EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

10 June 2021
EMA/226170/2021
Good Clinical Practice Inspectors Working Group (GCP IWG)

Guideline on computerised systems and electronic data in clinical trials

Draft

Adopted by GCP IWG for release for consultation	4 March 2021
Start of public consultation	18 June 2021
End of consultation (deadline for comments)	17 December 2021
Date for coming into effect	TBC

This guideline replaces 'Reflection paper on expectations for electronic source data and data transcribed to electronic data collection tools in clinical trials' (EMA/INS/GCP/454280/2010).

Comments should be provided using this template. The completed comments form should be sent to camelia.mihaescu@ema.europa.eu

Keywords ***Computerised systems, electronic data, validation, qualification, audit trail, user management, security, electronic clinical outcome assessment (eCOA), Interactive response technology (IRT), case report form (CRF), electronic signatures, artificial intelligence***

Guideline on computerised systems and electronic data in clinical trials

Table of contents

Glossary and abbreviations

Generally used terms

Unless otherwise specified (e.g. "source data" or "source document") and in order to simplify the text, "data" will be used in this guideline in a broad meaning which may include documents (e.g. in electronic trial master files (eTMF)), records or any form of information.

All references to a sponsor in this guideline also apply to a contract research organisation (CRO) to the extent that a CRO has assumed the trial related duties and functions of a sponsor (ICH-GCP 5.2.4).

When a computerised system is implemented by the institution where the investigator is conducting a clinical trial, any reference to the investigator in this guideline also includes that institution, as provided for by ICH-GCP 1.35 (investigator / institution: An expression meaning "the investigator and/or institution, where required by the applicable regulatory requirements"), except for those responsibilities assigned by ICH-GCP to the investigator personally and not to the investigator / institution.

The word "trial participant" is used in this text as a synonym for the term "subject", defined in Directive 2001/20/EC as "an individual who participates in a clinical trial as a recipient of the investigational medicinal product (IMP) or a control".

For the purpose of this guideline, the term "information" reflects meaningful organisation and processing of data and documentation and "data" reflects measurement and assessment of variable parameters relevant to specific outcomes. The "results" are a composition of organised and fit-for-purpose information.

Artificial intelligence

Artificial intelligence (AI) covers a very broad set of algorithms which enable computers to mimic human intelligence. It ranges from simple if-then rules and decision trees to machine learning and deep learning. Machine learning (ML) is a subset of AI and includes computer algorithms which are trained to classify or predict data, without actually being programmed to do so. ML is divided into supervised and unsupervised learning.

Deep learning (DL) is a subset of ML and contains algorithms which allow software to train itself by exposing multi-layered neural networks to vast amounts of data.

Audit trail (in computerised systems)

"Documentation that allows reconstruction of the course of events." (ICH-GCP 1.9)

In computerised systems an audit trail is a secure, computer generated, time-stamped electronic record that allows reconstruction of the course of events relating to the access, creation, modification, and deletion of an electronic record or use of the computerised system itself.

Case report form (CRF)

"*A printed, optical, or electronic document designed to record information to be reported to the sponsor on each trial subject*." (ICH-GCP 1.11)

Certified copy

"A copy (irrespective of the type of media used) of the original record that has been verified (i.e., by a dated signature or by generation through a validated process) to have the same information, including data that describe the context, content, and structure, as the original." (ICH-GCP 1.63)

Clinical outcome assessment (COA)

COA employs a tool for direct reporting of outcomes by clinicians, trial site staff, trial participants and their caregivers. The term COA is proposed as an umbrella term to cover both single dimension and multi-dimension measures of symptoms, health-related quality of life (HRQL), health status, adherence to treatment, satisfaction with treatment, etc.

Data governance

The totality of arrangements to ensure that data fulfils the ALCOA^{++} principles (see section 4.5) throughout the entire data life cycle.

Data life cycle

All processes related to the creating, recording, processing, reviewing, analysing, reporting, transferring, storing, migrating, archiving, retrieving and deleting of data.

Dynamic file formats

Dynamic files (e.g. spreadsheets with automatic calculations) include automatic processing and/or enable an interactive relationship with the user to change content (e.g. eCRF). A certified electronic copy may be retained in different electronic file formats to the original record, but the equivalent dynamic nature (including metadata) of the original record should be retained.

Good documentation practice

Good documentation practice is used to describe a standard for creation and maintenance of documentation in order to ensure its integrity. It includes, but is not limited to, that a record is made at the time of the corresponding event, that documents are printed or written (e.g. signed) with indelible and lasting ink, that critical entries are verified by a second person, that pages (e.g. in notebooks) are numbered, that documents, where applicable, are reviewed, approved, signed and dated by appropriate personnel, and that any later alterations are made as 'GxP corrections'. The latter implies that changes include the name and the signature of person *who* made the change, full visibility of *what* was changed including both the new and old text (altered text is not obscured), the date and if relevant the time *when* the change was made, and whenever not completely obvious, the reason or justification *why* the change was made. These essential characteristics apply equally for both paper and electronic records.

There is a strong bond between good documentation practice and the ALCOA++ principles (see section 4.4) and between GxP corrections and an audit trail (see section 6.2).

Important aspects are implementation of practices such as contracts, change control including version control and traceability, review, approval and distribution processes etc. for critical documents. In general, essential documents should be approved, signed and dated by the relevant/authorised persons. See also EU GMP Chapter 4.

Patient-reported outcome (PRO)

Any outcome reported directly by the trial participant and based on the trial participant's perception of a disease and its treatment(s) is called patient-reported outcome (PRO). The term PRO is proposed as an umbrella term to cover both single dimension and multi-dimension measurements of symptoms, HRQL, health status, adherence to treatment, satisfaction with treatment, etc. (Source: CHMP Reflection paper on the regulatory guidance for the use of HRQL measures in the evaluation of medicinal products - EMEA/CHMP/EWP/139391/2004)

Qualification

"Action of proving and documenting that equipment or ancillary systems are properly installed, work correctly, and actually lead to the expected results. Qualification is part of validation, but the individual qualification steps alone do not constitute process validation." (ICH Q7 20 Glossary)

Expected results for system qualification should be traceable to a system specification, e.g. a User Requirements Specification (URS).

Source data

"All information in original records and certified copies of original records of clinical findings, observations, or other activities in a clinical trial necessary for the reconstruction and evaluation of the

trial. Source data are contained in source documents (original records or certified copies)." (ICH-GCP 1.51)

Source documents

"Original documents, data, and records (e.g., hospital records, clinical and office charts, laboratory notes, memoranda, subjects' diaries or evaluation checklists, pharmacy dispensing records, recorded data from automated instruments, copies or transcriptions certified after verification as being accurate copies, microfiches, photographic negatives, microfilm or magnetic media, X-rays, subject files, and records kept at the pharmacy, at the laboratories and at medico-technical departments involved in the clinical trial)." (ICH-GCP 1.52)

Static file formats

Static files (e.g. PDF scan) containing information or data that are fixed/frozen and allow no interaction to change the content. Paper document digitised as pdf, e.g. scanned ethics approval letter.

System life cycle

The life cycle of a computerised system includes all phases of the system; i.e. typically 1) the concept phase where the regulated party considers to automate a process and where user requirements are collected, 2) the project phase where a contracted party is selected, a risk-assessment is made and the system is implemented and qualified, 3) the operational phase where a system is used in a regulated environment and changes are implemented in a manner which maintains data confidentiality, integrity and availability, and finally, 4) a retirement phase which includes decisions about data retention, migration or destruction and management of these processes.

Validation

"A process of establishing and documenting that the specified requirements of a computerized system can be consistently fulfilled from design until decommissioning of the system or transition to a new system. The approach to validation should be based on a risk assessment that takes into consideration the intended use of the system and the potential of the system to affect human subject protection and reliability of clinical trial results.". (ICH-GCP 1.65)

Abbreviations

AI	artificial intelligence
BYOD	bring your own device
(e)COA	electronic clinical outcome assessment
(e)CRF	electronic case report form
COTS	commercial of the shelf
CRO	contract research organisation
CTMS	clinical trial management systems
DMP	data management plan
DEXA	dual-energy x-ray absorptiometry
ECG	electrocardiogram
EDC	electronic data collection
EEA	European Economic Area
EU	European Union
GCP	good clinical practice
GCP-IWG	GCP Inspectors' Working Group
GPS	global positioning system
(e)HR	electronic health records
HRQL	health-related quality of life

HTTPS	hypertext transfer protocol secure
IB	investigator brochures
ICH	International Conference on Harmonisation
IMEI	international mobile eEquipment identity
IMP	investigational medicinal product
IaaS	Infrastructure as a service
IQ/PQ	installation qualification/performance qualification
IRT	interactive response technology
IT	information technology
IVRS	interactive voice response system
MEID	mobile equipment identifier
PI	principal investigator
PaaS	Platform as a service
PC	personal computer
SaaS	software as a service
SOP	standard operating procedure
SUSAR	suspected unexpected serious adverse reaction
(e)TMF	electronic trial master file
UAT	user acceptance testing
URS	user requirements specification
UTC	universal time coordinated
VAS	visual analogue scales
VPN	virtual private network

Executive summary

Computerised systems are being increasingly used in clinical research. The complexity of such systems has evolved rapidly during the last years from eCRF, ePROs, to various wearable devices used to continuously monitor trial participants for clinically relevant parameters and ultimately to the use of AI. The latter will be further elaborated on in a future Annex. Changes in trial types (e.g. implementation of fully or partly decentralised trials) will also mean an increased use of computerised systems. Hence there is a need to provide guidance to sponsors, CROs, investigators, and other parties involved in the design, conduct and reporting of clinical trials reflective of these changes in data types and trial types on the use of computerised systems and on the collection of electronic data, as this is important to ensure the quality and reliability of trial data, as well as the safety and wellbeing of the trial participants. This would ultimately contribute to a robust decision-making process based on such clinical data.

1. Introduction

As described above, the change in data and trial types and thereby the use of computerised systems presents new challenges. The EMA '*Reflection Paper on expectations for electronic source data and data transcribed to electronic data collection tools in clinical trials*' started to address these when it was published in 2010. However, the development of and experience with such systems has progressed. A more up to date guideline is needed.

2. Scope

The scope of this guideline is computerised systems, (including instruments, software and services) used in clinical trials in the creation/capture of electronic clinical data and to the control of other processes in the conduct of a clinical trial of investigational medicinal products. These include, but may not be limited to the following:

- Electronic Health Records (eHR), used by the investigator for capture of all health information as per normal clinical practice.
- Tools supplied to investigators/trial participants for recording clinical data by data entry (e.g. COAs).
    - Electronic trial participant data capture devices used to collect ePRO data, e.g. mobile devices supplied to trial participants or applications for the use by the trial participant on their own device (bring your own device (BYOD)).
    - Electronic devices used by clinicians to collect data e.g. mobile devices supplied to clinicians.
- Tools supplied for automatic capture of events such as biometric measures (e.g. blood pressure, respiratory measures or electrocardiogram (ECG) monitoring).
- eCRFs e.g. desktop or mobile device-based programs or access to web-based applications, which may contain source data directly entered, transcribed data or data transferred from other sources, or any combination of these.
- Tools that automatically capture data related to transit and storage temperatures for IMP or clinical samples.
- Tools to capture, generate, handle or store data in a clinical environment where analysis, tests, scans, imaging, evaluations, etc. involving trial participants or samples from trial participants are performed in support of clinical trials (e.g. dual-energy x-ray absorptiometry (DEXA) or X-ray machines and related software).
- eTMFs, which are used to maintain the clinical trial essential documentation.
- Electronic informed consent, for provision of information and/or capture of the informed consent when this is allowed according to national legislation, e.g. desktop or mobile device-based programs supplied to potential trial participants or applications for the use by the potential trial participants on their BYOD or access to web-based applications.
- Interactive Response Technologies (IRT), for management of randomisation, supply and receipt of IMP, e.g. via a web-based application.
- Portals for supplying information from the sponsor to the sites e.g. investigator brochures (IBs), suspected unexpected serious adverse reactions (SUSARs), training material and for documenting site review, training etc.
- Other computerised systems implemented by the sponsor holding/managing and/or analysing data relevant to the clinical trial e.g. clinical trial management systems (CTMS), pharmacovigilance databases, statistical software programming pharmacovigilance databases, statistical software, document management systems and central monitoring software.
- AI used in clinical trials e.g. for trial participant recruitment, determination of eligibility, coding of events and concomitant medication and data clarification and cleaning processes.

The approach towards computerised systems and medical devices used in clinical practice (e.g. regarding validation) should be risk proportionate. The risk-assessment should consider the relevance of the system use for the safety of the participant and the importance and integrity of derived clinical trial data i.e. whether the system is used for standard care and safety measurements for participants or if systems are used to generate primary efficacy data that are relied on in e.g. a marketing authorisation application. Systems used outside approved setting is inherently of higher risk. In case of well-established computerised systems, which are used in line with approval in a routine setting for less critical trial data, the certification by a notified body may suffice as documentation whereas other more critical systems may require a more in-depth validation effort. This decision should be justified pre-trial.

