swiss
clinical
trial
organisation

Appendix 2

DATA MANAGEMENT GUIDELINES

→ under revision

Version

2.0

INTRODUCTION

The CTU network developed in 2009 the "Guidelines for Good Operational Practice" (GGOP) in collaboration with the partner organisation Swiss Group for Clinical Cancer Research (SAKK) under the lead of the SCTO. They were written to prepare the ground for the standardised state-of-the-art management of clinical research within the CTU network in line with national and international legal and regulatory requirements. Similarly, Guidelines for Data Management for the CTU network were established in 2012 and were now integrated into the GGOP during the major revision in response to the implementation of the Human Research Act (HRA)[1] in 2014.

Data Management (DM) is an integral part of clinical research management, which keeps gaining in importance and complexity as the use of IT systems is increasing in all processes. Moreover, data management is an extremely fast-changing field. Consequently, common guidelines are essential for harmonised data management processes within the CTU network, especially in view of the conduct of multicentre projects that run on a national and international level. Therefore the specific requirements for data management of the CTU network were established.

There are only few specific regulatory requirements regarding data management in clinical research apart from ICH GCP. These are detailed in the relevant ordinances to the HRA, the ClinO Art. 18 and HRO Art. 5[2]. In all activities, the utmost priority should be given to the ICH GCP principles, which require that "all clinical trial information should be recorded, handled, and stored in a way that allows its accurate reporting, interpretation and verification" [ICH GCP 2.10] and that "confidentiality of records that could identify persons should be protected, respecting the privacy and confidentiality rules in accordance with the applicable regulatory requirement(s)" [ICH GCP 2.11].

In September 2011, the European Clinical Research Infrastructures Network (ECRIN) published the "Requirements for Certification of ECRIN Data Centres"[3] (referred to as ECRIN requirements below), which were revised in July 2012 and published in April 2013[4]. The revised standard requirements now also contain extended explanations and examples ("Explanation and Elaboration of Standards"). The ECRIN requirements take into account the legal and regulatory requirements as well as the internationally acknowledged standards (e.g. ISO 27001[5]) and guidelines (e.g. Good Clinical Data Management Practices, GCDMP[6]). They provide an open and widely used set of requirements for GCP-compliant data management, particularly in academic trial units. The ECRIN requirements, established by an international group of experts, describe the systems and functionality that a trial unit needs in order to become certified as an "ECRIN Data Centre"; amongst other things, a trial unit has to meet a series of standards – some dealing mainly with the IT systems, others focused on data management practices, but all indicative of high quality data processing.

The ECRIN requirements draw up a clear road map for the development of a GCP-compliant data management policy that can be adopted by all ECRIN member states. Data centres belonging to the ECRIN "Scientific Partners", which since January 2012 also include Switzerland, are strongly advised to follow the guidelines issued by the European network.

Consequently, the CTU network has decided to adopt the ECRIN requirements as their standard for good data management practice and established the Data Management Guidelines of the CTU network, closely following the ECRIN Guidelines.

As with the overall GGOP, it is the decision of each CTU to adopt the following Data Management Guidelines of the CTU network or not, depending on the specific needs of the individual organisation. The organisational environment of the superordinate organisations, e.g. (university) hospitals, the particular objectives, the size and the organisational structure of the individual CTU as well as its financial and human resources, respectively, may have a considerable impact on these needs. Besides, implementation may also be influenced by the type of research projects conducted and the type of project-related activities offered by the individual CTU or organisation.

