
**EUROPEAN CLINICAL RESEARCH INFRASTRUCTURES NETWORK AND
BIOTHERAPY FACILITIES: PREPARATION PHASE FOR THE
INFRASTRUCTURE**

ECRIN-PPI



**FP7 Capacities – Research Infrastructures
ECRIN-PPI No. 211738**

Additional file 1

***Standard requirements for GCP-
compliant data management in
multinational clinical trials***

Version 1 from 27 May 2010 developed by the European Clinical Research Infrastructures Network (ECRIN) Working Group on Data Centres.

Contents

Introduction	3
Abbreviations	4
IT01. Procurement and Installation (Servers)	6
IT02. Physical Security and Management	6
IT03. Logical Security and Management	7
IT04. Logical Access Control	8
IT05. Business Continuity	9
IT06. General System Validation	9
IT07. Local Software Development	10
IT08. Clinical DBMS Systems	11
IT09. Treatment Allocation Systems	12
IT10. Reporting	12
IT11. Data Export	13
IT12. Importing & Uploading Data	14
IT13. Directly Amending Data	14
IT14. Delivery of Data for Analysis	15
IT15. Long Term (electronic) Data Curation	15
DM01. Clinical Data Management Application - Design and Development	17
DM02. Clinical Data Management Application - Validation	18
DM03. Clinical Data Management Application - Change management	18
DM04. Treatment Allocation and (Un)Blinding Management	19
DM05. Site Management, Training & Support	19
DM06. Data Entry and Processing	20
DM07. Data Quality Checks	21
DM08. Query Management	22
DM09. Data Coding and Standards	22
DM10. Safety Data Management Application	23
DM11. Pre-Analysis Data Management	23
DM12. Managing (physical) Archives	23
IN01. International Aspects	24
ST01. Trials Unit staff competence	24

Introduction

The Working Group on Data Centres of the European Clinical Research Infrastructures Network (ECRIN) has developed a standard describing the requirements of GCP-compliant data management in multinational clinical trials. The standard requirements are based on international, European and national regulations and guidelines relevant to GCP, data security and IT infrastructure, as well as ECRIN documents developed previously. The requirements were developed by expert consensus of the ECRIN Working group on Data Centres, using a structured and standardised process. The requirements are divided into two main parts: an IT part covering standards for the IT infrastructure and computer systems in general, and a Data Management (DM) part covering requirements for data management applications in clinical trials. The standard developed includes 115 IT-requirements, split into 15 separate sections, 107 DM-requirements (in 12 sections) and 13 other requirements (2 sections). Sections IT01 to IT05 deals with the basic IT infrastructure while IT06 and IT07 cover validation and local software development. IT08 to IT015 concerned the aspects of IT systems that directly support clinical trial management. Sections DM01 to DM03 cover the implementation of a specific clinical data management application, i.e. a specific trial, whilst DM04 to DM12 address the data management of trials across the unit. Section IN01 is dedicated to international aspects and ST01 to the competence of a trials unit's staff. Each individual requirement is characterized by an ID number, a precise description, and categorised as either a 'minimal' requirement or 'best practice'.

Abbreviations

AE	Adverse Event
ASCII	American Standard Code for Information Interchange
BC	Business Continuity
BP	best practice
Cat	category of requirement
CDISC	Clinical Data Interchange Standards Consortium (http://www.cdisc.org/)
CDMS	Clinical Data Management System
Citrix	product of Citrix Systems, Inc (desktop virtualisation)
CONSORT	Consolidated Standards of Reporting Trials (http://www.consort-statement.org/)
CRF	Case Report Form
CSV	Comma-Separated Values
DBA	Database Application
DBMS	Database Management System
DDI	Data Documentation Initiative
DM	Data Management
eCRF	electronic Case Report Form
ECRIN	European Clinical Research Infrastructures Network (www.ecriin.org)
eRDC	electronic Remote Data Capture
FDA	Food and Drug Administration (www.fda.gov)
GAMP	Guide for Validation of Automated Systems
GCP	Good Clinical Practice
HTML	Hypertext Markup Language
iCRF	interim Case Report Form
ID	identification number of ECRIN standard requirements
IN	international requirements
IT	Information Technology
MedDRA	Medical Dictionary for Regulatory Activities (www.meddrasso.com)
Min	minimal requirement
ODM	Operational Data Model

PC	personal computer
pCRF	paper-based Case Report Form
PDF	Portable Document Format
PID	personal identifier
QA	Quality Assurance
R	R-Project for Statistical Computing, statistical software (http://www.r-project.org)
SAE	Serious Adverse Events
SAS	statistical software, product of the SAS Institute Inc.
SC	staff competence requirements
SLA	Service Level Agreement
SOP	Standard Operating Procedure
SPSS	statistical software, product of IBM Corporation
Stata	Data Analysis and Statistical Software, product of StataCorp LP
UI	user interface
UPS	Uninterruptible Power Supply (apparatus that provides emergency power)
USB	Universal Serial Bus (specification to establish communication between devices)
XML	eXtensible Markup Language
XMLschema	description of a XML document

IT 01: Procurement and Installation (Servers)

<i>ID</i>	<i>Cat.</i>	<i>Requirement</i>
IT01.01	<i>min</i>	<i>Server Specification:</i> Servers and similar equipment should be specified and selected according to the specific requirements of the trials unit and the functions being supported
IT01.02	<i>min</i>	<i>Server Builds:</i> Detailed records of builds must be available, for maintenance and safe rebuilding
IT01.03	<i>min</i>	<i>Warranties and Support:</i> Sufficient support arrangement should be in place for the expected lifetime of the equipment
IT01.04	<i>bp</i>	<i>Server Procurement:</i> Purchases should show evidence of appropriate selection between alternative suppliers and / or comply with policies stipulated by the host organisation
IT01.05	<i>bp</i>	<i>Procurement Planning:</i> There should be a defined retirement / replacement policy for servers, given expected lifetimes

Notes

IT01.N1: This section only applies to servers and other high price or specialist items, e.g. network attached storage. It does not apply to the purchase of PCs and laptops, printers and routers and other more standard equipment.