3. Legal and regulatory background

- Directive 2001/20/EC (until repealed by Regulation (EU) No 536/2014)
- Directive 2005/28/EC (until repealed by Regulation (EU) No 536/2014)
- Regulation (EU) No 536/2014

- ICH Guideline for good clinical practice E6(R2), (EMA/CHMP/ICH/135/1995 Revision 2)

This guideline is intended to assist the sponsors, investigators, and other parties involved in clinical trials in complying with the requirements of the current legislation (Directive 2001/20/EC and Directive 2005/28/EC), as well as ICH E6 Good Clinical Practice (GCP) Guideline ('ICH-GCP guideline'), regarding the use of computerised systems and collection of electronic data in clinical trials.

The guideline applies to the legal representatives and CROs, which according to the ICH-GCP guideline includes any contracted party such as vendors and service providers to the extent of their assumed trial-related duties and functions.

The risk-based approach to quality management also has an impact on the use of computerised systems and collection of electronic data. To ensure continued guidance once the Clinical Trials Regulation (EU) No. 536/2014 ('Regulation') comes into application, this guideline already prospectively considers the specific requirements of the Regulation with respect to these systems and data.

Consideration should also be given to meeting the requirements of any additional current legal and regulatory framework that may in addition apply to the medicinal product regulatory framework, depending on the digital technology. These may include e.g. medical devices, data protection legislation and legislation on electronic identification.

Further elaboration of EU GCP Inspectors' Working group's (GCP IWG) expectations on various topics, including those of computerised systems can be found as GCP Q&As published on the EMA website

4. Principles and definition of key concepts

The following sections outline the basic principles that apply to all computerised systems used in clinical trials.

4.1. Data integrity

Data integrity is achieved when data (irrespective of media) are collected and maintained in a secure manner, to fulfil the ALCOA++ principles of being attributable, legible, contemporaneous, original, accurate, complete, consistent, enduring and traceable as described in section 4.5 in order for the data to adequately support robust results and good decision making throughout the data life cycle. Assuring data integrity requires appropriate quality and risk management systems as described in section 4.6., including adherence to sound scientific principles and good documentation practices.

Data governance should address data ownership and responsibility throughout the life cycle, and consider the design, operation and monitoring of processes/systems to comply with the principles of data integrity including control over intentional and unintentional changes to data.

Data governance systems should include staff training in the importance of data integrity principles and the creation of a working environment that enables visibility, and actively encourages reporting of errors, omissions and undesirable results.

Lack of integrity before the mandated retention period can ultimately render the data unusable and is equivalent to data loss/destruction and is considered GCP noncompliant.

4.2. Responsibilities

Roles and responsibilities in clinical trials should be clear. The responsibility for the conduct of clinical trials is assigned via legislation to two parties, which may each have implemented computerised systems for holding/managing data, in the context of clinical trials:

- Investigators and their institutions, laboratories and other technical departments or clinics, generate the data, construct the record and may use their own software and hardware (purchased, part of national or institutional health information systems, or locally developed).

- Sponsors, supplying, and/or, managing and operating computerised systems (including software and instruments) and the records generated by them. The sponsors may do this directly, or via CROs, including organisations providing ePRO, eCRF, or interactive voice response system (IVRS) specialists that collect and store data on behalf of sponsors.

Please refer to Annex 1 regarding the contracting out of tasks related to computerised systems.

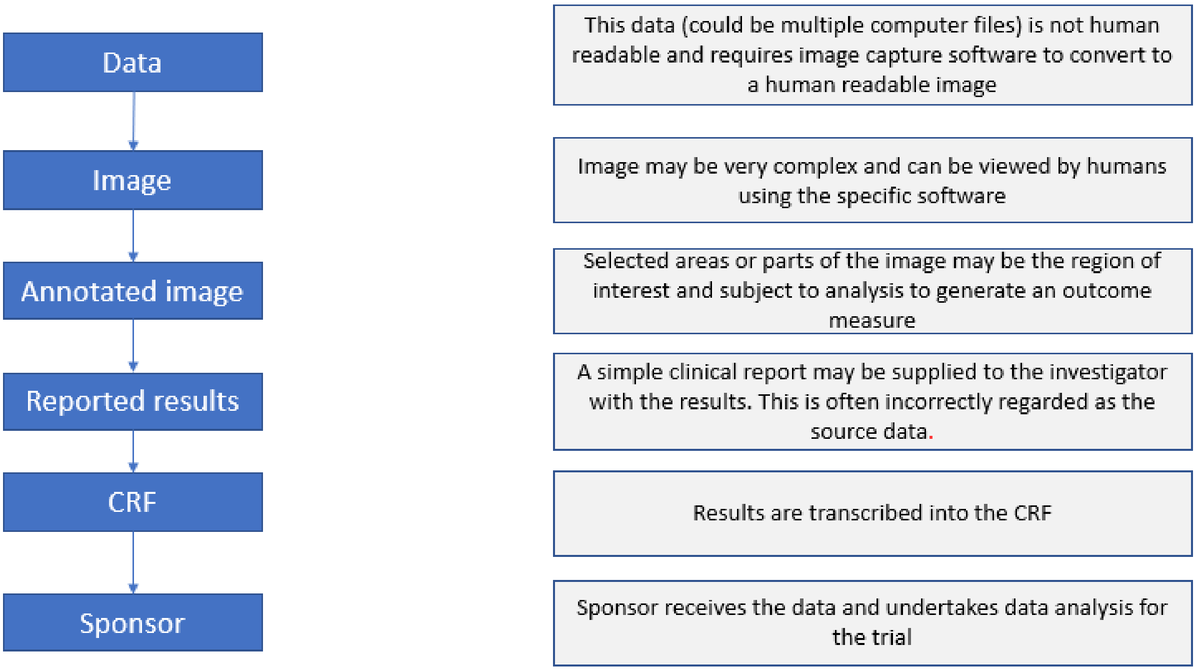
4.3. Electronic data

Data consists of collected individual data points. Data becomes information when viewed in context. Metadata is providing context for the data point. Different types of metadata exist such as: variable name, unit, field value before and after change, reason for change, TMF location document identifier, time stamp, user. Typically, these are data that describe the characteristics, structure, data elements and inter-relationships of data e.g. audit trails. Metadata also permit data to be attributable to an individual (or if automatically generated, to the original data source). Metadata form an integral part of the original record. Without the context provided by metadata the data has no meaning.

4.4. Source data

The term source data usually refers to the original reported observation in a source document. However, source data can be processed to a certain degree. Part of the collection process already transforms values e.g. CT scanning images.
Source data files could be e.g. hospital records, clinical and office charts, laboratory notes. Further examples include e-mails, spreadsheets, audio and/or video files, images and tables in databases. An electronic document that contains source data is considered an electronic source document. It is important to ensure that the true source data list is understood, defined and retained.

The location of source documents and the associated source data they contain, should be clearly identified at all points within the data capture process.
Below is an example (figure 1) of a situation where the true source data (e.g. imaging, but could also relate to information from a wearable) is often not used for source data verification, or it is not ensured that it is retained.



This data (could be multiple computer files) is not human readable and requires image capture software to convert to a human readable image

Image may be very complex and can be viewed by humans using the specific software

Selected areas or parts of the image may be the region of interest and subject to analysis to generate an outcome measure

A simple clinical report may be supplied to the investigator with the results. This is often incorrectly regarded as the source data.

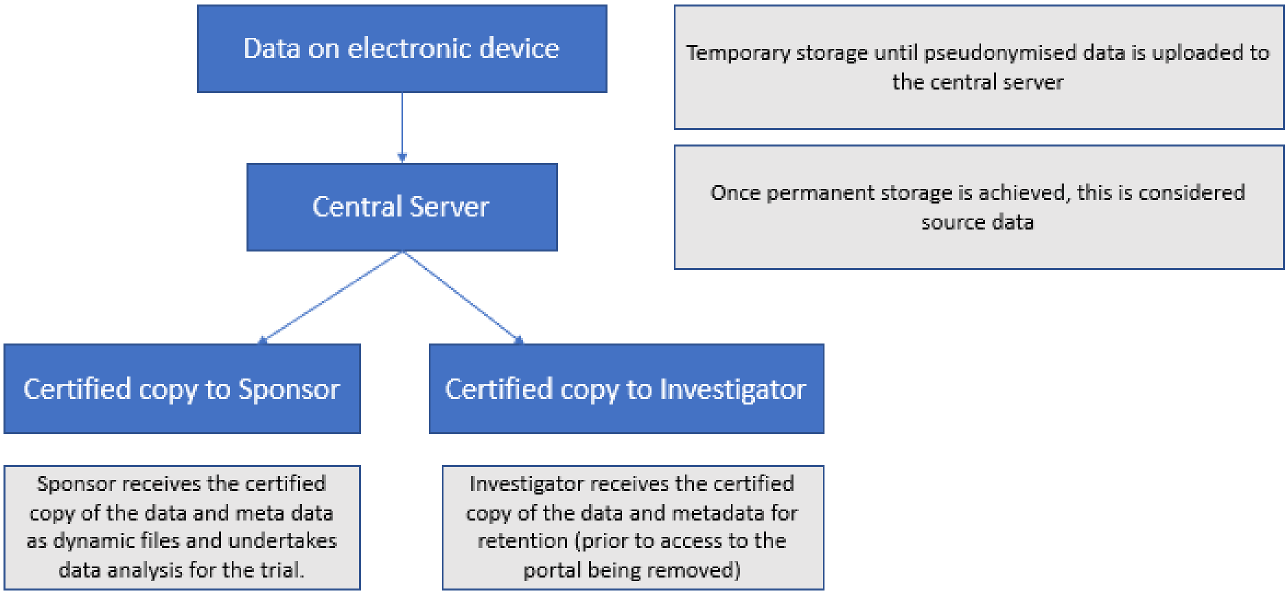
Results are transcribed into the CRF

Sponsor receives the data and undertakes data analysis for the trial

Fig. 1

From a practical point of view, the first obtainable permanent data from an electronic data generation/capture should be considered and defined as the electronic source data. This process should be validated to ensure that the source data generated/captured is representative of the original observation and should contain metadata, including audit trail, to ensure data is attributable, legible, complete, original and accurate (see minimum requirements for electronic source data). See section 4.5. The logical location where the source data is first obtained should be part of the metadata.

Below is an example of a typical data flow for the use of ePRO, wearables etc. (figure 2):


Data on electronic device
Central Server
Certified copy to Sponsor
Certified copy to Investigator

Temporary storage until pseudonymised data is uploaded to the central server

Once permanent storage is achieved, this is considered source data

Sponsor receives the certified copy of the data and meta data as dynamic files and undertakes data analysis for the trial.

Investigator receives the certified copy of the data and metadata for retention (prior to access to the portal being removed)

Fig. 2

4.5. ALCOA(++) principles

A number of attributes are considered of universal importance to data. These include that the data are:

Attributable

Data should be attributable to the person generating the data. Based on the criticality of the data, it should also be traceable to the system/device, in which the data were generated/captured. The information about originator (e.g. system operator, data originator) and system (e.g. device, process) should be kept as part of the metadata.

Legible

Data should be maintained in a readable form to allow review in its original context. Therefore, changes to data, such as compression, encryption and coding should be completely reversible to facilitate this.

Contemporaneous

Data should be generated by a system or captured by a person at the time of the observation. The information of the timepoint of observation and the time point of permanent save should be kept as part of the metadata, including audit trail. Accurate date and time information should be automatically captured and should be linked and set by an external standard (e.g. universal time coordinated (UTC), central server).

Original

Data should be the original first generation/capture of the observation. Certified copies can replace original data (See section on certified copies: 6.5.). Information that is originally captured in a dynamic state should remain available in that state.

Accurate

The use of computerised systems should ensure that the data are at least as accurate as those recorded by paper means. The coding process, which consists in matching text or data collected on the CRF to terms in a standard dictionary, thesaurus or tables (e.g. units, scales), should be controlled. The process of data transfer between systems should be validated to ensure the data remains accurate.

Data should be an accurate representation of the observations made. Metadata should contain information to describe the observations and, where appropriate, it could also contain information to confirm its accuracy.

Complete

To reconstruct and fully understand an event, data should be a complete representation of the observation made and should be represented in the original context and associated metadata, including audit trail. Data where the original context or the metadata, including audit trail, were lost and/or detached is not complete.

Consistent

Processes should be in place to ensure consistency of the definition, generation/capturing and management (including migration) of data throughout the data life cycle. Processes should be implemented to minimise the risk of contradictions e.g. by the use of standardisation, data validation and appropriate training.

Enduring

Data should be maintained appropriately such that they remain intact and durable through the entire data life cycle, as appropriate, according to regulatory retention requirements. (See section on back-up and archiving: 6.8).