1 Humanforschungsgesetz (HFG) / Loi relative à la recherche sur l'être humain (LRH) (www.admin.ch/opc/en/classified-compilation/20061313/index.html)

2 Ordinance on Clinical Trials in Human Research (Clinical Trials Ordinance, ClinO; www.admin.ch/opc/en/classified-compilation/20121176/index.html) and the Ordinance on Human Research with the Exception of Clinical Trials (Human Research Ordinance, HRO; www.admin.ch/ch/e/rs/810_301/index.html)

3 Standard requirements for GCP-compliant data management in multinational clinical trials, Trials, 2011; 12:85; doi:10.1186/1745-6215-12-85, www.trialsjournal.com/content/pdf/1745-6215-12-85.pdf, including additional file: www.trialsjournal.com/content/supplementary/1745-6215- 12-85-s1.pdf

4 Ohmann et al. Revising the ECRIN standard requirements for information technology and data management in clinical trials, Trials, 2013; 14:97; doi:10.1186/1745-6215-14-97, www.trialsjournal.com/content/pdf/1745-6215-14-97.pdf

5 ISO 27001 Information Security Management – Specification With Guidance for Use

6 Good Clinical Data Management Practices, Society for Clinical Data Management, July 2009

OBJECTIVES

The Data Management Guidelines of the CTU network give guidance for clear and concise GCP-compliant data management processes in clinical research management in the CTU network. They are in line with both the general GGOP and the ECRIN requirements.

STRUCTURE

Similarly to the general GGOP, the Data Management Guidelines of the CTU network are divided into two parts:

Part I specifies the standards relating to the IT infrastructure.

Part II describes the standards concerning data management applications in clinical research projects.

For the requirements regarding general infrastructure, e.g. human and financial resources, etc., as well as regarding other processes involved in research projects, please refer to the general part of the GGOP.

The Data Management Guidelines of the CTU network consist of six main chapters, which are closely interrelated. The standards described in these chapters correspond to the ECRIN requirements, which are referenced in the headers (in square brackets).

Each chapter lists requirements which are deemed necessary for the good data management practice of a CTU. The standards are divided into detailed criteria, listed as bullet-points. By following the instructions given in the bullet-points, CTUs can meet the standards. Each bullet-point corresponds to one of the requirements described in the ECRIN document mentioned above.

Definitions for the most important specific Data Management terms can be found in Appendix 1: Glossary. They are linked and underlined in green in this document when used for the first time.

Whenever the masculine gender is used, both men and women are included, unless otherwise stated.

PART I: IT Infrastructure

Part I describes the standards for the management of IT infrastructure, its security, backup and validation processes, as well as software development, data extraction and reporting. The following standards complement the GGOP Chapters 3 Management of Resources: Infrastructure and Working Environment, 6 Management of Resources: Purchasing and Suppliers and 7 Change Management. They correspond to the chapters concerning the standards for IT infrastructure as stipulated in the ECRIN requirements.

1 MANAGEMENT OF IT INFRASTRUCTURE

The introductory paragraph of the general GGOP Part II Management of Clinical Research is particularly relevant for the underlying Part I. A majority or all of the processes regarding the IT infrastructure are usually outsourced by CTUs. Hardware procurement, for instance, very often depends on the policies of the superordinate institutions. Therefore, the specific requirements for IT infrastructure are not listed in this document. Should an organisation need to prove compliance with requirements issued by ECRIN, the detailed specifications can be found in the current version (V2.2) of the ECRIN requirements.

1.1 Management of Servers [IT01]

CTUs should ensure that server specifications and processes for support, maintenance and retirement of servers are defined in line with the management of resources (see GGOP Chapter 3 Management of Resources: Infrastructure and Working Environment).

1.2 Physical Security [IT02]

CTUs should make sure that servers are installed in a physically secure facility (e.g. a locked room with limited access), and that procedures for disaster prevention are in place (e.g. secured power supply, fire alarm, etc.).

1.3 Logical Security [IT03]

CTUs should ensure commitment to and compliance with the Swiss legislation (Federal Act on Data Protection (FADP) and the Human Research Act (HRA)) and maintain a security system for electronic data handling that prevents unauthorised access to the data [ICH GCP 5.5.3 (d); ClinO Art. 18 (1) lit. b; HRO Art. 5 (1) lit. b].

