EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

9 March 2023
EMA/INS/GCP/112288/2023
Good Clinical Practice Inspectors Working Group (GCP IWG)

Guideline on computerised systems and electronic data in clinical trials

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
Final version adopted by the GCP IWG	7 March 2023
Date of coming into effect	6 months after publication

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

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

Official address Domenico Scarlattilaan 6 ● 1083 HS Amsterdam ● The Netherlands
Address for visits and deliveries Refer to www.ema.europa.eu/how-to-find-us
Send us a question Go to www.ema.europa.eu/contact **Telephone** +31 (0)88 781 6000 An agency of the European Union

© European Medicines Agency, 2023. Reproduction is authorised provided the source is acknowledged.

Guideline on computerised systems and electronic data in clinical trials

Table of contents

Glossary **5**
Abbreviations **7**
Executive summary **8**
1. Introduction **8**
2. Scope **9**
3. Legal and regulatory background **10**
4. Principles and definition of key concepts **10**
4.1. Data integrity 10
4.2. Responsibilities 11
4.3. Data and metadata 11
4.4. Source data 11
4.5. ALCOA++ principles 12
4.6. Criticality and risks 13
4.7. Data capture 14
4.8. Electronic signatures 15
4.9. Data protection 16
4.10. Validation of systems 16
4.11. Direct access 16
5. Computerised systems **17**
5.1. Description of systems 17
5.2. Documented procedures 17
5.3. Training 17
5.4. Security and access control 17
5.5. Timestamp 18
6. Electronic data **18**
6.1. Data capture and location 18
6.1.1. Transcription 18
6.1.2. Transfer 18
6.1.3. Direct capture 19
6.1.4. Edit checks 19
6.2. Audit trail and audit trail review 19
6.2.1. Audit trail 19
6.2.2. Audit trail review 20
6.3. Sign-off of data 21
6.4. Copying data 21
6.5. Certified copies 22
6.6. Control of data 22
6.7. Cloud solutions 23

6.8. Backup of data 24
6.9. Contingency plans 24
6.10. Migration of data 24
6.11. Archiving 25
6.12. Database decommissioning 25
Annex 1 Agreements 27
Annex 2 Computerised systems validation 30
A2.1 General principles 30
A2.2 User requirements 31
A2.3 Trial specific configuration and customisation 31
A2.4 Traceability of requirements 31
A2.5 Validation and test plans 31
A2.6 Test execution and reporting 32
A2.7 Release for production 32
A2.8 User helpdesk 32
A2.9 Periodic review 33
A2.10 Change control 33
Annex 3 User management 34
A3.1 User management 34
A3.2 User reviews 34
A3.3 Segregation of duties 34
A3.4 Least-privilege rule 34
A3.5 Individual accounts 34
A3.6 Unique usernames 35
Annex 4 Security 36
A4.1 Ongoing security measures 36
A4.2 Physical security 36
A4.3 Firewalls 36
A4.4 Vulnerability management 36
A4.5 Platform management 37
A4.6 Bi-directional devices 37
A4.7 Anti-virus software 37
A4.8 Penetration testing 37
A4.9 Intrusion detection and prevention 37
A4.10 Internal activity monitoring 37
A4.11 Security incident management 38
A4.12 Authentication method 38
A4.13 Remote authentication 38
A4.14 Password managers 38
A4.15 Password policies 39
A4.16 Password confidentiality 39
A4.17 Inactivity logout 39
A4.18 Remote connection 39
A4.19 Protection against unauthorised back-end changes 39

Annex 5 Additional consideration to specific systems 40
A5.1 Electronic clinical outcome assessment..... 40
A5.2 Interactive response technology system 45
A5.3 Electronic informed consent 46
Annex 6 Clinical systems 50
A6.1 Purchasing, developing, or updating computerised systems by sites 50
A6.2 Site qualification by the sponsor..... 50
A6.3 Training 50
A6.4 Documentation of medical oversight 50
A6.5 Confidentiality..... 51
A6.6 Security 51
A6.7 User management 51
A6.8 Direct access 51
A6.9 Trial specific data acquisition tools..... 52
A6.10 Archiving 52

Glossary

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, records or any form of information.

All references to sponsors and investigators in this guideline also apply to their service providers, irrespective of the services provided.

When a computerised system is implemented by an institution where the investigator is conducting a clinical trial, any reference to the investigator in this guideline also includes the institution, when applicable.

The term '*trial participant*' is used in this text as a synonym for the term '*subject*', which is defined in Regulation (EU) No 536/2014 as '*an individual who participates in a clinical trial, either as a recipient of the IMP or as a control*'.

The term '*responsible party*' is frequently used instead of sponsor or principal investigator. Please also refer to section 4.2. and Annex 1.

The term '*agreement*' is used as an overarching term for all types of documented agreements, including contracts.

The term '*validation*' encompasses aspects usually known as '*qualification and validation*'.

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.

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

Clinical outcome assessment
Clinical outcome assessment (COA) employs a tool for the reporting of outcomes by clinicians, trial site staff, observers, trial participants and their caregivers. The term COA is proposed as an umbrella term to cover measurements of signs and symptoms, events, endpoints, health-related quality of life (HRQL), health status, adherence to treatment, satisfaction with treatment, etc.

Computerised 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 responsible party considers to automate a process and where user requirements are collected, 2) the project phase where a service provider can be selected, a risk-assessment is made, and the system is implemented and validated, 3) the operational phase where a system is used in a regulated environment and changes are implemented in a manner that maintains data confidentiality, integrity and availability, and finally, 4) a retirement phase, which includes decisions about data retention/archiving, migration or destruction and the management of these processes.