Available when needed

Data should be stored at all times in order to be readily available for review when needed.

Traceable

Data should be traceable throughout the data life cycle. Any changes to the data, to the context or metadata should be traceable, should not obscure the original information and should be explained, if necessary. Changes should be documented as part of the metadata (e.g. audit trail).

4.6. Criticality and risks

ICH-GCP E6(R2) introduces the need for a quality management system with a risk-based approach. Risks should be considered at both the system level e.g. standard operating procedures (SOPs), computerised systems and staff, and for the specific clinical trial e.g. trial specific data and data collection tools or trial specific builds/configurations of systems.

Risks in relation to the use of computerised systems and especially those related to the assurance of data integrity should be identified, analysed and mitigated or accepted throughout the system life cycle. Where applicable, mitigating actions include revised system design, configuration or customisation, increased system qualification or revised SOPs for the use of systems and data governance culture.

In general, risks should be determined based on system used, operator, use of system and data involved. High-risk component parts of any system should always be addressed. For example, a component part of an IRT system that calculates IMP dose based on data input by the investigator would be high risk compared to other functionality such as generation of an IMP shipment report. The complicity between each component should be taken into consideration.

All data collected in the context of an approved clinical trial should be reliable. Consequently, the arrangements for data governance to ensure that data, irrespective of the format in which they are generated, are recorded, processed (including analysis, alteration/imputation, transformation or migration), used, retained (archived), retrieved and destroyed should be considered for data integrity risks and appropriate control processes implemented.

The approach used to reduce risks to an acceptable level should be proportionate to the significance of the risk. Risk reduction activities may be incorporated in protocol design and implementation, system design, build and validation, monitoring plans, agreements between parties defining roles and responsibilities, systematic safeguards to ensure adherence to SOPs, training in processes and procedures etc.

The identification of the most effective and efficient risk-based control, including periodic review of the data and metadata can be determined and implemented.

There are special risks to take into consideration when activities are contracted out. These are further elaborated in Annex 1 on contracts.

4.7. Performing data capture in clinical trials

The approved clinical trial protocol should specify which data is to be generated/captured by whom and when and which tools or procedures are to be used.
The protocol should identify any data to be recorded directly into the eCRFs and considered to be source data (ICH-GCP 6.4.9). This is equally applicable to other specific data collection systems, such as ePRO. Data directly captured in these tools without prior identification in the protocol to be source data is considered as GCP-noncompliant.

Tools used to generate, capture, transfer, manipulate or store data such as a CRF and other instruments such as COA and trial participant diary tools which report clinical data to the sponsor should be an accurate representation of the protocol ensuring capture and transfer of only the data as specified within the protocol.

The sponsor and investigator should maintain a record of the location(s) of their respective essential documents including source documents (ICH-GCP 8.1). Investigators should document source data consistently in accordance with the source data location list.
The source data and their respective capture methods should be clearly defined prior to the recruitment of the trial participants.

A detailed diagram and description of the transmission of electronic data should be available. The sponsor should describe which data will be transferred and in which format, the origin and destination of the data, the parties with access to the transferred data, the timing of the transfer and any actions that may be applied to the data, for example, data validation, reconciliation, verification and review. The use of a data management plan (DMP) is strongly encouraged.

Any data generated/captured and transferred to the sponsor or CRO that is not stated in the protocol or related documents is considered GCP-noncompliant.

There is no requirement or expectation that the sponsors and investigators use computerised systems to collect data; however, the use of electronic data collection (EDC) tools if implemented and controlled to the described standard, offers a wide variety of functions to improve data completeness, consistency and unambiguity, e.g. automatic edit checks, validation checks, assisting information and workflow control.

4.8. Electronic signatures

Whenever an electronic signature is used within a clinical trial to replace a wet-ink signature required by GCP, the electronic signature functionality should meet the expectations stated below regarding *authentication*, *non-repudiation*, *unbreakable* link and *timestamp* of the signature:

The system should thus include functionality to 1) *authenticate* the signatory, i.e. establish a high degree of certainty that a record was signed by the claimed signatory, 2) ensure *non-repudiation*, i.e. that the signatory cannot later deny having signed the record, 3) ensure an *unbreakable link* between the electronic record and its signature, i.e. that the contents of a signed (approved) version of a record cannot later be changed by anyone without automatically being rendered visibly un-signed (un-approved), and 4) provide a *timestamp*, i.e. that the date, time and time zone when the signature was applied is recorded.

Electronic signatures can further be divided into two groups depending on whether the identity of the signatory is known in advance or not; i.e. signatures executed in *closed* and in *open* systems.

For *closed* systems which constitute the majority of systems used in GCP and which are typically provided by the sponsor, a CRO or an investigator, the system owner knows the identity of all users and signatories and has full control over these. The electronic signature functionality in these systems should be proven during system qualification to have the qualities mentioned above.

However, EU Regulation 910/2014 (“eIDAS”) on electronic identification and trust services for electronic transactions is not applicable for closed systems (“eIDAS” clause 21 and article 2.2).

For *open* systems, the signatories (and users) are not known in advance, and hence, identification of a signatory should be based on a personal qualified certificate for electronic signatures. Implementation of electronic signatures in open systems should meet EU Regulation 910/2014 (“eIDAS”).

A special case of electronic signatures is *hybrid electronic signatures*, where electronic records in a computerised system are signed using wet-ink signatures on paper. In this case, it follows from the above that there should be an unbreakable link between the electronic record in the computerised system and the signature page on paper, e.g. by means of a checksum (hash code) calculated for the electronic record and printed by the system on the signature page.

Biometric approaches are currently not specifically addressed by ICH-GCP E6(R2). If using biometrics instead of signature or e-signature, investigator and sponsor should ensure that these fulfil the above mentioned requirements and local legal requirements.

4.9. Data protection

"The confidentiality of records that could identify trial participants should be protected, respecting the privacy and confidentiality rules in accordance with the applicable regulatory requirement(s)." (ICH-GCP 2.11). The requirements of Regulation (EU) 2016/679 (General Data Protection Regulation) on the protection of individuals with regard to the processing of personal data and on the free movement of such data should be followed except when specific requirements are implemented for clinical trials e.g. that a trial participant does not have the right to be forgotten (and consequently data deleted) as this would cause bias to e.g. safety data (Regulation 536/2014 recital 76). Trial participants should not be asked to waive their rights by informed consent processes (ICH-GCP section 4.8.4.).

In accordance with Union data protection legislation, the location of personal data processed (both at rest and in transit) must be within the EU/EEA. If personal data is transferred to a third country or international organisation, such data transfer must comply with applicable Union data protection. In summary, this means that the transfer must be either carried out on the basis of an adequacy decision (Article 45 of GDPR, Article 47 of EUDPR), otherwise the transfer must be subject to appropriate safeguards (as listed in Article 46 of GDPR or Article 48 of EUDPR) or the transfer may take only if a derogation for specific situations apply (under Article 49 of GDPR or Article 50 of EUDPR).

4.10. Validation of systems

All computerised systems used within a clinical trial should be subject to processes that confirm that the specified requirements of a computerised system are consistently fulfilled and that the system is fit for purpose. Validation should ensure accuracy, reliability and consistent intended performance, from design until decommissioning of the system or transition to a new system.

The processes used for the validation should be decided upon by the system owner (e.g. sponsors, investigators, technical facilities) and described, as applicable. System owners should ensure adequate oversight of validation activities and documentation (thereon) performed by contracted parties to ensure suitable procedures are in place and that they are being adhered to.

Documentation (including information within computerised systems used as process tools for validation activities) should be maintained to demonstrate that the system is maintained in the validated state. Such documentation should be available for both the validation of the software and for validation of the trial-specific configuration.

Validation of the trial-specific configuration should ensure that the system is consistent with the requirements of the approved clinical trial protocol and robust testing of functionality implementing such requirements is undertaken, for example, eligibility criteria questions in an eCRF, randomisation strata and dose calculations in an IRT system.

See Annex 2.4 for further detail on validation.

4.11. Direct access to computerised systems

All relevant computerised systems should be readily available and directly accessible (this requires a unique username and password) upon request by inspectors of regulatory authorities. If a computerised system is de-commissioned, direct access (with personal username and password) to the data should be still ensured (see section 6.11).

5. Computerised systems

Requirements for validation are described in section 4.10 and Annex 2, requirements for user management in Annex 3 and requirements for IT security in Annex 4 of this guideline.

5.1. Keeping a description of computerised systems

The responsible party should maintain a list of physical and logical location of the data e.g. servers, functionality and operational responsibility for computerised systems and databases used in a clinical trial together with an assessment of their fitness for purpose.
Where multiple computerised systems/databases are used, a clear overview should be available so the extent of computerisation can be understood. System interfaces should be described, defining how the systems interact, including validation status, methods used and implemented security measures.

5.2. Maintaining written procedures for the use of computerised systems

Written procedures should be in place to ensure correct use of computerised systems. GCP requires that sponsors maintain SOPs for using computerised systems (see ICH-GCP 5.5.3b).

5.3. Training requirements for computerised systems

"Each individual involved in conducting a clinical trial should be qualified by education, training, and experience to perform his or her respective task(s)." (ICH-GCP 2.8). This also applies to training in computerised systems. Systems and training should be designed to meet the specific needs of the users (e.g. in sponsors/CROs and investigator). Special considerations should be considered regarding training of trial participants where they are users (see also Annex 5, section A5.3).

There should be training on the relevant aspects of the legislation and guidelines for those involved in developing, building and managing trial specific computerised systems, for example, those employed at a contract organisation providing eCRF, IRT, ePRO, trial-specific configuration and management of the system during the clinical trial conduct.

All training should be documented, and the records retained in the appropriate part of the investigator site file/sponsor TMF.

5.4. Security

To maintain data integrity and protection of the rights of trial participants, computerised systems, used in clinical trials, should have security processes and features to prevent unauthorised access and accidental or deliberate data changes and maintain blinding of the treatment allocation where applicable. Checks should be used to ensure that only authorised individuals have access to the system and appropriate permissions (e.g. ability to enter or make changes to data). Records of authorisation of access to the systems, with the respective levels of access clearly documented should be maintained. The system should record changes to user roles and thereby access rights and permissions.

There should be documented training on the importance of security e.g. the need to protect and not to share passwords as well as enforcement of security systems and processes and identification and handling of serious breaches.

See Annex 4 for further guidance on IT security.

6. Electronic data

For each trial, it should be identified what electronic data and records will be collected, modified, imported and exported, archived and how they are retrieved and transmitted. Electronic source data, including its audit trail should be directly accessible to investigators, monitors, auditors and inspectors without compromising the confidentiality of participants' identities (ICH-GCP 1.21).

6.1. Data capture and location

The primary goal of data capture is to collect all data required by the protocol. All pertinent observations should be documented in a timely manner. The location of all source data should be specified prior to the start of the trial and updated during the conduct of the trial where applicable. (ICH-GCP 8.1. Addendum)

6.1.1. Transcription from paper to electronic format

Source data collected on paper (e.g. worksheets, paper CRFs or paper diaries or questionnaires) need to be transcribed either manually or by a validated entry tool into the EDC system or database(s). In case of manual transcription, risk-based methods should be implemented to ensure the quality of the transcribed data (e.g. double data entry and/or data monitoring)..

6.1.2. Transfer from electronic sources

Study data are transferred in and between systems on a regular basis. All file and data transfers need to be validated and should ensure that data and file integrity is assured for all transfers.

Data that is collected from external sources and transferred in open networks should be protected from unwarranted changes and secured/encrypted in a way which preclude disclosure of confidential information.

All transfers that are needed during the conduct of a clinical trial need to be pre-specified.

Qualification/validation of transfer should include appropriate challenging test sets and ensure that the process is available and functioning at clinical trial start (e.g. to enable ongoing sponsor review of diary data, lab data or adverse events by safety committees). Data transcribed or extracted and transferred from electronic sources and their associated audit trail should be continuously accessible (according to delegated roles and corresponding access rights) by the sponsor for ongoing review and by the investigator for the entire clinical trial and retention period (ICH-GCP 8.1).

Transfer of source data and records where the original data or file is not maintained is a critical process and appropriate considerations are expected in order to prevent loss of data and metadata.

6.1.3. Direct data capture

Direct data capture also can be done by using electronic data input devices and applications such as electronic diaries, electronic questionnaires and eCRFs for direct data entry. Where treatment-related pertinent information is captured first in a direct data capture tool such as a trial participant diary, a PRO form or a special questionnaire, a written procedure should exist to transfer or transcribe information into the medical record, when relevant. Please also refer to Annex 5.

Direct data capture can be done by automated devices such as wearables or laboratory or other technical equipment (e.g. medical imaging, ECG equipment) that are directly linked to an EDC tool. Such data should be accompanied by metadata concerning the device used (e.g. device version, device identifiers, firmware version, last calibration, data originator, UTC time stamp of events).