IT01.N2: It is recognised that hardware procurement is very often constrained by the policies of the host organisation (e.g. a University may insist that all servers are purchased from a single supplier).

IT02. Physical Security and Management

<i>ID</i>	<i>Cat.</i>	<i>Requirement</i>
IT02.01	<i>min</i>	<i>Locked Server Room:</i> Servers must be housed within a dedicated locked room with unescorted access limited to specified individuals
IT02.02	<i>min</i>	<i>Secured Power Supply:</i> The power supply to servers should be secured, e.g. by a UPS unit, to allow an orderly shutdown on power failure
IT02.03	<i>min</i>	<i>Encryption of non physically secure data:</i> no patient data should be stored on anything other than protected servers (e.g. on laptops, desktops, USB sticks etc.) unless it is encrypted
IT02.04	<i>min</i>	<i>Server Failure - Response:</i> Alerts on server failure within normal business hours should be sent automatically to relevant personnel
IT02.05	<i>bp</i>	<i>Server Failure - Response 24/7:</i> Alerts on server failure outside of normal business hours should be sent automatically to relevant personnel
IT02.06	<i>bp</i>	<i>Controlled Environment:</i> Servers should be housed in a temperature controlled environment
IT02.07	<i>bp</i>	<i>Theft and Malicious Damage:</i> The server room/building should have an alarm system with the alarm linked to a central response centre

IT02.08	<i>bp</i>	<i>Hazard Control - Fire Alarms:</i> The server room should be fitted with heat and smoke alarms, monitored 24/7
IT02.09	<i>bp</i>	<i>Hazard Control - Fire Response:</i> The server room should be fitted with automatic fire response measures (e.g. inert gas)
IT02.10	<i>bp</i>	<i>Hazard Control - Water:</i> Water ingress (e.g. from external flooding) that could inundate power supply / servers should be very unlikely

Notes

IT02.N1: The 'General Note on Scope and Responsibilities', at the beginning of this document is particularly relevant to this list of standards. Many of the functions listed above may be outside the direct control of the trials unit, and formal documents / agreements should therefore be available to provide evidence that the standards are being met.

IT03. Logical Security and Management

<i>ID</i>	<i>Cat.</i>	<i>Requirement</i>
IT03.01	<i>min</i>	<i>Security Management System:</i> Regular reviews of IT security systems, practices and documentation, followed by any necessary planning and actions, should occur as part of an ongoing Security Management System
IT03.02	<i>min</i>	<i>Commitment to Data Protection:</i> The unit or its parent organisation can demonstrate compliance with and commitment to local data protection legislation, including relevant policies, training and individuals with designated roles (e.g. 'Data protection officer')
IT03.03	<i>min</i>	<i>External Firewalls:</i> External firewalls should be in place and configured to block inappropriate access
IT03.04	<i>min</i>	<i>Encrypted Transmission:</i> Clinical data transmitted over the internet to or from the trials unit must be encrypted
IT03.05	<i>min</i>	<i>Server Admin Role:</i> Servers should be protected by a highly restricted administrator password (i.e. known to essential systems staff only)
IT03.06	<i>min</i>	<i>Admin Password Management:</i> The administrator password should be changed regularly according to locally agreed policies, and stored securely for emergency use (e.g. off site)
IT03.07	<i>min</i>	<i>Server Maintenance:</i> Necessary patches and updates should be identified and applied in a timely but safe manner to:.... the operating system, anti-malware systems, backup systems and major apps (e.g. Clinical DBMSs, Web servers, Remote Access systems, etc.)
IT03.08	<i>bp</i>	<i>Commitment to Information Security:</i> The unit or its parent organisation can demonstrate management commitment to information security, including relevant groups, policies, training and individuals with designated roles (e.g. 'IT security officer')

IT03.09	<i>bp</i>	<i>Internal Firewalls:</i> Internal firewalls should be in place and correctly configured, e.g. blocking access to other departments, students
IT03.10	<i>bp</i>	<i>Security Testing:</i> Regular security testing should be carried out and is documented
IT03.11	<i>bp</i>	<i>Traffic Monitoring:</i> Traffic activity should be monitored and hacking attempts identified and investigated

Notes

IT03.N1: Again there may be a need for formal documents / agreements (e.g. SLAs) between the data centre and the organisation (e.g. the host university, a hosting service) that may provide or manage many of these facilities.

IT04. Logical Access Control

<i>ID</i>	<i>Cat.</i>	<i>Requirement</i>
IT04.01	<i>min</i>	<i>Logical Access Procedures:</i> SOPs and policies for access control to the network(s) and specific systems should be in place
IT04.02	<i>min</i>	<i>Access Control Management:</i> Each system requiring access controls should have mechanisms, e.g. using roles, group membership, etc., that can be used to effectively differentiate and manage access
IT04.03	<i>min</i>	<i>Granularity of Access:</i> Access control mechanisms should be granular enough so that users only see the data they need to see
IT04.04	<i>min</i>	<i>Password management:</i> Network password management should be enforced on all users, including regular password change and password complexity
IT04.05	<i>min</i>	<i>Remote Access:</i> Remote access (e.g. via Citrix) should be controlled to the same standards as above, and should not normally include access to the host's network
IT04.06	<i>min</i>	<i>Desktop Lockout:</i> Desktop logins should post a blank screen or screensaver after a locally determined shut down period, and require password re-activation
IT04.07	<i>min</i>	<i>Control - Clinical Data:</i> Access rights to Clinical Data Systems should be regularly reviewed, changes to access requested and actioned according to defined procedures, by designated individuals, with records kept of all rights, when granted, why and by whom.
IT04.08	<i>bp</i>	<i>Control - General:</i> Access rights to the network and general should be regularly reviewed, changes to access requested and actioned according to defined procedures, by designated individuals, with records kept of all rights, when granted , why and by whom

Notes

IT04.N1: This section applies to access control for users, both the initial access to the network (often managed by the host organisation) and the specific access required within applications (normally managed using those applications).

