractual arrangements.

5.1.1.1 Standard Operating Procedures (SOPs)

SOPs are written instructions communicating the agreed, defined methodology which must be followed to ensure that regularly performed tasks are completed consistently and uniformly across research teams and studies.

All BTC SOPs are written and reviewed in accordance with BTC-SOP-QM-001 Development and Management of Standard Operating Procedures.

All studies adopted by the BTC and all BTC staff follow the BTC SOPs (unless it has been agreed and documented that specific Sponsor SOP(s) will be used for a study).

Study-specific SOPs however should not be required; adequate instructions should be provided in the study protocol, or study-specific work instructions, manuals, or similar.

Where there is a request for a study-specific SOP an appropriate member of the senior BTC staff and/or the Quality Assurance manager should be consulted and agree in principle. If agreed, the SOP should be written by the CI or delegated to an identified individual deemed to be best qualified by experience or competency. If it is anticipated that the study specific SOP may deviate from what is outlined in the existing BTC SOPs, this must be discussed and agreed beforehand with the QA manager, and such agreed deviations must be documented in the Trial Master File (TMF).

5.1.1.2 Process documents

SOPs may be complemented by other documents (including but not limited to checklists, templates, work instructions, guidance, etc). These supporting documents may be developed and reviewed by the QA manager (or delegate) or other BTC Task and Finish Group as appropriate. Membership of these groups is published, and members of staff are expected to submit suggestions for quality improvements to the appropriate group.

5.1.2 Essential documents

Good documentation and document control is essential for ensuring the safety of participants and the quality of data in research studies. Essential documents are documents which individually and collectively permit evaluation of the conduct of a study and the quality of the data produced. Essential documents include protocols, participant information sheets/leaflets (PIS/PIL) and informed consent forms (ICF), General Practitioner (GP) letters, advertisements, and data collection tools including case report forms (CRFs).

All studies must have a TMF. All essential documents are either held in this file, or if held elsewhere (e.g. CRFs or master randomisation scheme), the location of these documents is recorded in the TMF. Each participating research site must keep an Investigator Site file (ISF).

Minutes documenting key decisions should be produced for all study-related meetings, including teleconferences. Study-related email correspondence should be saved to a study-specific mailbox.

Procedures for setting up, maintaining and archiving the TMF and ISF are detailed in the BTC-SOP-TM-001 Study Start Up, BTC-SOP-TM-002 Study Conduct and BTC-SOP-TM-003 Study Close Down SOPs, respectively.

5.1.3 Preparing a new document

Preparation of new documents will depend on the type of document.

Members of staff should liaise with the QA manager should a need for a new SOP or process document be identified, or an unscheduled update to a current SOP or process document be required. The procedure for preparing a new SOP is described in the BTC-SOP-QM-001 Development and Management of Standard Operating Procedures.

Study-specific documentation should be developed in accordance with the BTC-SOP-TM-001 Study Start Up.

A flowchart summarising the preparation of a new process document is provided in Appendix 1.

5.1.4 Document control

The purpose of a controlled document is to ensure that relevant personnel have access to the latest versions of the documents they need to do their job or undertake a specific task.

Controlled documents may be administrative, including quality management documents, and study-specific including those which are defined as essential documents (see section 5.1.2). They can be in hard copy or online or part of a document database.

Controlling documents involves the following:

- Ensure that documents are and remain legible and readily identifiable; this refers to a numbering/naming convention applied to identify documents, as well as the format of the document.
- Approve documents for adequacy prior to issue; depending on the type and importance of the document, it could just require approval by one person (e.g. a trial manager), or by multiple people (e.g. a senior BTC member of staff and the QA manager).
- Review and update as necessary and re-approve documents; this can be periodically and/or when changes occur which need to be captured.
- Ensure that changes and the current revision status of documents are identified; this includes versioning and revision history.
- Ensure that external documents determined to be necessary (e.g. procedure/user manual provided by Sponsor to be used in a study) are identified and their distribution is controlled; these documents should be controlled in the same way as the internal documents.
- Ensure that relevant versions of applicable documents are available at points of use; this includes storage and distribution of revised copies and notifications of changes.
- Prevent the unintended use of obsolete documents, and apply suitable identification to them if they are retained for any purpose i.e. moving the documents from a shared folder to archive.

Different types of documents will need different levels of control. The appropriate document control procedure should be applied to all documents produced by BTC staff and to documents generated externally where appropriate.

All SOPs must be controlled, maintained and reviewed in accordance with the BTC-SOP-QM-001 Development and Management of SOPs to ensure that they are current, written and authorised by appropriately competent personnel, regularly reviewed and fit for purpose.

For each study a record should be kept of which SOPs apply at which points for the duration of that study.

Study specific documents must be reviewed by suitably qualified member(s) of the research team, which may include BTC staff.

Specific requirements apply for certain documents such as the protocol, Case Report Forms (CRFs), Statistical Analysis Plan, database specification (e.g. sign off).

5.1.5 Version control and naming conventions

All documents must comply with a standard numbering and versioning system to ensure that only current finalised copies are used. The version number and title must be consistent throughout the document.

The version number is in the format of X.Y (e.g. 1.0). During the development of a new document, draft versions are numbered 0.1, 0.2 etc. Finalised documents have whole number version numbers. The first published version should be named Version 1.0. Reviews and redrafts of existing (previously finalised) documents are numbered by increasing to the next decimal (1.2, 1.3, 2.2, 2.3 etc.). Once a revised document is agreed it should take the next whole version number (2.0, 3.0 etc.)

This convention is applied to all documents (BTC wide quality management documents and study-specific).