1.4 Access Control [IT04]

CTUs should ensure that privacy and confidentiality regulations are enforced, both at the level of the initial access to the network and at the level of the specific access to documents and databases required within applications, by implementing the corresponding documented procedures [ICH GCP 5.5.3 lit. b, ClinO Art. 18 (1), HRO Art. 5 (1)].

1.5 Risk Management Plan [IT05]

As part of its Risk Management Plan (see GGOP Chapter 2.7 Risk Management), the CTU should have a policy for maintaining adequate backup of data [ICH GCP 5.5.3 lit. f] covering likely action in the event of a major loss of server function (e.g. by fire, long term power failure, full server failure) or sudden loss of key staff.

1.6 General System Validation [IT06]

If the CTU provides the electronic data processing system(s), the CTU should be able to ensure and document that the provided systems conform to the customer's established requirements and that appropriate documented validation processes exist and are being followed [ICH GCP 5.5.3 lit. a].

Note: Specific validation of systems that are applied to/ used by particular clinical research projects is covered in Chapter 3.2 Clinical Data Management Applications – Validation.

1.7 Local Software Development [IT07]

Local software development should be complemented by appropriate system documentation and documentation to support the tracing of programme execution and be supported by quality assurance measures.

1.8 Extracting and Reporting Data [IT08]

Any extracting and reporting of data should be planned (e.g. in a Statistical Analysis Plan, SAP) and validated.

PART II: Data Management in Clinical Research

The following Part II describes the requirements for the data management activities in clinical research. On no account should they be perceived in isolation from all other activities in clinical research, as they are presented in the GGOP chapters. Clinical research projects are complex, multifunctional projects. Depending on the set-up of the cross-functional project teams, some activities described herein may be performed by other members of the team and vice versa.

This Part II follows the structure of the general GGOP, listing the main standards for data management activities in clinical research throughout the course of a project. The standards are structured according to the phases of clinical research (as defined in the GGOP, Figure 2), and cross-referenced with the relevant chapters of the GGOP. These standards – listed below as bulletpoints – correspond to the ECRIN requirements specified in its "Data Management Standards" and "General Standards" sections.

It is important to note that depending on the nature and extent of clinical research, activities may be performed in a different order and therefore take place in different phases of the project.

2 CONCEPT PHASE

The concept phase begins with the submission of the clinical research by the potential customer (e.g. sponsor, investigator) to the CTU and ends with the validation of the project (e.g. contract, service level agreement).

If the project includes data management services, the respective specialist(s) should be included in the project assessment (see also GGOP Chapter 10.1.2 Project Assessment).

3 DEVELOPMENT PHASE

The development phase begins after signing the contract/service level agreement with the customer and ends on the date of obtaining the ethical and regulatory approvals or authorisation for the clinical research.

If per contract/service level agreement the data management will be performed by the CTU, the data manager(s) should be included in the project team from an early stage onwards and receive full information about the clinical research details (see GGOP Chapters 11.1 Project Management and 11.4 Data Management). The CTU should ensure that the requirements stipulated in ICH GCP are fulfilled [ICH GCP 5.5.3; ClinO Art. 18 (1)]. Preferably, an overall Data Management Plan (DMP)[7] should be established in agreement with the investigator and the customer, or data handling should be planned as defined in the protocol [ICH GCP 6.13].

3.1 Clinical Data Management Applications – Design and Development [DM01]

For the design and development of Clinical Data Management Applications (CDMAs) and Case Report Forms (CRFs), the main focus should be on the accurate and correct data collection according to the protocol. For general requirements on CRFs see also GGOP Chapter 11.5 Case Report Forms. Attention should be paid to the following points:

- Documented procedures covering the development of CDMAs and CRFs should be in place [ICH GCP 5.5.3 lit. b].
- CDMA and CRF development should be performed by a cross-disciplinary team of qualified individuals (e.g. investigator, study manager, statistician, data manager, programmer) [ICH GCP 5.4.1].
- The specification for CRFs should be driven by the protocol (e.g. primary safety and efficacy variables).
- CRF development should be compliant with the documented procedures at the CTU and include version control.