IT05. Business Continuity

<i>ID</i>	<i>Cat.</i>	<i>Requirement</i>
IT05.01	<i>min</i>	<i>Business Continuity Plan:</i> A Business Continuity plan should be present, covering likely action in the event of a major loss of function (e.g. fire, long term power failure, full server failure, sudden loss of key staff)
IT05.02	<i>min</i>	<i>Back Up Policies:</i> Documents detailing backup policy, procedures, restores and testing must be in place
IT05.03	<i>min</i>	<i>Back Up Frequency:</i> Back ups must be taken at least once every 24 hours, using a managed, documented regime
IT05.04	<i>min</i>	<i>Back Up Storage:</i> Back up media should be stored in a fire proof safe
IT05.05	<i>min</i>	<i>Recovery Testing:</i> Testing of full restore procedures, back to the original server, should take place at least annually
IT05.06	<i>min</i>	<i>Off site archiving:</i> The back up regime should involve regular offsite storage of archive media (e.g. monthly)
IT05.07	<i>bp</i>	<i>Business Continuity Integration:</i> The unit's BC should be integrated with the host organisation's BC plan and appropriate access arranged
IT05.08	<i>bp</i>	<i>Specified Downtime:</i> A trials unit should state, and adhere to, a specific maximum downtime to any potential user
IT05.09	<i>bp</i>	<i>Business Continuity Review:</i> Regular review, should occur, at least annually, of the detailed BC plan
IT05.10	<i>bp</i>	<i>Back up - Transaction Logs:</i> Transaction log backups should take place regularly through the working day, according to a locally agreed plan
IT05.11	<i>bp</i>	<i>Back up - Environment:</i> The server / DBA environment (groups, log-ins, jobs etc.) should be captured and restorable
IT05.12	<i>bp</i>	<i>Back up - Warm / Hot Failover:</i> Log shipping or a mirroring procedure should be in place to a warm / hot failover system
IT05.13	<i>bp</i>	<i>Failover testing Recovery:</i> If available, testing of full restore procedures from a warm / hot failover system should take place at least annually

IT06. General IT System Validation

<i>ID</i>	<i>Cat.</i>	<i>Requirement</i>
IT06.01	<i>min</i>	<i>Validation Policies:</i> Policies and SOPs should be in place covering system validation systems and processes
IT06.02	<i>min</i>	<i>Validation master plan:</i> The unit should have a validation master plan in place, identifying systems, the risks associated with each, and the consequent validation strategy for each

IT06.03	<i>min</i>	<i>Risk based approach:</i> The general approach to validation of any system should be based on analysis of potential risk, and take into account the system's usage, users and origins
IT06.04	<i>min</i>	<i>Individual validation plans:</i> Detailed validation plans should exist for any particular system, in line with the master plan and policies described above, detailing the validation required, how and when it should be done, and how it should be recorded
IT06.05	<i>min</i>	<i>Summaries and Recording:</i> A signed and dated summary of the results of each major validation episode should exist, for each system being validated
IT06.06	<i>min</i>	<i>Detailed Evidence:</i> More detailed evidence - e.g. of test results or signed user statements - should be available as evidence for the summary validation documents
IT06.07	<i>min</i>	<i>Change Control Policies:</i> Policies and SOPs should be in place defining change control mechanisms and their scope, who should authorise and review requests, and how they should be documented.
IT06.08	<i>min</i>	<i>Change and Re-validation:</i> Changes in systems should result in a review of the need for revalidation
IT06.09	<i>min</i>	<i>Software Development:</i> Evidence should be available that QA processes during software development have been implemented properly

Notes

IT06.N1: These standards apply to general validation of systems, and **not** the specific validation of systems as applied to / used by particular trials. That validation is the subject of DM 02: **Clinical Data Management Application** - Validation and DM 03: **Clinical Data Management Application** – Change management.

IT06.N2: There is no attempt to distinguish validation on different types of systems - e.g. hardware versus software, commercial versus locally developed. The standards above represent an attempt to specify the *general principles* that should be followed and demonstrated by an ECRIN data centre. In practice, different systems will have very different validation requirements - the centre needs to be able to justify the decisions taken.

IT06.N3: A variety of guides and plans exist to assist with validation. The GAMP® “Guide for Validation of Automated Systems”, for instance, is one that many people find useful.

IT07. Local Software Development

<i>ID</i>	<i>Cat.</i>	<i>Requirement</i>
IT07.01	<i>min</i>	<i>Documentation of in-house software:</i> All modules should be fully documented and specify inputs, outputs, purpose as well as a description of internal mechanisms and algorithms
IT07.02	<i>bp</i>	<i>Code Review:</i> Regular review and walk through of program code should occur

IT07.03	<i>bp</i>	<i>Re-usable Modules:</i> A library of reusable validated code / modules / components should be developed
IT07.04	<i>bp</i>	<i>Development Model:</i> A V-model based procedure is recommended, with constituent modules first validated individually and then integrated before re-validation at the system level
IT07.05	<i>bp</i>	<i>In line Commenting:</i> All code should have sufficient in line documentation to support tracing of program execution

Notes

IT07.N1: Aside from the initial requirement for comprehensive documentation these standards are really a set of recommendations about software development. The key remains the validation of the software, as covered in IT06. Thus the requirement to validate will be the same, and the requirement to assure properly controlled software development will be the same, whether the software is developed locally or purchased from a commercial software house.