When saving documents as electronic files, the filename should accurately reflect the document title, using abbreviations and acronyms only if clear. The filename should provide sufficient information to identify the document.

Document identification codes must be used for all SOPs and process documents, comprising a unique alphanumeric code: BTC, followed by a text prefix denoting the type of document (SOP, template, etc), followed by category, (e.g. trial management (TM), quality management (QM), etc.), as per BTC-SOP-QM-001 Development and Management of Standard Operating Procedures, followed by three digits indicating the document number (allocated sequentially beginning with 001 for all documents).

- SOPs: BTC-SOP-XX-001 where ‘XX’ indicates the SOP category and the last digits the document number
- Process documents and respective codes may be:
    - Work Instructions: WI – e.g. BTC-WI-TM-001
    - Templates: TEMP
    - Checklists: CHK
    - Forms: FM
    - Frequently Asked Questions: FAQ
    - Other resources, e.g. supporting documents or guidance: RES.

Study-specific documents names contain the acronym identifying the study, the type of document (e.g. protocol) and version number.

Electronic documents name will display the code and the name of the document or a brief description after the code and the version number.

All controlled documents should have the following information available on the front page and/or as a header/footer on each page:

- BTC logo and/or name (if appropriate).
- Page number (unless a single page), preferably using “page x of y”.
- Title of the document.
- Version number.
- Names of individuals responsible for the document (author/reviewer/authoriser) where appropriate.
- The effective date and/or implementation date as/where appropriate.
- “Uncontrolled version when printed” if appropriate.
- “Not to be used or reproduced without permission” if appropriate.

In addition, study-specific documents must always bear the study name/acronym and an official identifier, such as the IRAS ID and EudraCT number, as appropriate.

Minutes of meetings should also include the date of meeting and attendees and those who sent apologies.

5.1.6 Revisions

The procedure pertinent to SOP review and revisions is described in the BTC-SOP-QM-001 Development and Management of Standard Operating Procedures.

The revision procedures described in this SOP are applicable for both process documents and study-specific documents.

Revisions to current documents should be undertaken by individuals with the relevant qualifications and experience.

Brief details and reasons for the changes should be identified as appropriate e.g. by recording them in a Change History table. It should be clear whether the change is minor, administrative in nature, or it involves a change in processes.

Revisions will undergo the same draft and review procedure as described above until drafting is complete.

Documents that do not usually have a set review date should be updated as required (e.g. where new information becomes available, related documents have been revised, improved ways of working are identified, etc.)

Subsequent versions must be clearly distinguishable from previous versions. Following issue of the amended version, the previous version must be clearly identified as ‘SUPERSEDED’ and/or transferred to an archive (folder or library).

A document may be withdrawn if it describes a process or aspect that is obsolete. Any applicable register should be updated and the document removed from the ‘current versions’ folder or library. Document numbers assigned to documents that are withdrawn will not be re-used.

All superseded and withdrawn documents will be retained on a BTC server or the Intranet in folders and libraries respectively, clearly marked as ‘SUPERSEDED’ or ‘WITHDRAWN’.

Notice of new, amended or withdrawn process documents may be given via the following routes:

- Disseminated to staff at relevant team meetings e.g. All Staff Meetings, or specific groups (IT, trial managers);
- Inclusion on the BTC Teams;
- Direct email to members of staff;
- Email to methodological leads for further cascading;
- Direct email to research team members (coordinating team and sites, as applicable).

Members of staff are expected to use the respective repositories to access latest versions of documents, e.g. when using a template is required.

A flowchart summarising the revision of an existing document is provided in Appendix 2.

5.1.7 Access, security, storage

The SOPs and process documents are saved on the BTC Teams under appropriately named folders/libraries. Full edit access to the SOPs is restricted to the QA manager and administrators of the system. The SOPs are accessible to all other members of staff as read only copies.

Study specific documents are saved in a secure study specific folder. Access to study specific documents is restricted to authorised members of staff.

Current versions of documents should be saved in pdf format; this format should be used when sharing current versions of controlled documents unless an editable version is required, for example to update an SOP or allow participating sites to insert local contact details on a PIL.

5.1.8 Archiving

A master file containing original copies of the SOPs and the process documents will be retained indefinitely. The master file will include all versions of each SOP, including obsolete documents.

Archiving of essential documents and other study specific documents is detailed in the BTC-SOP-TM-003 Study closedown.

5.2 Staff training and qualifications

5.2.1 General principles

The GCP guidelines states that individuals involved in conducting research should be qualified by education, training and experience to perform his or her respective tasks. The maintenance of up-to-date training records provides a means of demonstrating the adequate training and experience of staff involved in the conduct or administration of clinical research.

All members of staff must have the appropriate training for their role and undergo regular further training in order to maintain the required level of skills and knowledge to carry out their duties and comply with regulatory requirements and guidance, local policies and SOPs, and any contractual arrangements pertinent to the functioning of the BTC.

Training requirements should be in accordance with the responsibilities of each individual in his or her respective task(s).

Training may be self-directed or be conducted by means of formal training sessions, meetings or small group discussions. Targeted, modular or refresher training can be undertaken.

Education, training and experience must be appropriately documented in a way which demonstrates that members of staff are adequately trained and experienced. A Curriculum Vitae (CV) must be maintained and retained for all BTC staff.

5.2.2 Training plan

Members of staff should discuss regularly with their line managers and peers their training requirements and available opportunities for training.

Training plans are finalised and documented at least annually during the institutional-led staff review process. Clear objectives in line with the individual's personal development, the needs of the BTC and where applicable, changes to regulatory and other guidelines should be set and monitored at that time.

Training records should be reviewed regularly by line manger to ensure completeness, identify training needs and inform the training plan.