7 Good Clinical Data Management Practices, Society for Clinical Data Management, July 2009

- CRF design and functional specifications should exist, identifying each data item on each CRF (including field names, types, units, validation logic, and conditional skipping).
- CRF design and functional specifications should be signed off and dated by the relevant signatories.
- CDMAs in development should be isolated from CDMAs used productively.
- Access to the CDMA for training purposes should be managed to ensure that it is isolated from live clinical data.
- For clinical research projects/sites using electronic Case Report Forms (eCRFs), procedures should be in place to generate accurate interim CRFs for sites when and if necessary.

3.2 Clinical Data Management Applications – Validation [DM02]

According to ICH GCP [5.5.3 lit. a], it should be ensured and documented that electronic data processing systems conform to the customer's established requirements. In addition, appropriate documented validation processes should exist.

- Documented procedures for CDMA validation should be in place.
- A project-specific test plan and a test documentation set for each CDMA should exist.
- Testing with sample data against functional specifications should be carried out for each CDMA before deployment to a live environment.
- Users should be involved in assessing CRFs for user-friendliness.
- Each CDMA should be formally approved, dated and signed by the relevant responsible person, before production use.
- For each CDMA all validation results, including any test data and protocols, should be archived.

4 PROJECT SET-UP PHASE

The set-up phase begins on the date of obtaining the ethical and regulatory approvals/authorisation and ends when the sponsor opens the clinical research project for accrual.

4.1 Site Management, Training & Support [GE02]

If agreed with the customer, the CTU should ensure that the clinical research project site(s) receive the necessary training and support for GCP-compliant data collection prior to the start of the project (see also GGOP Chapter 12.5 Site Initiation Visit).

- Documented procedures should be in place for opening sites for data collection and supporting research staff in terms of data management.
- User training with data entry instructions or guidelines for paper CRFs and/or eCRFs should be provided to investigators, site staff and monitors, if applicable.
- It should be clearly and consistently indicated on the screen if users are working on a test/training eCRF.
- A site should only be given access to a production CDMA once the sponsor (or his representative) has confirmed in writing that all relevant preparations have been completed and that all permissions and agreements have been obtained.
- Individuals should have access to production data only when they have been trained with the Clinical Data Management System (CDMS) and the specific CDMA.
- Processes should exist to update and redistribute site documentation when this is required as part of change management.
- Processes should exist to assure that up-to-date information about project duties, including the permission to enter data and/or sign off CRFs, is available to data centre staff.
- Help desk support and/or web-based support (details as agreed with customers) should be provided for rapid response to site requests, if applicable.
- For multicentre projects help desk/web support should be provided in the data centres' local language(s), if applicable. In the case of international clinical research projects, English instructions and/or support should also be available.

4.2 Treatment (Intervention) Allocation [GE03]

If agreed with the customer, the CTU should ensure the set-up and management of treatment (or intervention) allocation according to the protocol, including blinding and unblinding, if applicable. For general requirements see GGOP Chapter 11.11 Definition of Randomisation Process. The following requirements should be met in case of IT-based treatment (intervention) allocation:

- Documented procedures should be in place for the set-up and management of treatment (intervention) allocation.
- Documented procedures should exist covering the safeguarding of the blinding (if applicable) [ICH GCP 5.5.3 lit. g].
- Documented procedures should be in place to support the rapid and safe unblinding of blinded treatments (intervention), if required.
- The underlying algorithms and operations of all systems for allocating participants to treatments (interventions) should be clearly documented and validated.
- Details of the treatment (intervention) allocation specification for any specific project should be documented and recorded.
- Any problems or errors that arise in the treatment (intervention) allocation process should be tracked and the subsequent actions recorded.
- Staff handling allocation requests should be adequately trained on the randomisation process for every clinical research project they are involved in.
- Records should be kept of any allocation material generated and any allocation decisions made.
- (A) system(s) to deal with a loss of IT-based treatment (intervention) allocation (failover to manual) should be in place, if applicable. Staff should be trained on the handling of these systems.