IT08. Clinical DBMS Systems

<i>ID</i>	<i>Cat.</i>	<i>Requirement</i>
IT08.01	<i>min</i>	<i>Development and Production Instances:</i> The system offers two instances: development and production
IT08.02	<i>min</i>	<i>Timestamp Control:</i> Time synchronization within the CDMS is ensured. Sites using eRDC are not able to change the system's time stamp
IT08.03	<i>bp</i>	<i>Metadata Audit Trail:</i> An audit trail for metadata changes is implemented
IT08.04	<i>bp</i>	<i>Available audit trail:</i> The audit trail for any particular data item is visible and readable from the user interface for authorised users
IT08.05	<i>bp</i>	<i>Searchable audit trail:</i> The audit trail is searchable and capable of producing audit trail reports
IT08.06	<i>bp</i>	<i>Development, Production and Test Instances:</i> The system offers three instances: development, test, production. The test environment and the production environment are identical
IT08.07	<i>bp</i>	<i>Latin Characters:</i> Systems support a full range of accented Latin characters
IT08.08	<i>bp</i>	<i>Date/numerical Representation:</i> It is possible to set and use different date and numerical representations in the system

Notes

IT08.N1: These standards refer to the IT specific aspects of the database systems used for clinical trial data, the Clinical DBMSs (or CDMSs).

IT09. Treatment Allocation Systems

<i>ID</i>	<i>Cat.</i>	<i>Requirement</i>
IT09.01	<i>min</i>	<i>Documentation & Validation:</i> The underlying logic and operations of all systems for allocating subjects to treatments must be clearly documented and validated
IT09.02	<i>min</i>	<i>Record of Allocation:</i> A record of all allocation material generated (e.g. randomisation lists) and all decisions made (e.g. within a dynamic balancing system) must be maintained
IT09.03	<i>min</i>	<i>Failover to Manual:</i> System(s) must be in place, supported by training, to deal with a loss of normal electronic randomisation
IT09.04	<i>bp</i>	<i>Monitoring:</i> The randomness of list generation or minimisation should be monitored in the context of any particular trial

Notes

IT09.N1: These standards should be read in conjunction with DM04. Treatment Allocation and (Un)Blinding Management

IT09.N2: Documentation of algorithms for treatment allocation should make appropriate reference to the statistical literature. Similarly validation plans should include where possible formal tests of randomness and fitness for purpose drawn from the literature.

IT10. Reporting

<i>ID</i>	<i>Cat.</i>	<i>Requirement</i>
IT10.01	<i>min</i>	<i>Report access control:</i> Access to different reports should be controlled and match the users' requirements
IT10.02	<i>min</i>	<i>Report Validation:</i> The structure and accuracy of reports should be validated against the source data, frequency of validation being determined by a change control process
IT10.03	<i>min</i>	<i>Single Subject Data:</i> It should be possible to examine and export a full record of a single subject's data (excluding personal identifying data)
IT10.04	<i>bp</i>	<i>Standard Reports:</i> A set of frequently required (parameterised) reports should be available to appropriate users
IT10.05	<i>bp</i>	<i>UI Ad Hoc Reports:</i> It should be possible to extract ad-hoc filtered datasets (reports) via the UI
IT10.06	<i>bp</i>	<i>Audit Data:</i> Selected reports should include the option of including audit related data
IT10.07	<i>bp</i>	<i>Report Rerun:</i> Once a report is parameterised by user it should be possible to save and rerun it
IT10.08	<i>bp</i>	<i>Metadata included:</i> The option should exist to include a metadata description of extracted data

IT10.09	bp	<i>Study definition:</i> Standard reports should include the details of the current study definition in an approved XML schema (trial schedule and data items)
IT10.10	bp	<i>Format of Reports:</i> Report data can be generated / exported in formats agreed with local report consumers , e.g. PDF, HTML, XML
IT10.11	bp	<i>Data Personnel:</i> It should be possible to examine and export a record of a single data entry clerk's input data
IT10.12	bp	<i>Key Field Changes:</i> It should be possible to examine and export a full list of changes to identified key fields, e.g. fields reporting toxicity as part of monitoring
IT10.13	bp	<i>Automatic Generation:</i> The generation of reports can be automated and can be scheduled

IT11. Data Export

ID	Cat.	Requirement
IT11.01	min	<i>Data Export Procedures:</i> SOPs and policies for data exports should be in place
IT11.02	min	<i>Encryption of PID:</i> The inclusion of any patient identifiable data means any exported file(s) must be encrypted
IT11.03	min	<i>Purpose Recorded:</i> The purpose of the planned data transfer(s) and the nature of any further processing / transfer planned for the data should be known and logged
IT11.04	min	<i>Assuring Security:</i> The unit sending the data must have a written agreement / declaration from the recipient that the receiving organisation will maintain appropriate security of data
IT11.05	min	<i>Records of Transfers:</i> Details of any specific data transfer should be logged, including list of data items, sender, recipient and transfer method, and the date sent
IT11.06	min	<i>Retention of Copies:</i> Copies of the data sent should be retained within a read only regime and be available as a reference data set for audit / reconstruction purposes
IT11.07	bp	<i>Format of Transfers:</i> The format of data should be as specified by the recipient
IT11.08	bp	<i>Electronic Archiving:</i> Standardised formats for electronic archiving (e.g. ASCII, PDF, XML, CDISC ODM, FDA approved SAS format) are used

Notes

IT10.N1: These statements cover the export of any data from the trials unit to a collaborating organisation, e.g. in the context of meta-analysis, or for analysis by an external consultant, when electronic files are used. They are not restricted to electronic transfer, however, and include situations when a USB memory stick is sent by post.