5.2.3 Training requirements

All research personnel, both permanent and temporary, must be trained in all relevant systems and procedures so that they can meet the requirements of the research. The following training should be undertaken, as appropriate:

5.2.3.1 Essential training as required by the University of Bristol

The University of Bristol has a number of essential training courses they expect each member of staff to complete based on their role in the organisation. All individuals must conform to these training requirements to ensure a safe and compliant working environment.

- All staff must complete essential training modules as per the University requirements.
- Staff with first line management responsibilities should complete staff review and development training modules.

These modules can be accessed through the University of Bristol learning and development platform for staff.

It is the duty of each individual to check at least once per year whether their training log conforms to the institutional requirements, including requirements stipulated in any honorary contracts (University or NHS).

5.2.3.2 Good Clinical Practice (GCP)

Good clinical practice is an international ethical and scientific quality standard for designing, conducting, recording, and reporting trials that involve the participation of human subjects. All members of BTC deliveringresearch must have GCP training.

There are several ways to obtain GCP training e.g. face-to-face interactive classroom training or online training. Training is available in primary and secondary care from the NIHR Learning Gateway.

GCP training should be carried out every three years for BTC staff. Staff GCP training certificates are stored centrally on the BTC Teams.

The extent and manner in which each individual is trained should be proportionate to the involvement in the research. It may be appropriate for a small section of the whole GCP training course to be tailored to a particular staff group. The line manager and/or a senior BTC member of staff will advise on the level of training required, according to role.

5.2.3.3 Other relevant training

Where ongoing professional training is a key element of the requirements to maintaining an individual's professional status, and this professional status is essential for the role performed within the BTC, the individual is required to ensure that such training is conducted.

The University of Bristol runs an integrated research training programme. Relevant training courses can be found on the University learning and development platform.

Organisations, institutions and governmental bodies involved in clinical research (regulators, funders, professional networks, etc.) provide training and guidance which can be accessed by researchers and administrators of research, e.g. National Institute for Health Research (NIHR), Health Research Authority (HRA), Medicines and Healthcare products Regulatory Agency (MHRA), Human Tissue Authority (HTA), Medical Research Council (MRC), UK Trial Managers' Network (UKTMN), etc. Links to training courses and educational material may also be provided on the BTC Teams.

On occasions the BTC may support an individual in obtaining a further education qualification that will increase his/her ability to contribute to the overall tasks within the BTC. Individuals will identify these training needs through their annual staff review and if granted, study leave may be provided, in line with BTC and institutional policies.

5.2.3.4 Study specific training

Study specific training should be tailored to the role the member of staff will have in the study, but may include training on the study protocol, investigational medicinal product, or other procedures e.g. authorising user accounts for the database, central monitoring of consent forms, collection of tissue samples, taking informed consent, CRF completion, data management other relevant training determined by the CI/PI.

5.2.3.5 SOP training

Before implementation of an SOP, information about the relevant training should be given to all personnel to whom the SOP applies, based on their role and duties. The QA manager should identify which members of staff require training, and the type of training (i.e. "read and understand" and "awareness"). A matrix shall be used to lay out the training needs of staff by their role.

Once the training is complete, each person should record it on the SOP specific training log. The BTC-WI-QM-001 Training Work Instructions contain guidance on how to log SOP specific training.

The training log should contain the following fields:

- Member of staff name
- Professional group or role
- Document name and version
- Level of training completed, as follows:
    - "read and understand" whereby the member of staff understands the content thoroughly so that they can adhere to it in their day to day roles
    - "awareness" whereby the member of staff is aware of what is included in the SOP so that content can be accessed if/when needed
- Date training completed

The training record will be stored on the QA Reporting Teams in the SOP training forms channel.

It will be the responsibility of staff to familiarise themselves with the location and adhere to the requirements of all SOPs. Staff should flag any lack of understanding of, or perceived inability to comply with, any of the SOPs to their line manager and if appropriate, the QA manager.

5.2.4 Documenting evidence of training

It is the responsibility of the member of staff to establish and maintain their Training Record. For new employees, establishing a Training Record is part of the induction process and is highlighted in the Induction pack.

The training record is an ongoing, cumulative list of all internal and external training. Information should cover formal training courses, attendance at conferences, seminars, relevant meetings and 'on-the-job' training/shadowing. Training undertaken in a previous position may be included in the training records if appropriate to the current post.

Documentation can be in the form of a training certificate, training form or sign-in sheet of a meeting/training session together with the meeting/training agenda, or an automated confirmation that a training session has been completed created on the University learning and development platform. Forms and training certificates of staff should be saved or uploaded to the University learning and development platform.

Documentation of medical or other qualification, clinical/research experience, and training of BTC staff should be in the form of CVs. The CV Template BTC-TEMP-QM-002 is available on the BTC Intranet. The CVs must be reviewed and kept up to date, and should be stored centrally on the BTC Teams. The CVs should be signed and dated, however, upload of a CV from a personal account is admissible in place of the signature.

For process documents there is no formal training record, but members of staff should ensure that they are aware of these and use them as appropriate.

5.2.5 Compliance

The QA manager may review training records as part of the audit programme, to ensure compliance with the BTC SOPs and regulatory requirements.

5.3 Risk Assessment and Quality Management Plan

5.3.1 Study Risk Assessment

Each research study adopted by the BTC undergoes an initial risk proportionate assessment.

The risk assessment process should begin as early as possible (usually as the protocol is being developed) and should be carried out on a study-by-study basis i.e. must be specific to the proposed study.

The risk assessment should take into consideration potential hazards, their likelihood and the risks they pose to participants and their safety, samples, integrity of the study data, breach of research governance regulations and/or local policies, risks to members of staff and potentially to reputation of the BTC/University of Bristol.