6.1.4. Data entry checks

Computerised systems should validate manual and automatic data inputs to ensure a predefined set of validation criteria is adhered to. Data entry checks should be relevant for the protocol and developed and revised as needed. Data entry checks should be validated and implementation of the individual data entry checks should be controlled and documented. If data entry checks are paused at any time during the trial, this should be documented and justified. Data entry checks could be either immediately at data entry (edit checks), run automatically during defined intervals (e.g. daily) or manual.

6.2. Audit trail and audit trail review

6.2.1. Audit trail

An audit trail should be enabled for the original creation and subsequent modification of all electronic data (ICH-GCP 2.10, 4.9.0, 4.9.3 and 5.5.3.c). In computerised systems, the audit trail should be secure, computer generated and time stamped (e.g. UTC).

An audit trail is essential to ensure that changes to the data are traceable. Audit trails should be robust, and it should not be possible for "normal" users to deactivate them. If possible, for an audit trail to be de-activated by "admin users", this should automatically create an entry into a log file (e.g. audit trail). Entries in the audit trail should be protected against change, deletion, and access modification (e.g. edit rights, visibility rights). The audit trail should not be stored outside the system. The responsible investigator, sponsor, and inspector should be able to review and comprehend the audit trail and therefore audit trails should be in a humanly readable format.

Audit trails should be visible at data-point level in the live system and the entire audit trail should be available as an exported dynamic data file in order to allow for identification of systematic patterns or concerns in data across trial participants, sites etc. The audit trail should show initial entry and changes (value - previous and current-) made to what (field, data identifiers) by whom (username, role, organisation), when (date/time stamp), why (reason for change) in a GCP compliant manner.

A procedure should be in place to address the situation when a data originator (e.g. investigator or trial participant) realises that she/he has submitted incorrect data by mistake and wants to correct the recorded data.
It is important that original electronic entries are visible or accessible (e.g. in the audit trail) to ensure the changes are traceable. The audit trail should record all changes made as a result of data queries or a clarification process. The clarification process for data entered should be described and documented. Changes to data should only be performed when justified. Justification should be documented. In case the data originator is the trial participant, special considerations to data clarifications might be warranted. See Annex 5 section A5.1.1.41 for further details.

For certain types of systems (e.g. ePRO) data entered may not be uploaded immediately but may be temporally placed in local memory. Such data should not be edited or changed without the knowledge of the data originator prior to saving. Any changes or edits should be acknowledged by the data originator, should be documented in an audit trail and should be part of validation procedures. UTC date of data entry into the capture tool (e.g. eCRF) and UTC date of data saved to a hard drive should be recorded as part of the metadata. The duration between initial capture in local memory and upload to a central server should be short and traceable (i.e. transaction time), especially in case of direct source data entry.

Data extracts or database extracts for internal reporting and statistical analysis do not necessarily need to contain the audit trail information. However, the database audit trail should capture the generation of data extracts and exports.

Audit trails should capture any changes in data entry per field and not per page (e.g. CRF page). Where edit checks result in a change of data, the edit check should be part of the change rationale captured by the audit trail/event log.

In addition to audit trail, metadata could also include (among others) review of access logs, event logs, queries etc.

Access logs, including user name and user role, are in some cases to be considered important metadata and should consequently be available. This is considered necessary e.g. for systems that contain critical unblinded data.

Care should be taken to ensure that information jeopardising the blinding does not appear in the audit trail accessible to blinded users.

6.2.2. Audit trail review

Procedures for risk-based trial specific audit trail reviews should be in place and performance of data review should generally be documented. Data review should focus on critical data. Data review should be proactive and ongoing review is expected unless justified. Manual review as well as review by the use of technologies to facilitate review of larger datasets should be considered. Data review can be used to (among others) identify missing data, detect signs of data manipulation, identify abnormal data/outliers and data entered at unexpected or inconsistent hours and dates (individual data points, trial participants , sites), identify incorrect processing of data (e.g. non-automatic calculations), detect unauthorised accesses, detect device or system malfunction and detect if additional training is needed for trial participants /site staff etc. Audit trail review can also be used to detect situations where direct data capture has been defined in the protocol but where this is not taking place as described.

In addition to audit trail review, metadata review could also include (among others) review of access logs, event logs, queries etc.

The investigator should receive an introduction on how to navigate audit trail of own data in order to be able to review changes.

6.3. Sign-off of data

The investigators are responsible for data entered into eCRFs and other EDC tools under their supervision (electronic records). Those data should be reviewed and signed-off.

The signature of the principal investigator (PI) or authorised member of the investigator’s staff is considered as the documented confirmation that the data entered in the eCRF and submitted to the sponsor are attributable, legible, original, accurate, and complete and contemporaneous (ICH-GCP 4.9.1.). Any member of the staff authorised for sign-off (as per ICH-GCP 8.3.14) should be qualified to do so in order to fulfil the purpose of the review as described below. National law could dictate specific responsibilities, which should then be followed.

The acceptable timing and frequency for the sign-off needs to be defined and justified for each trial by the sponsor and should be determined by the sponsor on a risk-based manner. The sponsor should consider trial-specific risks and provide a rationale for the risk-based approach. Points of consideration are types of data entered, non-routine data, importance of data, data for analysis, length of the trial and the decision made by the sponsor based on the entered data, including the timing of such decisions. It is essential that data are confirmed prior to interim analysis and the final analysis and that important data related to e.g. reporting of SAEs, adjudication of important events and endpoint data, DSMB review, are signed off in a timely manner. In addition, a timely review and sign-off of data that are entered directly into the CRF as source is particularly important.

Therefore, it will rarely be sufficient to just implement one signature immediately prior to database lock. Signing of batches of workbooks is also not suited to ensure high data quality and undermines the purpose of timely and thorough data review.

For planned interim analysis, e.g. when filing a marketing authorisation application, all submitted data (e.g. eCRF pages) need to be signed off by the investigator or her/his designated and qualified representative before extracting data for analysis. The systems should be designed to support this functionality.

To facilitate timely data review and signing by the investigator or her/his designated representative, the design of the EDC tool should be laid out to support the signing of the data at the defined time points. Furthermore, it is important that the PI reviews the data on an ongoing basis in order to detect shortcomings and deficiencies in the trial conduct at an early stage, which is the precondition to undertake appropriate corrective and preventive actions.

Adequate oversight by the PI is a general requirement to ensure participant safety and data quality and integrity. Oversight can be demonstrated via various means, one of them being review of reported data. Lack of investigator oversight may prevent incorrect data from being corrected in a timely manner and necessary corrective and preventive actions being implemented at the investigator site.

6.4. Copying data

Data can be copied or transcribed for different purposes, either to replace source documents or essential documents or to be distributed amongst different stakeholders as working copies. If essential documents or source documents are irreversibly replaced by a copy, the copy should be certified (ICH-GCP 1.63). See section 6.5.

Copies should contain a faithful representation of the data and contextual information. Source documents and data should allow accurate copies to be made. The method for copying should be practical and should ensure that the resulting copy is complete and accurate, including relevant metadata. See also "Guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic), (EMA/INS/GCP/856758/2018), section 5 for further details on definition.

6.5. Certified copies

When creating a certified copy, the nature of the original document needs to be considered. For example, the content of the file is either static (e.g. PDF document) or dynamic (e.g. worksheet with automatic calculations) or the copy tries to capture the result of an interpreter (e.g. a web page, where a web-browser interprets written hypertext mark-up language (HTML), JavaScript among other programming languages). Either way the result of the copy process should be verified either automatically by a validated process or by hand to ensure to have the same information, including data that describe the context, content and structure, as the original.

In case of dynamic files e.g. when a database is decommissioned and copies of data and metadata is provided to sponsors, the resulting file should capture also the dynamic aspects of the original file. In case of files, which are the result of an interpreter, special care needs to be taken not only to consider the informative content of such a file, but also to capture and preserve aspects that are the results of the interactions of the used interpreter(s) and systems settings during the display. For example, window size, browser type, operating system employed and the availability of software dependences (e.g. Java Scripts enabled) can influence the structure and content displayed. Special considerations should be taken whenever copies are to replace original source documents, since (any) deviations of information, including data that describes context, content and structure would be considered GCP non-compliant.

6.6. Hosting and control of data

All data generated at the clinical trial site relating to the trial participants should be available to the investigator at all times during and after the trial. The sponsor should not have exclusive control of the data entered in a computerised system at any point in time. All data held by the sponsor that has been generated in a clinical trial should be verifiable to a copy of these data that is not held (or that has not been held) by the sponsor.

The requirements above are not met if data are captured in a computerised system and the data are stored on a central server under the sole control of the sponsor or under the control of a contracted party that is not considered to be independent from the sponsor or if the sponsor is distributing the data to the investigator instead of the independent third party. This is because the investigator does not hold an independent copy of the data and therefore the sponsor has exclusive control of the data. In order to meet the requirements, the investigator should be able to download a contemporaneous certified copy of the data. This is in addition to the record maintained at an independent third party.

Data entered to EDC tools by the investigator should be available to the investigator throughout the whole legally mandated duration and for the full duration of local legal requirements. This can be ensured either by contemporaneous local copies at the trial site or e.g. by the use of an independent third party. Access to the data may be amended to read only as part of the database lock process. Prior to read-only access to the investigator being revoked, a copy including audit trail should be made available to the investigator in a complete and comprehensive way. In the situation where an independent third party is hosting the data. the copy should not be provided via the sponsor, as this would temporarily provide the sponsor with exclusive control over the data and thereby jeopardise the investigator’s control. Copies should not be provided in a way that requires advanced technical skills by the investigators. The period between provision of the copy to the investigator and the closure of the investigators’ read only access to the database(s) should allow sufficient time for the investigator to review the copy and access should not be closed until such a review has been performed.

Any contractual agreements regarding hosting should ensure investigator control. If the sponsor is arranging hosting on behalf of the investigators by an independent third party, contracts should ensure the level of investigator control mentioned above.
Investigators delegating hosting of such data to third parties themselves should ensure that the intended use is covered by local legal requirements and in-house rules of the institution.

6.7. Cloud solutions

Irrespective whether a computerised system is installed at the premises of the sponsor, investigator, another party involved in the trial or whether it is made available by a contracted party as a cloud solution, the requirements in this guideline are applicable. There are, however, specific points to be considered as described below.

Cloud solutions cover a wide variety of services related to the computerised systems used in clinical trials. These can range from Infrastructure as a service (IaaS) over Platform as a service (PaaS) to Software as a service (SaaS). Common for these services is, that they provide sponsors and investigators, on-demand availability of computerised system resources over the internet, without having the need or even possibility to directly manage these services.

In case of cloud solution being used the sponsor (ICH-GCP 5.2.1) and/or of the investigator (ICH-GCP 4.2.6) should ensure that the contracted party providing the cloud is qualified (see Annex 4).

By buying in cloud computing, the sponsor and/or investigator are at a certain risk, because many services are managed less visibly by the cloud provider.
Contractual obligations with the cloud solution provider should be detailed and explicit and refer to all GCP relevant topics and to all relevant legal requirements (see Annex 1).

Data jurisdiction may be complex given the nature of cloud solutions and services being shared over several sites, countries and continents; however, any uncertainties should be addressed and solved by contractual obligations prior to the use of a cloud solution.
If the responsible party choses to perform his own qualification of the computerised system, the cloud provider should make a test environment available which is identical to the production environment.

6.8. Adequate back-up of data

Data stored in a computerised system are susceptible to system malfunction, intended or unintended attempts to alter or destroy data and physical destruction of media and infrastructure and are therefore at risk to be lost. Data and configurations should be regularly backed up. Please also refer to Annex 4 for further details on IT security.

The use of replicated servers is strongly recommended. Back-ups should be stored in separate physical locations and logical networks and not behind the same firewall as the original data to avoid simultaneous destruction or alteration.

Frequency of backups (e.g. hourly, daily, weekly) and their retention (e.g. a day, a week, a month) should be determined through a risk-based approach.

Checks of accessibility to data, irrespective of format, including relevant metadata, should be undertaken to confirm that the data are enduring, continue to be available, readable and understandable by a human being. There should be procedures in place for risk-based (e.g. in connection with major updates) restore test from back up of the complete database(s) and configurations and the performed restore tests should be documented.

Disaster mitigation and recovery plans should be in place to deal with events, which endanger data security. Such plans should be regularly reviewed. Disaster mitigation and recovery plans should be part of the contractual agreement where the sponsor subcontracts.

6.9. Migration of data

Migration as opposed to transfer of data (as described in section 6.1.2) is the process of permanently moving existing data (including metadata) from one system into another system e.g. migration of individual safety reports from one safety database to another. It should be ensured that the migration does not adversely affect existing data and metadata.

In the course of design or purchase of a new system and of subsequent data migration from an old system, qualification of the data migration process should have no less focus than qualification of the system itself.