IT12. Importing & Uploading Data

<i>ID</i>	<i>Cat.</i>	<i>Requirement</i>
IT12.01	<i>min</i>	<i>Upload Procedures:</i> SOPs and policies for importing / uploading data should be in place
IT12.02	<i>min</i>	<i>File Retention I:</i> The original files received should be retained within a read only regime, and be available as a reference data set for audit / reconstruction purposes
IT12.03	<i>min</i>	<i>Logging of Uploads:</i> Each upload process should be documented and logged
IT12.04	<i>bp</i>	<i>File Retention II:</i> Any files prepared from the originals and used as the direct source of the upload should be kept securely within a read only regime for audit / reconstruction purposes
IT12305	<i>bp</i>	<i>Data Validation on Input:</i> Data uploaded to clinical data systems should be checked and annotated as per normal data entry

Notes

IT11.N1: These standards cover uploading bulk data, e.g. from laboratories and collaborators, whether manually, machine or system generated.

IT13. Directly Amending Data

<i>ID</i>	<i>Cat.</i>	<i>Requirement</i>
IT13.01	<i>min</i>	<i>Requests for Amendment:</i> Any requests must be in writing and retained, and must include the justification for the change
IT13.02	<i>min</i>	<i>Recording Amendments:</i> Any changes made must be logged and the details noted

Notes

IT12.N1: These two standards cover the relatively unusual situation of a data centre being asked to directly amend data in a database, i.e. without using the normal system UI and therefore without the normal audit trail. This may occur if data originally collected outside the system (e.g. from collaborators, monitors, the randomisation system) needs later amendment for some reason. Strict controls must be applied and the related standard statements are given above.

IT14. Delivery of Data for Analysis

<i>ID</i>	<i>Cat.</i>	<i>Requirement</i>
IT14.01	<i>min</i>	<i>Preparation for Analysis Procedures:</i> SOPs and policies for generating and preserving datasets for analysis should be in place
IT14.02	<i>min</i>	<i>R/O Analysis Data Retention:</i> The base data provided for analysis is retained within a read only regime, and is available as a reference data set for any future re-analysis or audit
IT14.03	<i>min</i>	<i>Extracted Data Validation:</i> The data generated for analysis, and / or the extraction process, should be validated against the source data in the clinical database (not necessarily by IT staff)
IT14.05	<i>bp</i>	<i>Extracted Data - Formats:</i> The data generated can be generated in Stata, SAS, R and SPSS native formats (as well as CSV, XML)

Notes

IT13.N1: These standards should be read in conjunction with DM11: Pre-Analysis Data Management.

IT13.N2: The notion of locking or freezing a database at the very end of data input is of limited relevance in many trials, where a succession of safety and efficacy analyses are run at different time points, and where data collection may be planned indefinitely (or at least until all subjects have died). The title of this list reflects this.

IT15. Long Term (electronic) Data Curation

<i>ID</i>	<i>Cat.</i>	<i>Requirement</i>
IT15.01	<i>min</i>	<i>Data Preparation Policies:</i> Policies / SOPs about <i>what</i> data would normally be curated (should normally include metadata, the protocol and other documents as well as all clinical data) should be in place
IT15.02	<i>min</i>	<i>Data Retrieval from Curation:</i> Policies / SOPs about <i>how</i> data would normally be retrieved/ accessed, and who is authorised to do so by the sponsor / investigator, should be in place
IT15.03	<i>min</i>	<i>Data Destruction:</i> Final destruction of data, if required /allowed, should be as specified by regulations, funding body and/or sponsor
IT15.04	<i>min</i>	<i>Recovery Testing:</i> The recovery process(es) should be documented and tested
IT15.05	<i>bp</i>	<i>Data Preparation formats:</i> Data from databases should be decrypted if necessary and transformed into pre-approved XML schemas (e.g. CDISC ODM, Data Documentation Initiative (DDI) 3), or into plain ASCII text files
IT15.06	<i>bp</i>	<i>Data Preparation - Identifiers:</i> Subject identifiers should be reduced to a minimum or removed altogether, depending on policies / requirements

IT15.07	<i>bp</i>	<i>Data Preparation - Records:</i> The data preparation process, its inputs, dates and details, should be logged
IT15.08	<i>bp</i>	<i>Additional Material Generation:</i> Additional electronically stored material may be generated to ensure copies of paper only documents are available (i.e. by scanning)
IT15.09	<i>bp</i>	<i>Curation Facilities:</i> Service level agreements should be in place with specialist curation providers, providing physical and logically secure long term storage

Notes

IT14.N1: Long term curation generally refers to the permanent storage of data which is no longer being used, but for which restoration and re-access may nevertheless be required in the future. It may involve the removal of the data from the original system. These standards only refer to the processes involved in the *logical* preparation of data for long term curation. The physical and technical aspects of this form of storage are specialised and it is envisaged that centralised and / or third party services would normally be used (as reflected in the relevant statements below).

IT14.N2: This list should be read in conjunction with DM12: Managing (physical) Archives.