The risk assessment should document:

- the risk/hazards associated with undertaking the study
- mitigating strategies to minimise the probability of a hazard occurring, or its adverse consequences
- the parties responsible for implementing the mitigating actions
- timelines for implementation of the required mitigations/actions.

Relevant expertise should be sought when considering risks pertinent to certain departments or processes e.g. CI/PI, statistician, data manager, affiliated staff (pharmacy, radiology, labs, etc.).

The following considerations should be taken into account during the risk assessment; however the list is not exhaustive:

- Study phase, design, randomisation/blinding
- For CTIMPs, whether the trial is considered to be Type A, B or C in relation to the MHRA trial categories (as detailed in the MRC/DH/MHRA Joint Project Risk-adapted Approaches to the Management of Clinical Trials of Investigational Medicinal Products)
- Intervention, study procedures and outcome assessments (scans, samples etc)
- If blinded, how to maintain blinding during reporting of serious adverse events (SAEs), in Development Safety Update Reports (DSURs) and reports to the Data Monitoring and Safety Committee (DSMC) (if appropriate), out of hours cover/cover for absence
- Use of a placebo
- Management of safety events
- Participating sites
- Use of support services (e.g. Laboratories, Radiology, etc)
- Sources of bias
- Risks to data integrity and participant confidentiality
- Protocol deviations and non-compliance with GCP

The level of quality checks/monitoring required will be determined during the study risk assessment. The risk assessment is reviewed periodically at study progress meetings. The results of the risk assessment and a record of measures to be put in place, and all revisions, must also be documented.

5.3.2 Quality management plan

A quality management plan is developed, implemented and evaluated for each research project, drawn up based on the BTC initial risk assessment, and any risk assessment undertaken by the study Sponsor.

The plan specifies the QA and Quality Control (QC) procedures and related tasks specific to a study, in order to minimise the likelihood of the potential risks identified during the risk assessment and to ensure the timely detection of any issues in order to mitigate their impact. The frequency with which the quality criteria are reviewed is also specified. The following areas are considered when establishing the type of QA/QC reviews:

- Recruitment (informed consent form and process, eligibility criteria)
- Compliance, including protocol breaches (essential documents, missed visits or tests, prohibited/ concomitant medications, temperature breaches, confidentiality, study drug or device administration)
- Data accuracy, completeness and validity (Source Document Verification, accuracy checks on the case report forms (CRFs) and consistency with data entered into the database
- Safety monitoring (identification and reporting, monitoring of safety events)

Any changes to the risk assessment (through regular review or as a result of a serious non-compliance) is followed by a review of the quality management plan. Immediate review (e.g. within 5 working days) is required when a quality issue is considered serious (as determined by the protocol, or an oversight group/committee).

Any changes to the risk assessment and/or quality management plan must be documented.

The quality management plan will include a monitoring plan which should be developed at the same time.

5.3.2.1 Monitoring plan

Monitoring is defined as the act of overseeing the progress of a clinical trial, and of ensuring that it is conducted, recorded, and reported in accordance with the protocol, SOPs, GCP, and the applicable regulatory requirements.

The purpose of monitoring is to verify that:

- The rights and well-being of the participants are protected;
- The reported study data are accurate, complete and verifiable from source documents;
- The conduct of the study complies with the currently approved; protocol/amendment(s), GCP and the applicable regulatory requirements.

The monitoring plan should describe the monitoring strategy, the monitoring responsibilities of all the parties involved, the various monitoring methods to be used, and the rationale for their use if relevant. The BTC-CHK-TM-005 Central monitoring Items Checklist may be used to record how aspects of the are being/will be monitored.

The following may be considered for review:

- Informed Consent process and documentation
- Inclusion and Exclusion criteria verification
- Completed source documents and CRFs, data completeness and other types of data queries
- Study procedure and / or intervention compliance
- Sample collection and laboratory results
- IMP accountability and management (if applicable)
- Safety documentation and adverse events reporting
- Protocol deviations

Study monitoring ensures correction of deficiencies. It should be performed by members of the research team. Collaboration with other staff to get a “second set of eyes” on study aspects being monitored should be encouraged (e.g. a study coordinator of study A monitors study B).

The quality of the study data may be monitored through centralised database monitoring. The validation checks are documented in the database specification document. Data completeness and accuracy checks can be run through the study databases. Data queries are reported via the study database and may be supplemented by additional independent data checks carried out by the study statistical team.

Other study monitoring activities may also be carried out, e.g. remote site monitoring, on site monitoring. Monitoring is covered in more detail in the BTC Study Conduct SOP.

The quality management plan, risk assessment and/or the monitoring plan can be integrated into one document.

5.3.2.2 Statistical analysis plan

A statistical analysis plan is developed in order to ensure that the analyses to evaluate all planned study hypotheses are conducted in a scientifically valid manner. See BTC-SOP-ST-001 Statistics SOP.

5.4 Data Protection and Confidentiality

5.4.1 General considerations

Information collected during the research process must be recorded, handled and stored in such a way that appropriate confidentiality is maintained but access and use is allowed, as applicable, whilst satisfying the legal requirements and guidelines relating to the protection of research participant confidentiality. All information held in either manual or electronic format that identifies an individual must be processed (held, obtained, recorded, used and shared) in a secure and organised manner and in accordance with the principles of the Data Protection Act (DPA) 2018 and UK General Data Protection Regulation (UK GDPR).

All staff have a legal obligation to keep information secure and to protect confidential information from disclosure under the Common Law Duty of Confidentiality.

All BTC staff are required to undertake essential training on data protection and information security.