The qualification of data migration should take into consideration the complexity of the task and any foreseen possibilities that may exist to verify the migrated data (e.g. checksum, case counts, quality control of records).

Prior to migration, this process should be planned in detail. A risk analysis identifying the most probable risks should take place and should yield appropriate mitigation strategies. After the planning, the intended procedure should be validated with mock data and results should be considered for risk-assessment and mitigation. A data verification focused on key data should be performed post migration.

Verification of migrated data can be simple or rather complex, depending on the different platforms and systems involved. Regardless of effort needed, the migration process should be documented in such detail that throughout all data operations/transformations data changes remain traceable. Mapping from the old system onto the new system should be retained.

Data, contextual information and audit trail should not be separated. In case migration of data into a new system results in a loss of relevant data, adequate mitigating actions should be taken to establish a robust method to join audit trail and data for continuous access by all stakeholders. A detailed explanation is expected, why no system was available, which allowed migration of data and audit trail. Arrangements should ensure that the link between data and metadata can be established. If several parties are involved, contracts should be in place to ensure this.

6.10. Archiving

The investigator and sponsor should be aware of the required retention periods for clinical trial data and essential documents, including metadata. Retention periods should respect the data protection principle of storage limitation. Clinical trial management systems (e.g. TMF) should be in place to keep an inventory of all essential data and documents and corresponding retention periods. It should be clearly defined which data is related to each clinical trial activity and where this record is located and who has access/edit rights to the document. Security controls should be in place to ensure data confidentiality, integrity and availability.

It should be verified that the file remains accessible and depending on the media used for storage and available software through the retention period. This could imply e.g. migration of data (see section 6.9).

Suitable archiving systems should be in place to safeguard the data integrity for the periods established by the regulatory requirements including those in any of the regions where the data may be used for regulatory submissions, and not just those of the country where the data are generated.

Source documents and data should always be available when needed to authorised individuals to meet their regulatory obligations. For direct access please refer to section 4.6.

Data should be maintained in a secure manner and should only be transferred between different (physical) locations in a validated process. Data should be archived in a read only state.

6.11. Database decommissioning

After the finalisation of the trial, the database(s) might be decommissioned. It is recommended that the time of decommissioning is decided taking into consideration e.g., whether or not the clinical trial will be used in the terms of a marketing authorisation application in the near future in which case it could be recommended to keep the database(s) live. A dated and certified copy of the database(s) and data should be archived and available on request. In case of decommissioning, the sponsor should ensure (contractually if done by a contracted party) that archived formats provide the possibility to restore the database(s). This includes restoring of dynamic functionality and all relevant metadata (audit trail, event logs, implemented edit checks, queries, user logs etc.). Where recommissioning is no longer possible, the sponsor should ensure that all the data including metadata files (e.g. audit trails) is available in dynamic data files. The sponsor should review the system to determine the audit trails and logs available in the system and how these would be retained as dynamic files. Where a third party is involved, this should be addressed in the contractual arrangements. Static formats of dynamic data will not be considered adequate. See definitions section regarding static and dynamic formats.

Annex 1 Contracts

Sponsors and investigators outsource an increasing number of tasks in clinical trials, especially in the area of computerised systems where the responsible party might lack internal knowledge or resources or they wish to purchase a product or a service that has been used by others. Sponsors/investigators can delegate tasks to an accomplished third party, but nevertheless the full responsibility for the data integrity, security and confidentiality resides with the sponsor/investigator. (ICH-GCP 4.2.6 and 5.2.1)

Contracts can cover a variety of tasks such as system and trial specific build, provision of license to an application, full clinical trial service including data management tasks e.g. site contact, training, data clarification processes etc., but could also be restricted to hosting services.

The responsible party should ensure that the distribution of tasks is clearly documented and agreed on. It should be ensured that each party has the control of and access to data and information that their legal responsibilities require and that the ethics committees and regulatory authorities approving trials have been properly informed of these activities as part of the clinical trial application process. This should be carefully documented, in the protocol, procedures, contracts or agreements and other documents. It is important to consider who is providing and controlling the computerised system being used. In general, tasks including handling of data under the responsibility of the investigator can only be performed by parties, contractually obligated to the institution or investigator and data under the responsibility of the sponsor can only be handled by parties contractually obligated to the sponsor.

Clear contracts should be in place and appropriately signed by all involved parties prior to provision of services or systems. Contracts should be maintained/updated as appropriate. Sub-contracting and conditions for sub-contracting should be specified.

The responsible parties should ensure oversight of these trial-related duties e.g. by review of defined key performance indicators (KPI) or reconciliations.

If appropriate contracts cannot be put in place, e.g. because a contracted party does not allow provision of e.g. access to system requirements specifications, pre-qualification audits or access for GCP inspectors, systems from such a vendor shall not be used in clinical trials.

All parties involved in the conduct of the clinical trial should comply with ICH-GCP and this includes vendors of computerised systems. Therefore, any relevant standards to be followed, e.g. clinical trial legislation and guidance should be specified in the contract. A number of the tasks involve access to, review, collection and/or analysis of data, much of it personal/pseudonymised data. In addition, in specific cases contact with (potential) trial participants and consequently data protection legislation needs to be followed, in addition to the clinical trial legislation and guidance.

The protocol, implicitly, defines part of the specification for system build and there should be consistency between the protocol and the wording of the contract. In addition, it should be clear how subsequent changes to the protocol are handled so that the vendor can implement changes to the computerised system appropriately.

It should be clear from contracts which tasks are delegated also in relation to retaining essential documentation for performed activities. In the context of clinical trials, the retention period for system-documentation (including e.g. software/system validation documentation, vendor standard operating procedures (SOPs), training records, issues log/resolutions) as well as Trial Master File (TMF) documentation related to the individual clinical trial (including e.g. helpdesk tickets or meeting minutes) is considerable. It should be clear from the contract which party is retaining and maintaining which documentation and how and in what format that documentation is made available when needed e.g. for an audit or an inspection. There should be no difference in availability of documentation irrespective of whether the documentation is held by the sponsor/investigator or a contracted (or sub-contracted) party.

The responsible party is ultimately responsible for e.g. the validation and operation of the computerised system and for providing adequate documented evidence of applicable processes.

Responsible parties should be able to provide the GCP inspectors of the EU/EEA authorities with access to the requested documentation regarding the qualification, validation and operation of computerised systems irrespective of who performed these activities.

It should be specified in contracts that the sponsor or the institution, as applicable, should have the right to conduct audits at the vendor site and that the vendor site could be subject to inspections (by national and/or international authorities) and shall accept these.

The sponsor has a responsibility to escalate serious breaches, including important security breaches, to authorities within short timelines. To avoid undue delay in sponsor reporting from the time of discovery e.g. by a vendor, contracts should specify which information should be escalated and within which (short) deadlines.

As set out in ICH-GCP 8.1 to ensure that the investigator, rather than the sponsor, maintains control over their data, it should be specified in contracts how investigators' access to and control over data is ensured during and after the trial and the revocation of investigator access to data in case of decommissioning should be described. It should also be specified which outputs the involved parties (e.g. sponsor and investigators) will receive during and after the clinical trial and in which formats.

Arrangements about decommissioning of the database(s) should be clear, including the possibility to restore the database(s) to full functionality (including dynamic features) for instance for inspection purposes.

The contracts should address expectations regarding potential system "down-time" and the preparation of contingency plans.

Tasks contracted out could include hosting of data. If data are hosted by a vendor, location of data storage and control of this (e.g. use of cloud services) should be described.

To ensure reliable access to the data, the sponsor/investigator should employ measures to guarantee access to data for the sponsor and investigator in case of foreclosure (bankruptcy), shutdown, disaster of the vendor or for other reasons chosen by the sponsor/investigator (e.g. change of vendor).

Special consideration should be given on training and quality systems. Vendors accepting tasks on computerised systems should not only be knowledgeable on computerised systems and data protection legislation, but also on GCP requirements, quality systems, etc.

Further details on contracts with IT vendors are set up in related Q&A documents.

Annex 2 Computerised systems validation

A2.1 Establishing requirements and ensuring documenting consistent intended performance (validation)

All responsible parties should ensure appropriate qualification and validation, as per ICH-GCP 5.5.3a, "*the sponsor should ensure and document that the electronic data processing system(s) conforms to the sponsor' established requirements for completeness, accuracy, reliability, and consistent intended performance (i.e. validation)*". Similarly, investigators or institutions are expected to demonstrate that their computerised systems meet the requirements defined in ICH-GCP 4.9.0.

Validation should include validation of the core software by the vendor for a commercial of the shelf (COTS) and/or software as a service (SaaS) or validation of the software developed by the sponsor or investigator (including the use of open source) and of its subsequent configuration. A further validation may be required where the installed software is then used for specific trials requiring a configuration or build based on the requirements of a specific trial.

The sponsor (or the investigator in case of a system implemented by the investigator's institution) is ultimately responsible for the validation of the computerised systems used in clinical trial processes. They may rely on qualification documentation provided by the vendor if the qualification activities performed by the vendor have been assessed as adequate, but may also have to perform additional qualification/validation activities based on a documented risk-assessment e.g. during pre-qualification audits.
Where the responsible party is using a system (as intended) from a vendor, including the built-in possibilities for configuration, the considerations as described below should be taken into account. Different requirements will apply in cases where the software is changed, or functionalities are added to the system. The system in question may be a system validated by the supplier, but installed at the sponsor/institution, or a system provided as SaaS.

For the responsible party to use the vendor's qualification documentation, they should have a thorough knowledge about the vendor's quality system and qualification activities, which could usually be obtained through an in-depth assessment/audit. This assessment/audit should be performed by qualified staff, with sufficient time spent on the activities and with cooperation from the vendor. The assessment/audit should go sufficiently deep into the actual activities, and a suitable number of examples for relevant activities should be assessed (and documented). The assessment/audit report should document the vendor's qualification documentation to be satisfactory or shortcomings should be mitigated by the responsible party – e.g. by them performing part of the qualification. The responsible party, or where applicable the contract research organisation (CRO) performing these activities for them, should have a detailed knowledge about the qualification documentation and should be able to navigate through it and explain the activities as if they had performed the activities themselves.

As described in Annex 1 on contracts, the qualification documentation should be made available to the inspectors in a timely manner when requested during an inspection, irrespective of whether it is provided by the responsible party, a CRO or the vendor of the system.

Both the responsible party and the vendor should establish full configuration management for qualification and production environments and should be able to fully account for any differences between the vendor's validation environment and the responsible party's production environment. In case of differences, the responsible party should justify that these are considered insignificant.

The responsible party should perform an Installation Qualification/Performance Qualification (IQ/PQ) where the system depends on trained users.

Interfaces between the electronic case report form (eCRF) and other systems should be clearly defined and validated e.g. import of item response theory data, automatically generated emails to safety mailboxes etc.
Documentation supporting the validation of trial specific configurations/builds (e.g. edit checks, auto-calculations) are considered essential documents that form part of the TMF. The documentation for the software validation is also essential and should be retained to be made available, although not required to be in the TMF (see "Guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic), (EMA/INS/GCP/856758/2018)?)
Changes to systems are described in section A.2.8.

A2.2 Requirements documentation (URS, trial specific, edit check specifications)

Independently on whether a system is developed on request by the sponsor/institution, following the traditional V-model or agile principles, is purchased as a COTS product, or is provided as SaaS, all system functionalities intended to be used (including requirement for regulatory authorities' access/review) should be described in a requirements specification, often called a user requirements specification (URS). The URS should form the basis for system design, purchase customisation and configuration, but also for system qualification). In addition, other specification documents should be generated. For example, the use of the software for a trial specific build or configuration will also require specification documentation to be produced. This should make reference to the clinical trial protocol and version for which it was designed. The software development additional documents for functional and design specifications are produced.

The specification documentation should cover all functionality used by or relied on by the sponsor/investigator, including but not limited to operational, functional, data, technical, interface, performance, availability, security, and regulatory requirements.

The sponsor/investigator should take responsibility for the URS. This document should always be reviewed and approved by the sponsor/investigator.

The responsible party should ensure availability of qualification documentation. In case the responsible party cannot rely on a vendor to provide documentation, the responsible party has to requalify the system on the basis of their own and of the vendor's system requirement specifications.
Other specification documentation should be reviewed and approved by the sponsor/investigator as appropriate. For example, where the software is configured for the sponsor's/investigator's use or for trial specific configurations/builds the documentation should be reviewed by the responsible party; however, for COTS or SaaS software the review and approval of the responsible party could be limited to the URS.
The specification documentation should be maintained and updated throughout the system full life cycle as requirements to the system change. For example, there may be software enhancements, bug fixes and for trial specific configurations/builds there could be changes required from protocol amendments. The rationale for such changes to the specification documentation should be documented as part of the change control process.