5 CONDUCT PHASE

The conduct phase begins with participant recruitment and ends on the date of the database lock.

5.1 Receiving and Uploading Bulk Data [GE05]

Depending on the agreements with the customer, the CTU may receive and upload bulk data (bulk data transfer), e.g. from laboratories and collaborators. In this case, the following aspects should be respected, whether the data transfer is performed manually, machine or system generated.

- Documented procedures dealing with the receipt and upload of bulk data should be in place.
- Once received, the original files should be saved and retained as read-only files and be available as reference data sets for audit/reconstruction purposes.
- If imported data has to be pre-processed before upload to the CDMS, copies of the eventually uploaded data should be kept as read-only files.
- Each receipt and upload process should be documented and tracked.
- Documented procedures should be in place for agreeing on, specifying and documenting the format of the received data.
- Documented procedures should exist to deal with requests for direct changes of data in the database.
- Any direct amendments made should be tracked and the details documented, including the justification for the change.

5.2 Clinical Data Management Applications – Change Management [DM03]

The CTU shall ensure that any changes implemented during the course of a clinical research project are documented and reported. For general requirements regarding change management see also GGOP Chapter 13.7 Change Control Process.

- Documented procedures for CDMA change management should be in place.
- Individual requests for changes to CDMAs should be justified, itemised and documented.
- A risk analysis should be conducted and recorded when considering any change.
- Any change should be tested in the development/test environment and the test results should be recorded.
- Communication channels should be in place to inform relevant staff and users of changes and to provide support and explanatory material as required.
- Processes should exist to ensure on-going consistency between the CDMA and the associated project protocol.

5.3 Data Entry and Processing [DM04]

If data entry and processing are taken over by the CTU, the CTU should ensure that all clinical research information is recorded, handled, and stored in a way that allows its accurate reporting, interpretation and verification [ICH GCP 2.10]. If data are transformed during processing, it should always be possible to compare the original data and observations with the processed data [ICH GCP 5.5.4].

- Documented procedures for data entry and corrections should be in place.
- Access control should be fully implemented; data entry/review should only be accessible to authorised personnel and as needed.
- Site staff should only have access to their own data.
- Mechanisms should be in place to identify and report on missing or late CRF/eCRF and safety data.
- A receipt tracking system should be in place for CRFs.
- Processes should exist to allow the blinding of inappropriate patient-identifying information before it is submitted to the CTU.
- Simple checks on individual values (e.g. range checks) should be available and used where appropriate.
- Complex checks on multiple variables (e.g. for logical consistency across forms) should be available and used where appropriate.
- Clear guidelines and procedures should exist to identify and carry out self-evident corrections.
- All actions performed in the CDMA (insertions, updates, deletions) should have an audit trail, covering the date and time of the input, the person making the change and the old as well as the new values [ICH GCP 4.9.3].
- Sites using electronic Remote Data Capture (eRDC) should not be able to change the CDMS's time stamp.

5.4 Data Quality Checks [DM05]

Quality control should be applied to each stage of data handling to ensure that all data are reliable and have been processed correctly [ICH GCP 5.1.3]. For general requirements see also GGOP Chapter 13.2.3 Data Handling and Query Management.

- Documented procedures should be in place regarding data quality and the checks required to ensure it.
- Validation checks may be executed via a batch process to identify missing, illogical and inconsistent data. These checks should be used where appropriate and as defined in the Data Management Plan.
- Validated reports should be available in a format that supports the manual review of data (e.g. for consistency checking, medical review).
- Documented procedures for supporting Source Data Verification (SDV) should be in place. As a minimum, data access should be provided to the persons performing SDV (e.g. monitors).
- All data checking exercises should be documented and analysed, and any emerging issues reported to the appropriate person(s) for resolution.