DM 01: Clinical data management application - Design and Development

No.	Cat.	Requirement
DM01.01	<i>min</i>	<i>Development Lifecycle Policy</i> : SOPs covering the development lifecycle of the clinical data management application and the CRF (incl. development, testing and deployment) should be in place
DM01.02	<i>min</i>	<i>Design of CRFs</i> : Process of CRF design is documented, reviewed and includes version management
DM01.03	<i>min</i>	<i>Cross-disciplinary Team</i> : Clinical data management application and CRF development is performed by a cross- disciplinary team (e.g. programmer, trial manager, statistician, data manager)
DM01.04	<i>min</i>	<i>Requirement Specifications of CRF</i> : The requirements specification for the CRF is driven by the protocol (e.g. primary safety and efficacy variables) and takes into consideration the workflow of trial procedures and organizational aspects
DM01.05	<i>min</i>	<i>Standardized Questionnaires/Instruments</i> : Validated questions, scales or standard instruments are used where possible (e.g. quality of life questionnaires) and the integrity of validated questionnaires is maintained
DM01.06	<i>min</i>	<i>Data Non-redundancy</i> : CRF does not duplicate data (e.g. no redundant questions, if not for validation / data management purposes) or calculates results unnecessarily
DM01.07	<i>min</i>	<i>Functional Specifications of CRFs</i> : CRF functional specifications exist identifying each data item on each CRF (including field names, types, units, validation logic, conditional branching)
DM01.08	<i>min</i>	<i>Checking of clinical data management application</i> : Procedures are implemented for checking (e.g. proofreading) the clinical data management application including eCRF and pCRFs against specifications and protocol
DM01.09	<i>min</i>	<i>Delivery of CRFs</i> : CRFs are delivered to sites prior to enrolment
DM01.10	<i>min</i>	<i>Evaluation of CRF Usability</i> : The usability of eCRFs is evaluated and assessed before deployment to live environment
DM01.11	<i>bp</i>	<i>Review of CRFs</i> : CRFs are reviewed against the protocol, end-user expectations and CRF design best practice (e.g. use of validated questionnaires). An acceptance test for CRFs is conducted
DM01.12	<i>bp</i>	<i>Use of Interim CRF</i> : In cases of eCRF an interim CRF (iCRF) should be available to allow data to be accurately recorded / collated at sites prior to data entry for emergency cases (e.g. if eCRF not available)
DM01.13	<i>bp</i>	<i>Documentation Principles</i> : Common documentation principles are applied to data items (e.g. preferred coding system, numbering of items, types of missing data, complete answer categories, preference for positive formulated questions, etc.)

DM01.14	<i>bp</i>	<i>Libraries and Metadata Repositories:</i> Libraries with procedures concerning library management and/or a metadata repository are used, enabling reuse of predefined data items/forms
DM01.15	<i>bp</i>	<i>Quality Management:</i> Quality documents covering good design practice, usability, local design conventions, etc. are available
DM01.16	<i>bp</i>	<i>User Friendliness of CRFs:</i> CRFs are divided into appropriate sections with simple and clear instructions for completion and use consistent design principles

DM 02: Clinical data management application - Validation

No.	Cat.	Requirement
DM02.01	<i>min</i>	Clinical Data Management Application Policies: SOPs and policies for clinical data management application and CDMS validation are in place
DM02.02	<i>min</i>	<i>Trial-specific Test Plan:</i> A trial-specific test plan defines the test methodology, covering scope of test, item pass/fail criteria, etc.
DM02.03	<i>min</i>	<i>Test against Functional Specifications:</i> The testing with sample data against functional specifications is carried out before deployment to live environment
DM02.04	<i>min</i>	<i>Test of Data Checks:</i> tests of all validation checks and conditional data capture mechanisms, plus any derivations are conducted, documented and retained
DM02.05	<i>min</i>	<i>Validation Report:</i> data validation final report for the trial has to be provided and signed by responsible DM person
DM02.06	<i>min</i>	<i>CRF Approval:</i> approval of the CRF is signed off by key persons
DM02.07	<i>min</i>	<i>Check of Validation Programs, Lists and Scripts:</i> validation programs, lists and scripts are checked, tested, documented and retained
DM02.08	<i>bp</i>	<i>Validation against Specifications:</i> the process of clinical data management application design and data checks programming is validated against specifications
DM02.09	<i>bp</i>	<i>Validation Report Generation:</i> system is able to generate reports used for validation

DM 03: Clinical data management application - Change management

No.	Cat.	Requirement
DM03.01	<i>min</i>	<i>Change Management of Clinical Data Management Application:</i> SOPs and policies for clinical data management application change management are in place, including last minute changes
DM03.02	<i>min</i>	<i>Change Management of Metadata:</i> individual requests for change to metadata (e.g. meta-data, specification of CRF) are justified, itemised and recorded by authorised personnel

DM03.03	<i>min</i>	<i>Amendment for Change:</i> a risk analysis is conducted before major amendment for change. For each major change the changes, implications and consequent further actions are recorded
DM03.04	<i>min</i>	<i>Test of Amendments:</i> any amendment is tested in the test environment, following test specifications and the test results are recorded
DM03.05	<i>min</i>	<i>Renewed Training:</i> in the case of significant changes, the need for re-training is evaluated and implemented if necessary
DM03.06	<i>min</i>	<i>Information of Changes:</i> mechanisms are implemented to easily inform relevant staff and users of changes, and provide support and explanatory material as required
DM03.07	<i>bp</i>	<i>Requirements for amended CRF:</i> an amended CRF (that may require ethical approval) has to conform to requested amendments and/or revised protocol. Trial amendments, that may have consequences on the CRF, are taken into consideration
DM03.08	<i>bp</i>	<i>CRF-versioning:</i> CRF page numbering and version information is always updated to reflect the current status
DM03.09	<i>bp</i>	<i>Management of Change Requests:</i> change requests are accumulated to minimize amendments

DM 04: Treatment Allocation and (Un)Blinding Management

No.	Cat.	Requirement
DM04.01	<i>min</i>	<i>Policies for the Implementation of Randomisation:</i> SOPs and policies for the set up of randomisation in any particular trial are in place
DM04.02	<i>min</i>	<i>Policies for ensuring Randomisation/Blinding:</i> SOPs and policies exist for protection of blinding and conservation of random allocation to treatment groups
DM04.03	<i>min</i>	<i>Policies for Unblinding:</i> SOPs are in place to support rapid and safe unblinding of blinded treatments
DM04.04	<i>min</i>	<i>Specification of Randomisation:</i> specification for the underlying system(s) or the specific trial randomisation process is available
DM04.05	<i>min</i>	<i>Randomisation Implementation:</i> the randomisation implementation for any particular trial conforms to the protocol
DM04.06	<i>min</i>	<i>Specification of the Randomisation Design:</i> the study statistician is responsible for the specification of the randomisation design. A randomisation specification document is provided
DM04.07	<i>min</i>	<i>Problem Management of Randomisation:</i> any problems that arise in the randomisation process are logged and the subsequent actions recorded
DM04.08	<i>min</i>	<i>Randomisation Training:</i> all staff who handles randomisation requests is adequately trained for each specific trial randomisation process