A2.3 Requirements traceability matrix

For complex systems with a large number of requirements, it is not feasible to keep track of requirements and their corresponding test cases without having a systematic approach of documenting this, e.g.

traceability matrix. This document may have many forms and the process may even be automated by software, but it should be created during system development and qualification and be continuously updated as requirements are changed to ensure that for every requirement, there is at least one corresponding test case.

A2.4 Validation plans and test plans/scripts/cases

Validation activities should be planned and documented, for example validation plan and test plan. Test cases and individual test steps should be pre-approved and conducted accordingly. This is required for validation of both core software and trial specific configurations/builds.

Test cases may have many formats and while typically consisting of textual documents including tables with multiple columns corresponding to the elements below, they may be designed and contained in dedicated test management systems, which may even allow automatic execution of test cases (e.g. regression testing). However, expectations to key elements are the same.
Test cases should include exact reference to requirement identity, version of the software being tested (target), any pre-requisites or conditions prior to conducting the test, description of the step taken to test the functionality (input), expected result (acceptance criteria), and require the user to document the actual result as seen in the test step, evidence, if relevant (screen shot), conclusion of the test step (pass/fail), and deviation impact assessment and subsequent decisions regarding the deviations (if applicable).

Test cases for trial specific configurations/builds should ensure that the system meets the specification documentation and therefore the clinical trial protocol requirements.

A2.5 Test execution and reporting

Test execution should follow pre-approved protocols and test cases (see A2.4) and where applicable and required by test cases and test procedures, screen shots should be captured to document test steps and results when relevant. The person performing each test and his access rights (role) should be documented. Where previously passed scripts are not retested along with the testing of fixes for previous fails, this should be risk assessed and the rationale documented.

Testing of the software or trial specific configurations would typically comprise difference components. The software developers would undertake testing (e.g. unit testing/code review) prior to release of the system to user acceptance testing (UAT). The responsibilities for UAT, requirements for UAT test scripts and retention of executed scripts should be defined. There should be a process to control the different system environments and approval for transfer between them (e.g. move from UAT to production environment).

Prior to testing, it should be defined which requirements and tests are related to critical system functionality and consequently should have satisfactorily passed testing prior to deployment.

Deviations encountered during system qualification should be recorded and brought to closure. Any failure to meet requirements pre-defined to be critical should be solved prior to deployment or deployment should be justified and potential impact thoroughly assessed. Any known issues with the system on release should be documented in validation report and, where used, release notes.

A2.6 Release into production

Trial specific configurations/builds should only be released into production and made available to trained site users when all the necessary approvals for the clinical trial have been received, e.g. regulatory authority approval and all documentation is in place (e.g. signed protocol, signed agreement with investigator). This includes any updates to the system, e.g., changes to the system resulting from a protocol amendment should only be released into production once it is confirmed that the necessary approvals have been obtained.

There should be a mechanism to record and manage defects and issues raised by the users e.g. via helpdesk or in other ways becoming known (raised by stakeholders). The sponsor/investigator should be informed of any known defects that could potentially constitute a serious breach to ICH-GCP and/or the clinical trial protocol (e.g. through release notes and ad hoc as they arise). Defects/issues should be fixed in a timely manner.

At the end of testing and prior to release to production a validation report should be prepared and approved. At the time of release training materials and other resources for users should be available.

A2.7 Periodic review (maintenance of the validated state)

Validation of a system should be maintained throughout the full life cycle. Periodic (e.g. yearly or related to major updates) system reviews should be conducted to assess and document whether the system can still be considered to be in a validated state, or whether individual parts or the whole system needs re-validation. Depending on the system type and application, the following elements should be evaluated and concluded on, both individually and combined:

- (changes to) hardware/infrastructure;
- changes to operating system/platform;
- application changes;
- configurations, customisations;
- deviations (or recurrence of);
- security incidents;
- newly identified risks;
- new regulation;
- system accesses;
- and failed login attempts.

A2.8 Change control

There should be a formal change control process. Requests for change should be documented and should include details of change, risk-assessment (e.g. for data integrity, regulatory compliance) and testing requirements as a minimum. For trial specific configurations, the change request should include the details of the new version of the protocol if the request relates to a protocol amendment. As part of the change control process, all documentation should be updated as appropriate (e.g. specification documents, training materials, user manuals, test scripts) and a report of the validation activities prepared and approved prior to release into production. There should be version control of the system. The sponsor/investigator should ensure that any changes to the system do not result in data integrity or safety issues or interfere with the conduct of an ongoing trial. Any updates that result in the changes of a form should be highlighted and provided to the investigator in a comprehensive way and it should be clear when they were implemented.

Any changes to the system itself should be documented, should be attributable and if necessary, the change should be explained. Any significant changes to a data capture system should be authorised in writing by an appropriate decision maker.

Documentation on validation of previous or discontinued versions of systems should be retained (see "Guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic), (EMA/INS/GCP/856758/2018) section 6.3)

The eCRF and/or electronic data collection (EDC) system can change during the course of the trial. Examples could be correction of a question text, change of a visibility rule for a conditional question or the change in number or type of list items in a dropdown field. Any such changes could influence contextual properties that may change data entry behaviour, data interpretation and create issues for statistical analysis and should be sufficiently documented as part of the audit trail system.

Annex 3 User management

A3.1 User management

Organisations should grant, change and revoke system accesses in a timely manner as people begin, change and end their involvement/responsibility in the management and/or conduct of the clinical trial projects.

A3.2 User reviews

At any given time, an overview of current and previous access, roles and permissions should be available from the system. This information concerning actual users and their privileges on systems should be verified at suitable intervals to ensure that only necessary and approved users have access and that their roles and permissions are appropriate. There should be timely removal of access no longer required, or no longer permitted.

A3.3 Segregation of duties

System access should be granted based on a segregation of duties and also the responsibilities of the investigator and the sponsor as outlined in ICH-GCP. For example, a person employed by the sponsor/CRO should not have edit rights to data entered into the eCRF by the investigator.

Users with privileged or "admin access" typically have extensive rights in the system (operating system or application), including but not limited to changing any system setting (e.g. system time), defining or removing users (incl. "admin users"), activate or deactivate audit trail functionality (and sometimes even edit audit trail information) and making changes to data that are not captured in the audit trail (e.g. backend table changes in the database(s)). Users with privileged access should be sufficiently independent from and not be involved in the management and conduct of the clinical trial and in the generation, modification and review of data.

Users of computer clients (e.g. personal computer (PC)) which record or contain critical clinical trial data, should generally not have "admin access" to this equipment and when this is not the case, it needs to be justified.

Unblinded information should only be accessible to pre-identified user roles.

A3.4 Least-privilege rule

System access should be assigned according to the least-privilege rule, i.e. users should not have higher privileges and more access rights than actually necessary for them to undertake their required duties.

A3.5 Individual accounts

All system users should have individual accounts. Sharing of accounts (group accounts) is considered unacceptable and a violation of data integrity and ICH-GCP principles as data should be attributable.

A3.6 Unique user names

System user names should be unique within the system and across full life cycle of the system. User names should be traceable and those assigned to human users should be readily distinguishable from machine accounts.

Annex 4 Security

A4.1 Ongoing security measures, including management of firewalls, patching management, penetration testing etc.

The sponsor/investigator should maintain a security system that prevents unauthorised access to the data (ICH-GCP 2.11, 5.5.3 (d)). Threats and attacks on systems containing clinical trial data and corresponding measures to ensure security of such systems are constantly evolving, especially for systems and services being provided over or interfacing the internet.

A4.2 Physical security

Computerised systems and media containing clinical trial data should be protected against physical damage, unauthorised physical access and unavailability.

The extent of security measures depends on the criticality of the data. In the case where data are transferred from one system to another (e.g. from a hand-held device or local drive to a server), it also depends on whether the transfer has already taken place and on the availability of backups.

The responsible party should ensure an adequate level of security for datacentres as well as for local hardware such as USB drives, hard disks, tablets or laptops.

At a datacentre (e.g. hosting an eCRF system), physical access should be limited to the necessary minimum and be controlled by means of two-factor authentication. The data centre should be constructed to minimise the risk of flooding, there should be pest control and effective measures against fire, i.e. cooling, and fire detection and suppression. There should be emergency generators and uninterruptable power supplies (UPS) together with redundant IP providers. Disposed media (e.g. hard disks) should be properly destructed before being disposed of and in case of co-location (see Cloud services), the servers should be locked up in cages to prevent access from other clients.

Data should be replicated at an appropriate frequency from the primary data centre to a secondary failover site at an adequate physical distance to minimise the risk that the same fire or disaster destroys both datacentres.

A4.3 Firewalls

In order to provide a barrier between a trusted internal network and an untrusted external network and to control incoming and outgoing network traffic (from certain IP addresses, destinations, protocols, applications, or ports etc.), firewall rules should be defined. These should be defined as strict as practically feasible, only allowing necessary and permissible traffic.

As firewall settings tend to change over time (e.g. as software vendors and technicians need certain ports to be opened due to installation or maintenance of applications), firewall rules and settings should be periodically reviewed. This should ensure that firewall settings match approved firewall rules and the continued effectiveness of a firewall.

A4.4 Vulnerability management

Vulnerabilities in computer systems can be exploited to perform unauthorised actions, such as modifying data or making data inaccessible to legitimate users. Such exploitations could occur in operating systems for servers, computer clients, tablets and mobile phones, routers and platforms (e.g. databases). Consequently, relevant security patches for platforms and operating systems should be applied in a timely manner, according to vendor recommendations.

Systems, which are not timely security patched according to vendor recommendations, should be effectively isolated from computer networks and the internet.

A4.5 Platform management

Platforms and operating systems for critical applications and components should be updated in a timely manner according to vendor recommendations, in order to prevent their use in the unsupported state.
Unsupported platforms and operating systems, for which no security patches are made, are in a vulnerable state. Qualification of applications on the new platforms and operating systems and of the migration of data should be planned ahead and completed in due time prior to expiry of the supported state.
Unsupported platforms and operating systems should be effectively isolated from computer networks and the internet.

It should be ensured that software used in clinical trials, remains compatible with any changes to platforms/operating systems in order to avoid unintended impact on the conduct/management of the clinical trial due to interruption of functionality or requirements for alternative software and data migration.

A4.6 Use of bi-directional devices (e.g. USB devices)

Uncontrolled use of bi-directional devices, which come from or have been used outside the organisation, may intentionally or unintentionally introduce malware and impact data integrity, availability and rights of trial participants. Mitigation using updated antivirus software scans may be attempted.

A4.7 Anti-virus software

Software should be continuously updated with the most recent virus definitions and activated on systems containing critical data in order to identify, pacify and remove known computer viruses.
Systems compatibility should be taken into account and monitored prior to the installation of antivirus software.
Part of using anti-viral software is the need to monitor and review the task manager processes to be alerted in case the anti-virus process is terminated.

A4.8 Penetration testing

For systems facing the internet, penetration testing should be conducted at regular intervals in order to evaluate the adequacy of security measures and identify vulnerabilities in system security (e.g. code injection), including the potential for unauthorised parties to gain access to and control of the system and its data. Vulnerabilities identified, especially those related to a potential loss of data integrity, should be addressed and mitigated in a timely manner.

If the security measure requires input data modifications, reversibility and traceability should be considered as some inputs require full traceability (e.g. source data).

A4.9 Intrusion detection system

An effective intrusion detection system should be implemented on systems facing the internet in order to monitor the network for successful or unsuccessful intrusion attempts from external parties and for the design and maintenance of adequate information technology (IT) security procedures.

A4.10 Internal activity monitoring

An effective system for detecting any unusual activity from a user (e.g. excessive file downloads, copying or moving or backend data changes) should be in place.

A4.11 Security incident management

Organisations managing clinical trial data should have and work according to a procedure defining and documenting security incidents, rating criticality of incidents, and where applicable, implementing effective corrective and preventive actions to prevent recurrence. In cases where data have been, or may have been, compromised, the procedures should include ways to report incidents to relevant parties where applicable. When using a third party, the contract should ensure that incidents are escalated to the sponsor in a timely manner for the sponsor to be able to report serious breaches as applicable.

A4.12 Authentication method

The method of authentication on a system should positively identify users with a high degree of certainty. Methods should be determined based on the type of information in the system. As a minimum, an acceptable method would be user ID and password. Further augmentation depends upon criticality of data risk assessment and applicable legislation (including data protection legislation)

A4.13 Remote authentication and password managers Remote authentication

Remote access to clinical trial data, e.g. to cloud-based systems, raises specific challenges. The level of security should be proportionate to the sensitivity and confidentiality of the data (e.g. nominative data in electronic health records are highly sensitive) and to the access rights to be granted (read-only, write or even "admin" rights). A risk-based approach should be used to define the type of access control required. Depending on the level of risk, a two-factor authentication may be appropriate or necessary.