5.4.2 Data Protection Act and the UK General Data Protection Regulation

The processing of personal data for research purposes is governed by the UK GDPR and the DPA 2018. The basic principles of data privacy (fairness, lawfulness, transparency, data minimisation, accuracy, security, etc), and further information on the implications of the GDPR and the DPA 2018 for researchers is available on the University website (University Secretary's Office).

5.4.3 Access to personal data

Participant personal data will only be processed by BTC staff when:

- A justified purpose for doing so is clearly documented.
- REC/HRA and any other regulatory bodies approvals are in place.
- The legal basis for processing the data has been identified. Under GDPR, the legal basis for processing personal data in our research studies would usually be “in the public interest”. Consent can be used as the legal basis however the criteria for ensuring that patients are informed about what data will be used is very strict and therefore much more difficult to use.
- Protective measures have been taken to allow access to personal data only to authorised individuals; and
- Adequate Human Resources (HR) arrangements (e.g. substantive or honorary contracts, etc) are in place for individuals accessing personal data.

Access to personal data must be restricted to relevant members of staff, authorised by the Sponsor, CI, PI or host organisation.

Where BTC staff may need to have access to personal data at other sites, such as for monitoring purposes, this should be agreed in advance, usually in the site agreement or the Organisation Information Document. 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.

5.4.4 Security of personal data

Arrangements for data protection and security should be clearly described in the study protocol. The Participant Information Leaflet (PIL) and the Informed Consent Form (ICF) should contain information on: the items of personal data to be collected, including whether participants could be identified; the lawful basis for the processing of that data; how the data will be used; details of any

organisation that will collect, store and process the data; details of any data transfers; and the intended duration of data retention.

Files containing direct identifiers should be kept in a secure location, separated from other study data with access only to individuals who strictly need to see it for the purposes of conducting the study. If handling electronic files with direct identifiers such as names and addresses, the following should also be observed:

- Files should be password protected and/or encrypted and stored on a secure network or only available in a secure space such as on the N3 network (not directly onto a computer's hard drive) and security of the data protected.
- Workstations should be locked/users logged out if the user is leaving the computer unattended.
- Files containing direct identifiers should not be transferred via e-mail or by other means, except with the explicit consent of the participants (e.g. letters to their GP); University email and personal account email accounts should never be used.
- Files containing identifiers can only be sent between NHS secure accounts (e.g.nhs.net to nhs.net, Office 365 applications) or other means which are secure for the transmission of confidential patient information.

Participants' identifiable data must not be stored on home computers, personal laptops, unencrypted memory sticks, CDs, hand held devices, audio-recorders, digital cameras or other imaging equipment even if they are password protected. An encrypted memory stick may be used if required.

NB: Where working from home, accessing the University systems from a personally owned computer/device is acceptable as this is simply accessing the University network remotely and no data should be retained on the computer/device. When using the Staff Desktop, it is important to ensure that no data is copied or saved to any end user computer/device. This also applies when accessing the University's virtual private network, which provides secure access to University network resources from offsite.

Data where records are identified by a code are only identifiable if the means to "unlock" that code are also accessible.

Documents which include personal data should not be sent to any private (i.e. non-work) email addresses unless the information only concerns the recipient.

All IT systems and/or third-party organisations used to store, process or transmit any research data must be compliant with the applicable SOPs, policies and IT security requirements.

All personal data transfers including paper and electronic should be approved by the Sponsor or delegate e.g. CI, and must be documented. Where passwords are used and are required by the recipient to access the data, they should be communicated separately from the password-protected data, preferably by phone.

5.4.5 Keeping data

The guidance from the Information Commissioner's Office (ICO) (who regulate GDPR in the UK) states: "You can keep personal data indefinitely if you are holding it only for:

- archiving purposes in the public interest;
- scientific or historical research purposes; or
- statistical purposes."

Where it is not possible to completely anonymise data (e.g. source data verification is required), data must be 'pseudo-anonymised' as soon as possible. When data are pseudo-anonymised, one master list with the identifier/ codes and the participants' details must be kept separately in a locked cabinet/office/password protected file); no copies of this list should be made.

Research personal data must be archived appropriately in line with BTC-SOP-TM-003 Closedown and in accordance with the relevant REC/HRA approvals and any other relevant legislation.

For the long-term archiving of research data please also seek guidance from the Information Governance Team in the University Secretary's Office (data-protection@bristol.ac.uk), the Research Data Storage Facility (rdsf-help@bristol.ac.uk) or Special Collections (special-collections@bristol.ac.uk). Relevant information on long-term archiving and data sharing is provided in the BTC-SOP-TM-003 Closedown and BTC-WI-TM-005 Data Sharing Guidance document.

5.4.6 Personal data breaches

A personal data breach is defined 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."

Examples of personal data breaches include:

- Human error, for example an email attachment containing personal data being sent to the incorrect recipient or records being deleted accidentally
- Sharing of passwords or other credentials with third parties
- Documents containing personal data being left unattended to be copied, read or photographed by an unauthorised person
- Unlawful interception of email or telephone communications or online form submissions
- Loss or theft of a physical file or electronic device containing personal data
- Loss of a decryption key relating to securely encrypted personal data
- Damage caused by unforeseen circumstances such as fire or flood
- Opening or clicking a link within a malicious email which contains malware or viruses, a ransomware attack whereby access to systems or records containing personal data is disabled or encrypted or a cybersecurity attack whereby personal data are accessed, altered, deleted and/or disclosed by the attacker

All personal data breaches identified by staff including breaches pertinent to data held on NHS systems should be reported as a matter of urgency, and within 24 hours of becoming aware of the incident as follows:

- Speak to your line manager OR
- Contact the relevant Data Protection Officer (DPO).
- If the above options are not possible, and outside of normal business hours, breaches can be reported to the IT Service Desk (service-desk@bristol.ac.uk), which provides a 24/7 service.