5.5 Query Management [DM06]

For general requirements regarding query management see GGOP Chapter 13.2.3 Data Handling and Query Management. For electronic data handling the following aspects should be taken into consideration:

- Documented procedures should be available covering the query format and generation, data change and query resolution.
- Queries should be created – automatically and/or manually – based on documented staff roles, procedures and predetermined logical checks.
- Queries should be created in accordance with documented procedures from batch checking of data, as necessary.
- Responses should be recorded when returned, identified when outstanding and queries resent, if necessary.
- Query resolution is tracked, and appropriate actions taken and documented.

5.6 Delivery and Coding of Data for Analysis [DM07]

If the CTU is responsible for data delivery and coding, it should make sure that the processes concerned are in accordance with contracts/SLA (see also Chapter 6.1 Transferring Data).

- Interim analyses and database lock should be performed as foreseen by the protocol or earlier, if required by an independent data monitoring board (see also GGOP Chapters 13.7.6 Interim Analyses and 13.8 Clinical Research End).
- Documented procedures should be in place dealing with taking a snapshot of the research project data, and/or "locking" and "unlocking" that data.
- All relevant data (or all except for a pre-defined/pre-agreed fraction) should be received prior to data extraction for analysis.

- All queries (or all except for a pre-defined/pre-agreed fraction) should be resolved prior to data extraction for analysis.
- All external data (e.g. safety database, lab data) should be reconciled prior to data extraction for analysis (or all except for a pre-defined/pre-agreed fraction).
- Documented procedures should be in place detailing procedures to be followed if data needs to be altered after the snapshot or database lock.
- The data provided for analysis should be saved and archived within a read only regime, and is available as a reference data set for any future re-analysis or audit.
- The data generated for analysis should be validated against the data in the clinical database, unless the extraction process itself is validated.
- If applicable, documented procedures for data coding should be in place detailing the procedures to be used.
- If applicable, data coding should be performed only by personnel trained on the relevant systems with access to authorised research project-specific support material.

6 COMPLETION PHASE

The completion phase begins once the database is locked and ends when the appropriate data analysis is performed, the results are published, and the research project documents are archived.

6.1 Transferring Data [GE04]

The following points should be taken into account for the data export from the CTU to a collaborating organisation via electronic files (e.g. in the context of a meta-analysis, or for analysis by an external consultant), (see also GGOP Chapter 14.1 Data Analysis and Statistics).

- Documented procedures concerning the data transfer should be in place.
- Any files transferred out of the data centre of the CTU that include data relating to individuals should be encrypted.
- The purpose of the planned data transfer should be known and documented.
- The centre sending the data should have a written agreement/declaration from the recipient stating that the receiving organisation will maintain appropriate security of data (whilst the data remains in the direct care of that organisation).
- Procedures should be in place for agreeing on, specifying and documenting the format of the transferred data.
- Details of any specific data transfer should be logged and include a summary description of the data, sender, recipient and transfer method as well as the date on which the data was transferred.
- Copies of the data sent should be retained as read-only files and be available as a reference data set for audit/reconstruction purposes.
- If data is processed before being transferred, copies of the data as extracted before post-processing should be retained as well as copies of the data that was actually sent.

6.2 Long-Term Data Storage [GE06]

The CTU should ensure correct data storage as required by legal and regulatory requirements [ClinO Art. 18 (1); HRO Art. 5 (1)]. For general requirements regarding the archiving processes of data and documents, see also GGOP Chapter 14.5 Archiving.

- Documented procedures should be in place concerning the long-term storage of both research project documents and electronic data.
- Access to documents in physical and electronic long-term storage should be controlled, and removal or re-activation of any documents or data should be recorded.
- Measures should be in place to guarantee secure long-term storage (e.g. locked rooms and fire-proof cupboards).
- Procedures regarding the duration and content of long-term storage, which have previously been agreed upon with the customer, should be in place.
- Procedures should be in place to ensure the final destruction of physical and electronic data as required by regulations and/or the customer.