Two-factor authentication implies that two of the following three factors be used:

- something you know, e.g. a user ID and password
- something you have, e.g. a security token, a certificate or a mobile phone and an SMS pass code
- something you are, e.g. a fingerprint or an iris scan (biometrics)

The risk evaluation should take into consideration the potential use of password managers on devices or computers. Password managers represent an increased risk where the use of personal or otherwise uncontrolled equipment to access the computerised system is allowed or where access rights to the equipment itself are insufficiently implemented and controlled. Insufficiently or non-protected user accounts may result in unauthorised access to clinical trial computerised systems due to the automatic suggestion of user credentials. A policy or contractual arrangements banning the use of password managers would not be considered to provide a sufficient level of security, particularly if personal equipment is used.

The risk linked to the potential hacking of user equipment or to key loggers should also be considered.

A4.14 Password policies

Formal procedures for password policies should be implemented. The policies should include but not necessarily be limited to length, complexity, expiry, login attempts, and logout reset. The policies should be enforced by systems and verified during system qualification.

A4.15 Password confidentiality

Passwords should be kept confidential, sharing of passwords is unacceptable and a violation of data integrity. This implies that after a password is received from a manager or "system admin" (e.g. after a vacation), a new password should be set by the user. This should be mandated by the system.

A4.16 Inactivity logout

Systems should include an automatic inactivity logout, which logs out a user after a defined period of inactivity. The inactivity period should be hardcoded, or set by the "system admin", the user should not be able to set the inactivity logout time (outside defined and acceptable limits) or deactivate the functionality. Upon inactivity logout, a re-authentication should be required (e.g. entry of password).

A4.17 Date and time

Where the system captures date, time and time zone and/or the date, time and time zone are required for reconstructions of activities, procedures should be in place to ensure to be consistent irrespective of location and not to be subject to amendment by users (e.g. universal time coordinated (UTC)). This information should be linked to the data as part of the metadata and available throughout the retention period.

A4.18 Remote connection

When remotely connecting to systems over the internet, a secure and encrypted protocol (virtual private network (VPN) and/or hypertext transfer protocol secure (https)) should be used.

Annex 5 Requirements related to specific types of systems, processes and data.

All computerised systems used in clinical trials should fulfil the requirements described in the previous sections, and the general principles apply. The following sub-sections define more specific wording for selected types of systems where the GCP Inspectors' Working Group (GCP-IWG) has found that supplemental guidance is needed e.g. because the type of data collection method relatively new. For eTMFs and interactive response technology (IRT) systems, please refer to separate guidelines on these topics.[1] A few additional clarifications to IRT systems have been added below.

The use of EDC tools offers a wide variety of approaches to increase overall data quality by procedures such as automatic edit checks, validation checks, assisting information and workflow control. However, such approaches should always be limited by necessity, it should not bias data and it should be detectable e.g. when data are changed as a result of a fired edit check and/or notification.

Data entered into the EDC tools should not be changed by an automatic process or by the sponsor (e.g. edit rights given to make "self-evident" corrections) without timely authorisation by the investigator (or delegate) and such changes should be documented. Fields should not be prepopulated or automatically filled in, unless these fields are not editable and derived from already entered data (e.g., body surface area). Any algorithm used for such a process should be documented and validated. Data entered previously into the system may be used to repopulate fields.

Data entered into the eCRF should be consistent with source data, where applicable, and therefore data should be coded in a manner that shows the relation between the original source entry and the coded value. Categorical coding should be pre-specified. However, source data directly entered into an eCRF should be saved in a one to one correspondence.

Completion checks, range checks, sequence checks etc. should be considered to ensure data quality.

A5.1 Electronic clinical outcome assessment (eCOA)

eCOA employs technology for (direct) reporting of outcomes by investigators and trial participants/care givers. This guideline does not address the clinical validation or appropriateness of particular eCOA systems. The guideline aims at addressing the topics specifically related to these eCOA tools being electronic and also to those related to the situation where Bring-your-own-device (BYOD) solutions are used.

Data can be collected by any of several technologies and will be transferred to a server. Data should be made available to involved/responsible parties such as the PIs e.g. via portals, display of source data on the server, generation of alerts and reports etc. These processes (including access controls) should be controlled and clearly described in the protocol, and all parts of the processes should be validated.

EDC methods may offer more convenience to some trial participants and may increase participant compliance, data quality, reduce variability, reduce the amount of missing data (allowing automatic reminders) and potentially reduce data entry errors. Of importance, whilst use of EDC might be of benefit to some trial participants and patient groups, it may be inconvenient for or even excluding others. This should be considered when using any EDC tool and the choice should be justified.

[1] https://www.ema.europa.eu/en/documents/scientific-guideline/guideline-content-management-archiving-clinical-trial-master-file-paper/electronic_en.pdf
https://www.ema.europa.eu/en/documents/scientific-guideline/reflection-paper-use-interactive-response-technologies-interactive-voice/web-response-systems-clinical-trials-particular-emphasis-handling-expiry-dates_en.pdf

A5.1.1 Electronic patient reported outcome (ePRO)

A5.1.1.1 System design

The ePRO should be designed to meet the specific needs of the end users. It is recommended to involve site staff and the intended trial participant/patient population in the development e.g. demonstrated usability (such as UAT).

One of the advantages of using an ePRO system is the recording of time stamps of data entry. The date and time should record data entry time and not only data submission/transmission time.

Trial participants should have access to their own previously entered data, unless it is against the purpose of the clinical trial design or the protocol. Therefore, the length of time that data are viewable by the participant should be considered when designing the EDC tool. Decisions about 'view-period' for participants should be based on considerations regarding risk for bias on data to be entered but also considering that if view of recently entered data is not possible by the participant, then there is a risk that the participant could forget if relevant data have been collected – especially if the planned entry is not foreseeable and e.g. just requires e.g. input once daily but e.g. event-driven.

Logical checks should be in place to prevent data changes unreasonable "time travel" e.g. going back (months, years back in time) or forth into the future based on the protocol design.

It is recommended to include a scheduling/calendar component with alerts or reminders to ensure compliance.

A5.1.1.2 Data collection and data transfer

The same GCP standards apply for data collected via ePRO as for any other method of data collection, i.e. that there are processes in place to ensure the quality of the data, and that all clinical information is recorded, handled and stored in such a way as to be accurately reported, interpreted and verified.

An ePRO system typically requires an entry device. Data saved in the device is the original record created by the trial participant. Since the data stored in a temporary memory are at higher risk of physical loss, it is necessary to transfer the data to a durable server at an early stage, by a validated procedure and with appropriate security methods during data transmission. Data should be transferred to the server by a pre-defined timing and procedure. The data saved in the device are considered source data. After the data are transferred to the server via a validated procedure, the data on the server are considered a certified copy. The sponsor should identify the source documents in the protocol and document the timing and locations of source document storage.

Besides the general requirements on audit trail (please refer to section 6.2), if an ePRO system is designed to allow data correction, the data corrections should be documented and an audit trail should record if data saved in the device are changed before submission (if changeable).

Data loss on devices should be avoided. Procedures should be in place to prevent data loss if web access to the trial participant reported data is interrupted, (e.g. server outage, battery in device drained, loss of or unstable internet connection). There should be a procedure in place to handle failed or interrupted data transmission.

It should be ensured/monitored that transmission of data from the ePRO devices are successfully completed.

Important actions should be time stamped in an unambiguous way, e.g. data entries, transfer times and volume (bytes).

A5.1.1.3 Investigator access to ePRO data

Unlike data collected in the eCRF, ePRO source data are not managed (although available to review) by the investigator and are often hosted by a contracted party. The investigator is responsible for the trial participants' data (including metadata). Those should consequently be made available to the investigator in a timely manner. This will allow the investigator to fulfil her or his responsibilities for oversight of safety and compliance and thereby minimise the risk of missed adverse events or missing data.

A5.1.1.4 Data changes

As stated in section 6.2.1 on audit trails, a procedure should be in place to address the situation when a data originator (e.g. investigator or trial participant) realises that she/he has submitted incorrect data by mistake and wants to correct the recorded data.

Data changes for ePRO typically differ from that of other EDC tools because trial participants may not have access to correct data in the application. Hence, procedures need to be in place in order to implement changes when needed. This could be in the form of data clarification processes initiated by trial participants on their own reported data or initiated by investigators.

Data reported should always be reliable and it is not acceptable that data clarification procedures introduced by the sponsor or vendor whether or not described in the protocol do not allow for changes in trial participant data when justified e.g. if the trial participant realises that data has not been entered correctly.

It is expected that the possibility for changes is implemented based on a justified and trial-specific risk-assessment and that any changes are initiated in a timely manner by the participant or site staff and in case of the latter is based on solid source at investigator sites e.g. phone notes or emails from trial participants documenting the communication between sites and trial participants immediately after the error was made/discovered. Preferably such notes should be signed by the trial participant to avoid that sites are manipulating data e.g. to make participants/patients eligible for trial participation.

One of the advantages of direct data entry by the trial participant is that recall bias is minimised as the data are entered contemporaneously. Consequently, corrections should not be done at a much later stage without good reason and justification. Whether collected by paper or electronic means, the regulatory requirements are that all clinical data should be accurately reported and should be verifiable in relation to clinical trials.

It is expected that the amount of changes to ePRO data is limited; however, this requires both designs of ePROs that are appropriate to ensure proper understanding by trial participants and appropriate training of trial participants, thereby avoiding entry errors.

A5.1.1.5 Fall back procedures and tracking of devices

There should be fall-back procedures in place in case of device malfunction.

There should be an accountability log of devices handed out to trial participants and this should include the device identification number in order to be reconciled to a particular trial participant. In case of device malfunction or loss of devices, there should be a procedure in place to replace the device and to merge data from several devices of a trial participant without losing traceability.

A5.1.1.6 User name and password

The trial participant's passwords should only be known to the trial participant.

The authentication information should not contain any information, which would allow breach of confidentiality, e.g. trial participants name, trial participants email address, social security number.

In relation to BYOD, sponsors should ensure that basic user access controls are implemented. When mobile applications are used for data entry, access controls need to be in place to ensure attributability. See section A5.1.3 for further guidance on BYOD.

A5.1.1.7 Training

Training should be customised to meet the specific needs of the end users.

A5.1.1.8 User support

Support to the trial participant and the trial site staff should be readily available (e.g. support via phone or e-mail) in order to ensure reliable data and minimise the risk of data loss. Trial participant confidentiality should be ensured at all times, including in the communication process.

Procedures for service desk, user authentication and access restoration should be implemented.

A5.1.2 Clinician reported outcome

Tools to directly collect clinician reported outcomes should generally follow the same requirements as those described for systems in general. The main difference is the user (investigators, other clinicians or independent assessors instead of trial participants), not the system requirements. Special attention should be given to access control in order to avoid jeopardising any blinding, when relevant.

A5.1.3 Bring your own device (BYOD)

Both ePRO data and clinician reported outcome data may be captured by privately owned devices such as mobile phones, tablets, computers and wearables, i.e. BYOD. This can either be achieved via a web-application with pre-installed browser applications or by installing an application on the device. Solutions can be either a combination of web and application (hybrid) or coded to the device operating system (native).

It is necessary to provide alternative ways of data collection e.g. devices provided by the sponsor as the trial participants should not be excluded from a trial if not capable or willing to use BYOD.

A5.1.3.1 Technical and operational considerations

When decided to use BYOD, a multitude of devices and operating systems should be considered for the application. It should be ensured that it is not exclusive to one operating system. Qualification activities should also take things like upgrade of operating systems and different screen sizes into account e.g. for visual analogue scales (VAS), where the general presentation should be the same irrespective of device. Because the platform of the BYOD is not under the control of the sponsor, an assessment for updates and change of service terms for the applications and the web-applications should be done.

Measures should be in place to ensure that users cannot change critical settings including captured date and time or deactivate inactivity log out (refer to A4.17 and A4.18).

For each system intended, proper mitigation strategies should be in place and each system configuration should be validated.

Terms of service of the platform provider can be in conflict with ICH-GCP and (local) legal requirements; where such conflicts exist, the device may not be suitable for use.

Procedures and processes should be in place for when the trial participant discontinues the clinical trial or the clinical trial ends and access to applications and data collection should be terminated.

A5.1.3.2 Considerations on security and trial participant confidentiality

The confidentiality of data that could identify trial participants should be protected, respecting the privacy and confidentiality rules in accordance with the applicable regulatory requirements.

A number of challenges for BYOD are related to security and security should be ensured at all levels (mobile device security, data breach security, mobile application security etc.). As mobile devices may be lost or stolen and it cannot be ensured that the trial participants use passwords to secure their device, the security and access control should be at the application level.

Application and operating system (OS) vulnerabilities should be described and the risk minimised. Intentional or unintentional exposure of the data within the app should be prevented and local storage of data should be minimised.

The hardware, operating system and apps are all factors that affect the total security status of the device, and there should be procedures in place regarding e.g., when trial participants/clinicians use less secure devices. Minimum supported device requirements should be defined for personal devices when relevant (e.g. memory capacity, operating system). These should take into account which operating systems are still supported by the manufacturer and for which bug fixes and security patches are released when relevant.