Under the UK GDPR the University is required to report to the ICO any personal data breach that poses a risk to the rights and freedoms of individuals, within 72 hours of becoming aware of the breach. It also requires the University to notify the individuals affected in those cases where the breach is considered to pose a high risk to their rights and freedoms. Failure to comply with these requirements may result in the University being fined.

Further guidance on how to recognise a personal data breach and what to do in the event of a personal data breach or suspected personal data breach is available on the University Secretary's Office webpage.

The BTC will work with the CI, study team and/or the DPO to investigate, document and, where appropriate, report personal data breaches to relevant parties, such as sponsor, funders, insurers, REC, etc. Further details on non-compliance are provided in the section below and in the BTC-SOP-TM-002 Study Conduct.

5.5 Managing non-compliance

5.5.1 General considerations

All members of staff have a duty to the public, to themselves, to the University of Bristol, to other organisations where they hold an honorary contract (e.g. NHS Trust) and to funders to conduct research in a conscientious and responsible manner, and in accordance with the applicable SOPs, protocol, GCP and legal requirements, and any local policies.

Minor non-compliance is a departure from one or more of the protocol, SOP, GCP or regulatory requirements that have been identified retrospectively, which is neither critical or major and so not likely to effect to a significant degree the safety or physical or mental integrity of the research participant, or the scientific value of the research study.

Major non-compliance is a significant and unjustified departure from the protocol, SOP, GCP or regulatory requirements that may not have developed into a critical issue but may have the potential to do so unless addressed. Where there are a number of instances of minor non-compliance within a single area of responsibility, this indicates a systematic quality assurance failure and so should be collectively treated as major non-compliance.

5.5.2 Non-Compliance with Standard Operating Procedures

Compliance with the BTC SOPs is compulsory.

Non-compliance may come to light during the day-to-day running of a study or retrospectively when SOPs are being reviewed, during training, during internal audits or through other means. Members of staff are responsible for acting on information or reports of non-compliance received from any source.

When a non-compliance is apparent the QA manager or delegate is responsible for an initial review which may include verification from other sources, contacting individual/team directly to discuss their working practices etc.

A further review may be undertaken by the QA manager where a serious or continuing non-compliance is apparent. If confirmed, the QA manager should determine the relevant corrective actions.

The QA manager may determine that no further action is required (e.g. no or insufficient evidence of non-compliance) or that further training (at individual or group level) is required.

The QA manager will ensure that any corrective actions and any identified training are completed in a timely manner.

A log of non-compliances should be kept.

5.5.2.1 Exemptions

An exemption is required if it is identified prospectively that for exceptional reasons a BTC SOP cannot be followed in part or in its entirety (e.g. when implementation of a new SOP is impractical for the circumstances of a specific study). The individual/team needing the exemption should

identify the requirement as early as possible and discuss the situation with a QA manager. A suitable alternative process should be agreed with the QA manager and appropriate member of the senior BTC staff in place of the process outlined in the SOP. This should be documented.

5.5.3 Protocol / GCP Non-Compliance and Serious Breaches

The processes for assessing non-compliances of GCP or to the study protocol, identifying suspected serious breaches, notifying the REC and/or the MHRA and implementing the required follow-up actions are described in the BTC-SOP-TM-002 Study Conduct.

5.6 Audit

The quality management system within the BTC shall be subject to quality checks and internal audit to ensure that it is fit for purpose, and that the research studies adopted by the BTC are conducted and managed safely and effectively and in compliance with the protocols and the applicable SOPs and regulatory requirements.

5.6.1 Audit programme

An audit programme will be proposed annually by the QA manager or delegate and will be approved by the BTC Operations Group. The QA manager will review the programme periodically to determine whether changes are necessary. Any proposed changes will be approved by the Operations Group.

The audit programme may require updating as risks and priorities may change, such as:

- A Serious breach of GCP has been identified;
- Critical or Major findings identified during an MHRA Inspection;
- Findings from another audit highlight a potentially significant issue, or actions from a previous audit are not complete;
- Concerns regarding research practice are raised.

The extent, type and frequency of the planned internal audits shall vary, depending on the risks identified for the BTC research activity at the time e.g. adoption of studies in new areas (disease, population, methodology, etc.), implementation of new technologies or systems, etc.

The length and detail of each audit will depend on the complexity and regulatory requirements of the research studies. Where studies are considered to have higher risk factors (e.g. using novel interventions, working with vulnerable populations, inexperienced study team, international sites, complex study), they are more likely to be included in the programme.

In addition to audit activities, other quality checks can be used to assure the quality of work undertaken, identify and address gaps in processes, e.g. checklists to be completed as processes are followed (study set up, closedown, etc). These should also be included in the audit programme.

5.6.1.1 Scheduled audits

Centre-level scheduled audits can be, but are not restricted to:

- System audits - looking at the functionality of complete systems e.g. pharmacovigilance, data management;

- Process audits – looking at performance of specific processes within systems e.g. expectedness assessments, data query processes, documentation practices (e.g. review of study-specific or system documentation).

Research teams may, on occasion, request an audit of their study, and where deemed appropriate by the QA manager these will be added to the audit programme.

An audit reference number shall be issued and the QA manager shall maintain an audit schedule documenting the type and frequency of audits. A decision on how many systems/processes to audit versus studies should take into consideration the new systems/processes, the BTC portfolio of studies in addition to the CTU resources available for conducting audits.