DM 05: Site Management, Training & Support

No.	Cat.	Requirement
DM05.01	min	<i>Policies for Site Opening:</i> SOPs or policies for opening a centre for data collection are in place
DM05.02	min	<i>User Training for Data Entry:</i> user training with data entry instructions or guidelines, for both pCRFs and eCRFs, is provided for relevant site staff and is documented
DM05.03	min	<i>Test or Productive Environment:</i> it is clearly indicated to the user whether they are working on a test eCRF or whether the "real trial" has been opened
DM05.04	min	<i>Access to Production System:</i> site has access to production data systems only once all relevant paperwork and training has been completed; including ethical and research approvals, contracts, site initiation
DM05.05	min	<i>Site Documentation:</i> after significant changes site documentation is updated
DM05.06	min	<i>Responsibility list:</i> an up to date list of who can do what at each site, including complete CRFs, i.e. a 'delegate log', is maintained

DM 06: Data Entry and Processing

No.	Cat.	Requirement
DM06.01	min	<i>Data Entry Policies:</i> SOPs and policies for data entry and corrections are in place
DM06.02	min	<i>Restriction of Data Access:</i> site staff have access only to data of their site
DM06.03	min	<i>Data Security:</i> data manager and IT-staff involved will keep data secure and confidential at all times
DM06.04	min	<i>System Security:</i> system security and access control is ensured, data is only accessible to authorised personnel
DM06.05	min	<i>Tracking of CRFs:</i> a CRF tracking system is in place.
DM06.06	min	<i>Management of missing CRFs:</i> systems identify and report on missing or late CRFs /data
DM06.07	min	<i>Quality of Received Data:</i> data received is checked (pCRF and eCRF)
DM06.08	min	<i>Data Confidentiality:</i> the blinding of information submitted to the data centre with regard to subject identifying information conforms to national requirements (pseudonymisation)
DM06.09	min	<i>Self Evident Corrections:</i> clear guidelines and procedures exist to carry out self evident corrections
DM06.10	min	<i>Simple Checks:</i> simple checks (e.g. range checks) should be available with the possibility to unset for pCRF entry
DM06.11	min	<i>Complex Checks:</i> complex checks with critical variables (e.g. cross-form validation) are available

DM06.12	<i>min</i>	<i>Audit Trail</i> : all transactions to the trial database (insert, update, delete) have a clear and complete audit trail, covering the date and time of the input, the person making the change and the old and new values
DM06.13	<i>bp</i>	<i>Timelines for Data Entry</i> : time-lines for data entry are considered
DM06.14	<i>bp</i>	<i>Amendment/Truncation of Schedules</i> : logging systems can easily truncate and / or amend schedules to maintain accuracy in identifying outstanding data
DM06.15	<i>bp</i>	<i>Data Deletion</i> : complete deletion of data from the system is prevented unless it is to comply with a legal request. If indicated for legal reasons, total deletion only takes place using specified procedures and recording with explanatory information

DM 07: Data Quality Checks

No.	Cat.	Requirement
DM07.01	<i>min</i>	<i>Data Quality Policies</i> : SOPs and policies are in place regarding data checking, and refer as necessary to the protocol, agreed instructions, GCP and regulatory requirements
DM07.02	<i>min</i>	<i>Batch Validation Checks</i> : validation checks are able to be executed via a batch process, to identify new warnings, missing, illogical and inconsistent data
DM07.03	<i>min</i>	<i>Data Review</i> : systems are able to support data checks by generating specified data in formats that match input format (e.g. that mimic CRFs) for manual review of data, e.g. medical consistency checks, lab data pointing to an AE
DM07.04	<i>min</i>	<i>Risk Based Source Data Verification</i> : a risk based source data verification regime is implemented as specified in the protocol, with the emphasis on primary target variables and other essential data. A check of primary endpoints and other essential data is conducted
DM07.05	<i>min</i>	<i>Documentation of Checks</i> : All data checking exercises are documented
DM07.06	<i>min</i>	<i>Problem Management</i> : problems and issues are reported to the appropriate person for query generation or other resolution
DM07.07	<i>bp</i>	<i>Quality Monitoring of Sites</i> : centres are monitored for quantity / types of errors to identify potential problems, e.g. with particular preset trigger levels
DM07.08	<i>bp</i>	<i>Statistical Evaluation of Data Quality</i> : statistical methods are used to assess and evaluate data quality (e.g. measures to analyse possible problems and irregularities should cover e.g. multivariate analysis of possible outlier candidates, conspicuous data patterns, preferred numerical sequences, accumulation of values close to defined limits) and the impact on analysis should be evaluated

DM 08: Query Management

No.	Cat.	Requirement
DM08.01	<i>min</i>	<i>Query Policies:</i> SOPs and policies are available covering query format, generation, timelines, data change and resolution
DM08.02	<i>min</i>	<i>Query Resolution:</i> Procedure for resolving of queries exist
DM08.03	<i>min</i>	<i>Query Creation and Tracking:</i> Queries are created in accordance with specifications and documented procedures. Procedures for tracking of queries exist
DM08.04	<i>min</i>	<i>Responses to Queries:</i> responses are recorded when returned, identified when outstanding and resent as necessary
DM08.05	<i>min</i>	<i>Actions in Response to Queries:</i> query resolution tracked and appropriate action taken within agreed timelines and documented in the audit trail
DM08.06	<i>bp</i>	<i>Issuing of Queries:</i> queries are issued to sites within agreed timelines
DM08.07	<i>bp</i>	<i>Avoidance of Query Duplications:</i> systems avoids accidental duplication of queries
DM08.08	<i>bp</i>	<i>Generation of Messages:</i> system is able to generate messages to users not linked to specific data items (i.e. information giving, not expecting a reply)
DM08.09	<i>bp</i>	<i>Generation of Query Reports:</i> reports are generated showing query generation data, return times etc. broken down by site, by source form, etc.