Data capture by BYOD may require the device to be identified to ensure data attributability, including runtime environment information and physical properties (e.g. device details, application details, operation system (OS) details, browser details, screen size, IP address, international mobile equipment identity (IMEI)/ mobile equipment identifier (MEID) number). Only information that is needed for proper identification of and service to the user should be obtained. Trial participant confidentiality should be ensured if device identification information is stored. Access to the application and trial participant data may be protected with multiple barriers (e.g. unlock mobile phone, open application, access data).

If the device's inbuilt possibilities for auto fill formula data and/or using photo, video, and global positioning system (GPS) data etc. are used, this should be described and justified in the protocol, and procedures and processes should ensure that only protocol mandated data are collected and that the confidentiality of data is maintained. In accordance with the principle of 'data minimisation' mobile applications should only collect data which are necessary for the purposes of the data processing (i.e. the performance of the trial) and not access any other information on the person's device. For example, location data should only be collected if this is necessary for the clinical trials activities and the trial participant must be informed about this in the patient information and agree to this in the consent form.

If an app is to be installed on a BYOD, the privacy labels/practices (e.g. regarding tracking data, linked and not linked data) should be clearly communicated to the trial participant upfront.

A5.1.3.3 Installation and support

When using an application, it is recommended that well trained staff assist in the installation even if the application is available through an app-store or service provider platform.

Independently on whether the BYOD solution is based on an application installed on the device or a website/web application, the software and the use should be explained thoroughly in a user manual. Users of the system should have access to user support e.g. from a help desk. There should be a procedure in place in case an application cannot be installed, or the web service is unavailable on a device, if the device has malfunctioned or the participant has purchased a new device. Helpdesk contacts by users should be logged (participant or site staff study ID, purpose of contact, etc.) with due consideration of protecting participant information.

The software and software installation should not limit or interfere with the normal operations of the device. Any unavoidable limitation to the device after installation should be part of the informed consent material.

A5.1.3.4 Ownership of applications and data

Ownership of the clinical trial application and data should be specified.

A5.2 Interactive response technology (IRT) system

The GCP-IWG published separate a reflection paper on use of IRT in clinical trials.

A5.2.1 Testing of functionalities

In addition to the content of the IRT reflection paper and section A2.5, A2.8, of the present guideline, sponsors should also consider the issues mentioned below when writing test scripts for UAT.

A5.2.1.1 Dosage calculations

Where dosage calculations/assignments are made by the IRT system based on user entered data (e.g., trial participant body surface area or weight), and look up tables (dosage assignment based on trial participant parameters), the tables should be verified against the approved protocol and input data used to test allocations, including test data that would be on a borderline between differing doses. Assigning the incorrect dosage to a trial participant is a significant risk to safety and well-being and should be thoroughly mitigated.

A5.2.1.2 Stratified randomisation

Where the randomisation is stratified by factors inputted by the user, all the combinations of the strata should be tested to confirm the allocation from the correct randomisation table is occurring.

A5.2.1.3 Blinding and unblinding

Unblinded information should only be provided and accessible to pre-identified user roles.

A5.2.2 Emergency unblinding

The process for emergency unblinding should be tested.

Prior to the investigational medicinal product (IMP) being available/shipped at/to the clinical trial site, either of the following should be undertaken:

- Where emergency unblinding is undertaken by a site user, there should be confirmation that the investigator (or delegated personnel) who has the access role and permissions has successfully accessed the system.
- Where the unblinding is undertaken via a specific username/password contained in a sealed envelope provided to the site, its receipt by the site should be documented and confirmed.
- If alternative ways are used for unblinding, those processes should be established as well.

A5.2.3 IRT used for collection of clinical data from the trial site

Where the IRT system is collecting clinical data, important data should be subject to source data verification and/or reconciliation with the same data collected in the eCRF. For example, the data used for stratification may also be contained in the eCRF. Where clinical data is entered into the IRT system and integrated to the eCRF (electronic data transfer to eCRF) the IRT system meets the definition of an (e)CRF set out in ICH-GCP. In such cases, the additional functionality and GCP requirement concerning eCRFs should be addressed in the IRT system requirements and UAT. For example, investigator control of site entered data, authorisation of data changes by the investigator, authorisation of persons entering/editing data in the eCRF by the investigator.

A5.2.4 Web-based randomisation

Where justified, sponsor or investigator/sponsor may also use a web-based application to create randomisation lists for clinical trials. When using a web-service, the process to evaluate the suitability of the system and GCP compliance as well as the fit-for purpose of the created randomization list should be documented. Where possible the version of the service used, and the seed should be maintained.

Ad hoc randomization via a web-service is not recommended as randomization distribution is unknown and the seed may vary.

The sponsor should ensure that the process of randomisation can be reconstructed via retained documentation and data and that a final randomisation schedule, produced prior to the clinical trial commencing is retained.

A5.3 Electronic informed consent

Ethics committees will review all material related to the informed consent process. Before implementation of an electronic consent procedure is considered, the sponsor should clarify legality and GCP compliance with each country's ethics committees and national regulatory authorities.

The principles of consent as set out in legislation and guidance should be the same whether the process involves a computerised system or not. A hybrid approach could be considered, where national requirements preclude certain parts of an electronic informed consent procedure. At present, in some countries the failure to provide "written on paper" proof of trial participant's informed consent is considered a legal offense.

An electronic informed consent refers to the use of any digital media (e.g. text, graphics, audio, video, podcasts or websites) to firstly convey information related to the clinical trial to the trial participant and secondly document informed consent via an electronic device (e.g. mobile phones, tablets or computers). The electronic informed consent process involves electronic provision of information, the procedure for providing the opportunity to inquire about details of the clinical trial including the answering of questions and/or electronic signing of informed consent. For example, it would be possible for the trial participant to sign informed consent on a paper form following provision of the information electronically or the information and informed consent could be entirely electronic. If using a "wet ink" signature together with an electronic informed consent document (a hybrid approach), the patient information, the informed consent document and the signature should be indisputably linked e.g. by the use of a hash code.

Investigators should be aware that the use of electronic methods may unintentionally discriminate against people who are not comfortable with or who cannot use such technology, and this could introduce bias into the clinical trial. Alternative methods for provision of information and documentation of informed consent should be available for those unable or unwilling to use electronic methods. Any sole use of electronic informed consent should be justified and described in the protocol.

Face to face communication between one or more members of the research team and the potential trial participant is considered essential and could in some countries be mandatory at least for some specific situations (e.g. due to the characteristics of the disease or of trial).

A5.3.1 Provision of information about the clinical trial

The trial participants should have been informed of the nature, objectives, significance, implications, the expected benefit, risks and inconveniences of the clinical trial in an interview with the investigator, or another member of the investigating team delegated by the PI. The interview should take into account the individual disposition (e.g. comorbidities, patient references etc.) of the potential participant. This interview should allow interaction, the asking of questions and allow confirmation of the trial participant's identity and not just simply the provision of information. The interview should be conducted in person or, it could be done remotely where this can be justified and where allowed nationally and if approved by an ethics committee using electronic methods that allow for two-way communication in real time. Whichever method is used it is important that confidentiality is maintained, and therefore communication methods should be private/secure. Consideration should be given as to how the system would be presented documentarily to the ethics committee for approval such that it captures the functionality of the systems and the experience of the potential trial participant using it.

Provision of the information electronically *may* improve the trial participants' understanding of what taking part in the clinical trial will involve. Computerised system could facilitate features to assess the participant's understanding e.g. via questions at key points, which test the trial participants' understanding as they work their way through the information. This in turn can be used to highlight areas of uncertainty to the person seeking consent so that they can cover this area in more detail with the trial participant.

A5.3.2 Written informed consent

The informed consent of the trial participant should be in writing and electronic methods for documenting the trial participants informed consent should meet this requirement (ICH-GCP 4.8.8): The informed consent form should be **signed** and **personally dated** by at least two (natural) persons; the trial participant or the trial participant's legal representative, and the person who conducted the informed consent discussion. The identity of the persons signing should be ensured.

The method used to record consent should follow national legislation with regards to e.g. acceptability of electronic signatures (see section 4.8) and in some countries "wet ink" signature will be required.

If the use of electronic signatures is allowed by a country, the following applies: date (and where appropriate, time) of signature should be entered by the corresponding signatory. There should be no ambiguity about the time of signature. The system should use UTC for timestamps for the audit trail for the action of signing and dating by the trial participant and investigator, which cannot be manipulated by system settings (e.g. time zones). In cases where entered date and time diverge from the audit trail, a query may be issued, and satisfactory explanation is expected. Any alteration in the document should invalidate the electronic signature.

If an electronic signature is used, it should be possible for monitors, auditors and inspectors to access the signed informed consent forms and all information regarding the signatures, including the audit trail.

Secure archiving should ensure availability and legibility for the required retention period.

A5.3.3 Trial participant identity

It should always be possible to verify the identity of a trial participant with documentation at the trial site. Documentation which makes it possible to demonstrate that the person entering the electronic 'signature' was indeed the signatory, is required. The electronic signing should be captured by the audit trail.

Where consent is given remotely, and the trial participant is required at some point to visit a clinical trial site for the purposes of the trial, verification should be done in person e.g. by using information from an official photo identification if such an ID document is required in the trial site country.

Instead of an electronic signature, a biometric method may be considered.

A5.3.4 Sponsor notification on the consent process

Notification to the sponsor should only contain essential, non-personal identifiable information to allow the sponsor to have an overview of how many trial participants have been enrolled in a clinical trial so far and which versions of the electronic informed consent form have been used. Remote access by the sponsor to personal identifiable information in the electronic consent system should not be permitted. Any unjustified accesses from the sponsor or 3rd parties, which lead to the disclosure of non-pseudonymised information, are likely to be viewed as infringement of data privacy laws.

A5.3.5 Trial participant confidentiality

As for all other computerised systems in clinical trials, the confidentiality of data that could identify trial participants should be protected, respecting the privacy and confidentiality rules in accordance with the applicable national and EU regulatory requirements.

A5.3.6 Trial participant access to the informed consent documentation

Potential trial participants (or, where applicable, their legal representative) should be provided with access to written information about the clinical trial prior to seeking their informed consent. The trial participant should be provided with their own copy of the informed consent documentation (including all accompanying information and all linked information) once their consent has been obtained. This includes any changes to the data/documents made during the process.

The information about the clinical trial should be as a physical hard copy or electronic copy in a form that can be downloaded. The trial participants should also be provided with a copy of their signed and dated written informed consent form (either electronically or on paper). The copy should be available directly.

A5.3.7 Investigator responsibilities

The investigator should take appropriate measures to verify the identity of the potential trial participant (see section A.5.3.3) and ensure that the participant has understood the information given. The informed consent records are essential documentation that should be available at the trial site in the investigator TMF for the required retention period (see section A5.3.9). The investigator should retain control of the informed consent process and documentation (e.g. signed informed consent forms) and ensure that personal identifiable data are not inappropriately disclosed beyond the site. The system used should not limit the investigators ability to ensure that trial participants' confidentiality is protected with appropriate access and retention controls to the system. The investigator should ensure an appropriate process for the copy of the informed consent documentation (information sheet and signed consent form) be provided to the trial participant. All versions of signed and dated electronic consents should be available to the trial participant for the duration of and after the trial. The system used should ensure that the investigator can grant access to the electronic informed consent system to the regulatory authority for inspections and that such access does not require the sponsor's involvement.

A5.3.8 Version control and availability to sites

The electronic informed consent information (electronic trial participant information and informed consent form) are subject to updates and changes during the course of the trial. Regardless of the nature of change or update, the new version containing relevant information has to be submitted to the ethics committee(s) in charge prior to its use for receiving its (their) opinion/approval. Additional information should be made available to the ethics committee(s) in charge concerning technical aspects of the electronic informed consent procedure to ensure continued understanding of the informed consent processes. Only versions approved by the ethics committee(s) in charge should be enabled and used for informed consent process and documentation. Release of electronic trial participant information and informed consent forms to the sites prior to IRB/IEC approval should be prevented. The system should prevent the use of obsolete versions of the information and informed consent document.

A5.3.9 Availability in the investigator TMF

All documents of the informed consent procedure (including all accompanying information and all linked information) are considered to be essential documents and should be archived as such. Replacement of the documents with copies thereof is only acceptable if the copies are certified copies (see section 6.5).

A5.3.10 Withdrawal from the trial

There should be procedures and processes in place for a trial participant to be able to withdraw her/his consent. If there is a possibility for the trial participant to withdraw from the trial through the computerised system, it should be ensured that such a withdrawal of consent generates an alert to the investigator in order to initiate the relevant steps as per protocol and according to the extent of withdrawal. Any withdrawal of informed consent should not affect the results of activities already carried out, such as the storage and use of data obtained on the basis of informed consent before withdrawal.