5.6.1.2 Unscheduled or ‘ triggered’ audits

When the QA manager is made aware of any concerns (non-compliance or other triggers), an audit may be initiated. Possible causes include (but are not restricted to):

- Notification of safety concerns;
- Notification of non-compliance (e.g. with protocol or SOPs);
- Submission of a potential serious breach.

Planning for this type of audits will be different to those for scheduled audits as they cannot be allocated in advance and may therefore affect other planned audit activities.

5.6.2 Audit process

5.6.2.1 Audit plan

An individual audit plan should be prepared by the QA manager..

The following should be documented in the audit plan:

- Purpose/background and Scope of the audit;
- Objectives of the audit
- Audit criteria and reference documents
- Audit methodology
- Audit location and personnel involved.

5.6.2.2 Document review

The QA manager or delegate shall review applicable regulations, standards, SOPs, policies, procedures and protocol specific requirements as well as account for any previous audit findings and non-compliances (e.g. MHRA inspection findings).

5.6.2.3 Audit documentation

Audit templates/checklists may be used if appropriate checklists already exist, or may be specifically prepared by the QA manager or delegate. Consideration shall be given to previous or systematic findings, and these may be included in the scope of the audit.

5.6.2.4 Audit notification

Prior to the audit being undertaken, the QA manager or delegate shall contact the teams/individuals concerned (auditees) to notify them of the intention to audit and agree an appropriate timescale for the audit.

NB: The QA manager or delegate may perform unannounced audits if this is deemed appropriate, e.g. triggered audits.

5.6.2.5 Undertake audit

The audit is performed in accordance with the audit plan. The scope of the audit shall be discussed with all those concerned. The sources of information for gathering evidence can vary according to objectives, scope and complexity of the audit. Sources of information may include, but are not limited to, the following:

- Discussions with BTC staff and other persons/members of the study team;
- Observations of activities;
- Documentation, i.e. policies, SOPs, contracts with third parties, etc.;
- All 'essential documents' (as described by ICH GCP and other applicable regulations) associated with a study;
- Computerised databases, analyses and reports.

Only information relevant to the objectives, scope and criteria of the audit should be collected.

During an audit it may be necessary to deviate from the audit plan if an area of concern, outside the scope of the audit, is identified. Any deviation from the audit plan should be recorded in the audit report.

5.6.3 Audit findings and recommendations

Any findings identified during the audit shall be discussed with auditee(s) as part of the audit process. If appropriate, Corrective Actions and Preventive Action (CAPA) shall be discussed and agreed.

Findings shall be reported as non-compliances if they do not comply with the principles of GCP, the study protocol, BTC SOPs or study specific instructions.

A non-compliance that affects (or has the potential to affect) the rights, wellbeing or safety of participants, or affects (or has the potential to affect) the scientific integrity of a clinical trial shall be treated as a serious breach requiring immediate attention. Such findings shall be dealt with as per the BTC-SOP-TM-002 Study Conduct.

Significant findings and any trends from findings shall inform further development of quality management systems and the audit programme. These should also be included in periodic reports to the Operations Group by the QA manager.

5.6.3.1 Audit report

An audit summary report shall be issued to the auditee (and any other interested parties) within an agreed timescale.

The report shall include the following:

- Audit reference number, title and date of the audit
- Audit type
- Lead auditor (QA manager and/or delegate)
- Scheduled and actual start date, end date and duration
- Status ('performed' or 'closed')
- Date reported
- All findings of non-compliance with the standards listed in the audit plan. If there are no findings raised this shall be indicated.

- The report will also detail any observations and recommendations which will be in an advisory capacity to support best research practice and prevent non-compliance(s) in the future

Auditees are required to respond within an agreed timescale, highlighting any concern or queries they may have, and proposed CAPA (see section below).

Follow-up discussions can take place to clarify any issues and review progress.

The QA manager or delegate shall confirm with the auditee once all non-compliances, and the audit, are closed, by email. The audit report can be finalised and distributed to the agreed relevant staff or groups (e.g. the auditee(s) and the relevant team, and the QAG).

5.6.3.2 CAPAs

The auditee(s) will propose CAPAs to address each finding. It is recommended that these are discussed with the relevant parties (e.g. CI, trial manager, statistician, etc, depending on the nature of the audit and expertise of staff in that area), who will review the proposed CAPA and advise whether they are considered to be sufficient to address the audit finding.

The CAPA plan will be sent to the QA manager or delegate within the given timeframe.

The QA manager will confirm whether the CAPAs are adequate. If any CAPAs are considered inadequate, the QA manager will liaise with the auditee(s) until CAPAs are agreed.

Once CAPAs have been agreed, the auditee(s) is (are) responsible for completing all CAPAs. Failure to complete CAPA within agreed timescales shall result in further referral to the QA manager and is itself regarded as a non-compliance.

Once all CAPAs have been completed, the audit will be considered closed and the QA manager or delegate will issue the final report.

If it is not possible to reach an agreement regarding the appropriate CAPAs or there is a delay in implementing the actions agreed, the issue may be escalated (see below).

5.6.3.3 Audit escalation

The QA manager or delegate liaises with auditee(s) to resolve any issues. If the assurance level is not agreed upon, the report will be referred to the most relevant senior member of staff. Once the auditee accepts the findings

The QA manager may escalate issues to the BTC Director or research Sponsor if the findings are serious, if suitable CAPAs are not proposed to address the findings, if insufficient action is taken to address findings, or if the auditee/study team fail to engage with the audit in a timely manner.

5.6.3.4 Documentation

The auditee(s) must ensure that confirmation that the audit is closed and a copy of the audit final report are filed alongside all the documentation that was audited, as evidence that an audit took place.