DM 09: Data Coding and Standards

No.	Cat.	Requirement
DM09.01	<i>min</i>	<i>Policies for Coding:</i> SOPs and policies for coding are in place (e.g. to promote consistency and proper use of versions)
DM09.02	<i>min</i>	<i>Coding Training:</i> coding or categorisation is carried out by personnel trained on the relevant systems
DM09.03	<i>min</i>	<i>Support of CONSORT:</i> the protocol, clinical data management application and CRF, should support the CONSORT trial reporting requirements
DM09.04	<i>min</i>	<i>Coding of SAEs:</i> The constituent symptoms of all Serious AEs are coded prior to analysis (e.g. MedDRA for drugs)
DM09.05	<i>bp</i>	<i>Use of Standards for Coding:</i> coding uses named standard systems for particular types of data (e.g. MedDRA) where possible
DM09.06	<i>bp</i>	<i>Consistency of Coding:</i> coding uses consistent systems across different trials and follow consistent conventions and rules in their use
DM09.07	<i>bp</i>	<i>Coding of AEs:</i> the constituent symptoms of all AEs should be coded prior to analysis
DM09.08	<i>bp</i>	<i>Autocoding:</i> use of autoencoder(s) and synonym list(s) where possible, however within well defined limits and with authorisation from senior staff, otherwise manual coding is performed

DM 10: Safety Data Management application

No.	Cat.	Requirement
DM10.01	<i>min</i>	<i>Policies for Safety Data Management:</i> SOPs and policies for safety data management are in place
DM10.02	<i>min</i>	<i>Safety Data Management:</i> safety data management application allow the logging of all forms, faxes and correspondence involved, and subsequent information / evaluation requests
DM10.03	<i>min</i>	<i>Expedited Reporting:</i> safety data management application supports expedited reporting to authorities
DM10.04	<i>min</i>	<i>Routine Reporting:</i> safety data management application supports routine reporting to all relevant authorities when required (e.g. annual line listings)
DM10.05	<i>bp</i>	<i>Electronic Reporting:</i> Safety data management application supports reporting via electronic transfer to authorities
DM10.06	<i>bp</i>	<i>Safety Data Reconciliation:</i> safety data management application supports the reconciliation of SAEs with other safety data

DM 11: Pre-Analysis Data Management

No.	Cat.	Requirement
DM11.01	<i>min</i>	<i>Policies for Data Base Locking:</i> SOPs and policies regarding taking a fixed image of the database (snapshot) and, if required,, 'locking' and 'unlocking' databases are in place. In case a locked database is unlocked a documented reason is provided
DM11.02	<i>min</i>	<i>Data Completion:</i> all relevant data (or all except for a pre-defined / pre-agreed fraction) have been received prior to data extraction for analysis (database lock)
DM11.03	<i>min</i>	<i>Query resolution completion:</i> All queries (or all except for a pre-defined / pre-agreed fraction) have been resolved
DM11.04	<i>min</i>	<i>Data Reconciliation:</i> all external data (e.g. safety database, lab data) has been reconciled
DM11.05	<i>min</i>	<i>Data Base Consistency Check:</i> relevant batch consistency checks of database have been completed and actioned
DM11.06	<i>bp</i>	<i>Review of Coding:</i> all relevant coding has been reviewed
DM11.07	<i>bp</i>	<i>Data Base Audit:</i> database audit should be carried out, documenting error rate

DM 12: Managing (physical) Archives

No.	Cat.	Requirement
DM12.01	<i>min</i>	<i>Policies for Archiving:</i> SOPs and policies are in place concerning physical archiving of essential trial documents
DM12.02	<i>min</i>	<i>Access to Archive:</i> access to study archive is documented
DM12.03	<i>min</i>	<i>Protection of Archive:</i> measures are in place to guarantee safe archiving

		(e.g. locked rooms and fire-proof cupboards, safe area, protected and controlled access for authorized staff only)
DM12.04	<i>min</i>	<i>Archiving Duration</i> : essential trial documents (including data) are archived for as long as specified by protocol, regulations, funding body and/or sponsor
DM12.05	<i>min</i>	<i>Trial Reconstitution</i> : conduct of trial can be reconstituted from archived essential trial documents

IN 01: International Aspects

No.	Cat.	Requirement
IN01.01	<i>min</i>	<i>User Support</i> : eRDC Help Desk and Hot Line is provided covering user hours
IN01.02	<i>bp</i>	<i>CRF Translation</i> : if necessary, CRFs/eCRFs can be translated into the language(s) required for the trial, including messages associated with error checking. Translations are verified
IN01.03	<i>bp</i>	<i>Support of National Regulations</i> : application display, change or hide questions / CRFs to better support national legislation (without using different versions)
IN01.04	<i>bp</i>	<i>Multilingual User Support</i> : help desk and hot line can deal with the language of the users and provide some sort of help

SC01: Trials Unit staff competence

No.	Cat.	Requirement
SC01.01	<i>min</i>	<i>Policies for Training</i> : SOPs and policies are in place describing induction and training requirements / policies / procedures
SC01.02	<i>min</i>	<i>Staff Competence</i> : DM-staff is competent, trained or being trained to do the job(s) required of them
SC01.03	<i>min</i>	<i>Documentation of Training</i> : records of training are kept for all DM-staff, kept centrally and / or by the staff themselves
SC01.04	<i>min</i>	<i>Staff Support</i> : help and support for DM-staff is available
SC01.05	<i>bp</i>	<i>Planning of Staff Training</i> : training plans are linked to annual appraisal
SC01.06	<i>bp</i>	<i>Ticketing System</i> : a formal mechanism for requesting support and logging requests / actions should exist