The QM manager is responsible for ensuring that all documentation associated with the audit (including the audit plan, relevant notes, the report, CAPA plan, and associated correspondence) are retained by the BTC. The audit report (and its contents) should be treated confidentially and should not be shared outside of BTC.

6. SUPPORTING DOCUMENTS TO BE USED

Number	Title
BTC-RES-TM-001	Definitions, Acronyms and Abbreviations Relevant to Research Projects and Management of Research
BTC-WI-TM-005	Data Sharing Guidance
BTC-SOP-QM-001	Development and Management of Standard Operating Procedures SOP
BTC-SOP-TM-001	Study Start Up SOP
BTC-SOP-TM-002	Study Conduct SOP
BTC-SOP-TM-003	Study Closedown SOP
BTC-SOP-ST-001	Statistics SOP
BTC-WI-QM-001	BTC SOPs Training Work Instructions
BTC-TEMP-QM-002	CV Template
BTC-CHK-TM-005	Quality Management Plan

7. CHANGE HISTORY

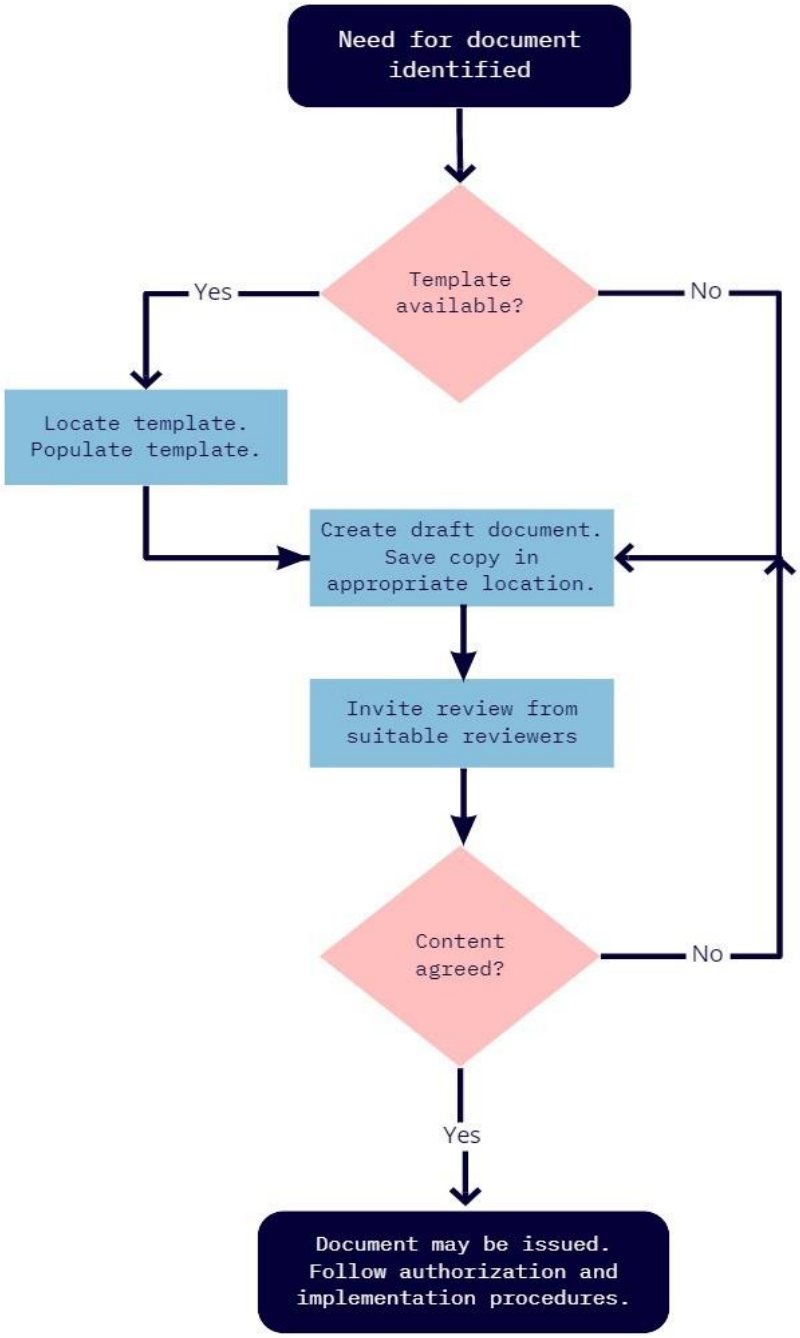
Previous version and date	New version and date	Summary of review
NIL	V1, 19 Jul 2021	New document
V1, 19 Jul 2021	V2, 9 Feb 2022	Clarification that a record should be kept of applicable SOPs for each study, for the duration of that study Clarification that CVs must be maintained and retained for all BTC staff Requirement to store centrally CVs and GCP training certificates for BTC staff on the BTC Intranet; reference to the CV template; clarification that where CVs are uploaded onto the BTC Intranet from a personal account a signature in the CV is not required Clarification that other secure means may be used for transmission of confidential information, in addition to nhs.net to nhs.net

		Clarification that a log of non-compliances should be kept centrally
V2, 9 Feb 2022	V3, 26/02/2024	Reference to the BTC Sharepoint was removed and replaced with BTC Teams site as relevant. Reference to the Quality Assurance Group and BTC working groups was removed as these groups no longer exist in the new BTC structure. Reference to the BTC-CHK-TM-005 Central monitoring Items Checklist and BTC-WI-TM-005 Data Sharing Guidance document added.

8. APPENDICES

8.1 Appendix 1

Preparing a new document



8.2 Appendix 2

Revising a document