Configuration
Configuration sets up a system using existing (out-of-the-box) functionality. It requires no programming knowledge.

Customisation
Customisation modifies and adds to existing functionality by custom coding. It requires programming knowledge.

Data governance
The total of activities, processes, roles, policies, and standards used to manage and control the data during the entire data life cycle, while adhering to ALCOA++ principles (see section 4.5.).

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

Dynamic file formats
Dynamic files include automatic processing and/or enable an interactive relationship with the user. A certified electronic copy may be retained in electronic file formats that are different from the original record, but the equivalent dynamic nature (including metadata) of the original record should be retained.

Event log
An automated log of events in relation to the use of a system like system access, alerts or firing of edit checks.

Patient-reported outcome
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)

Static file formats
Static files containing information or data that are fixed and allow no dynamic interaction.

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 E6 R2 1.65)

Abbreviations

AI	artificial intelligence
ALCOA++	attributable, legible, contemporaneous, original, accurate, complete, consistent, enduring, available when needed and traceable
BYOD	bring your own device
COA	clinical outcome assessment
CTMS	clinical trial management systems
DMP	data management plan
DSMB	data and safety monitoring board
eCOA	electronic COA
eCRF	electronic case report form
EDC	electronic data collection
EMA	European Medicines Agency
ePRO	electronic PRO
eSource	electronic source
eTMF	electronic TMF
GCP IWG	GCP inspectors' working group
GCP	good clinical practice
GPS	global positioning system
HQRL	health-related quality of life
HTML	hypertext mark-up language
HTTPS	hypertext transfer protocol secure
IaaS	infrastructure as a service
IB	investigator brochures
IMP	investigational medicinal product
IRT	interactive response technologies
IT	information technology
JS	JavaScript
KPI	key performance indicator
PaaS	platform as a service
PC	personal computer
PDF	portable document format
PRO	patient-reported outcome

SaaS	software as a service
SAE	serious adverse event
SOP	standard operating procedures
SUSAR	suspected unexpected serious adverse reactions
TMF	trial master file
UAT	user acceptance test
UPS	uninterruptable power supplies
URS	user requirements specification
USB	universal serial bus
UTC	coordinated universal time
VPN	virtual private network

Executive summary

Computerised systems are being increasingly used in clinical research. The complexity of such systems has evolved rapidly in the last few years from electronic case report forms (eCRF), electronic patient reported outcomes (ePROs) to various wearable devices used to continuously monitor trial participants for clinically relevant parameters and ultimately to the use of artificial intelligence (AI). Hence, there is a need to provide guidance to all stakeholders involved in 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 rights, dignity, safety and wellbeing of the trial participants. This would ultimately contribute to a robust decision-making process based on such clinical data.

This guideline will describe some generally applicable principles and definition of key concepts. It also covers requirements and expectations for computerised systems, including validation, user management, security, and electronic data for the data life cycle. Requirements and expectations are also covered related to specific types of systems, processes, and data.

1. Introduction

As described above, the change in data and trial types and thereby the use of computerised systems presents new challenges. The European Medicines Agency (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 to replace the Reflection Paper.

There is no requirement or expectation that the sponsors and investigators use computerised systems to collect data; however, the use of data acquisition 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, automated data transfers, validation checks, assisting information and workflow control.

2. Scope

The scope of this guideline is computerised systems, (including instruments, software and '*as a service*') used in the creation/capture of electronic clinical data and to the control of other processes with the potential to affect participant protection and reliability of trial data, in the conduct of a clinical trial of investigational medicinal products (IMPs). These include, but may not be limited to the following:

- Electronic medical records, used by the investigator to capture of all health information as per normal clinical practice.
- Tools supplied to investigators/trial participants for recording clinical data via data entry (e.g. electronic clinical outcome assessments [eCOAs]).
    - Electronic trial participant data capture devices used to collect ePRO data, e.g. mobile devices supplied to trial participants or applications for use by the trial participant on their own device i.e. bring your own device (BYOD).
    - Electronic devices used by clinicians to collect data e.g. mobile devices supplied to clinicians.
- Tools supplied for the automatic capture of data for trial participants such as biometrics, e.g. wearables or sensors.
- 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 the transit and storage temperatures for investigational medicinal product (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. LC-MS/MS systems, medical imaging and related software).
- eTMFs, which are used to maintain and archive the clinical trial essential documentation.
- Electronic informed consent, for the 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 use by the potential trial participants on their BYOD or access to web-based applications.
- Interactive Response Technologies (IRT), for the management of randomisation, supply and receipt of IMP, e.g. via a web-based application.
- Portals or other systems for supplying information from the sponsor to the sites (e.g. investigator brochures (IBs), suspected unexpected serious adverse reactions (SUSARs) or training material), from the sites to the sponsor (e.g. the documentation of the investigator's review of important safety information), or from the sponsor or the site to adjudication committees and others.
- Systems/tools used to conduct remote activities such as monitoring or auditing.
- Other computerised systems implemented by the sponsor holding/managing and/or analysing or reporting data relevant to the clinical trial e.g. clinical trial management systems (CTMS), pharmacovigilance databases, statistical software, document management systems, test 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, data clarification, query processes and event adjudication. Requirements to AI beyond the generally applicable expectations to all systems will not be covered in this guideline initially. This may be covered in a future Annex.

The approach towards computerised systems used in clinical practice (e.g. regarding validation) should be risk proportionate (please also refer to section 4.6.).

3. Legal and regulatory background

- Regulation (EU) No 536/2014, or Directive 2001/20/EC and Directive 2005/28/EC
- 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 to comply with the requirements of the current legislation (Regulation (EU) No 536/2014, Directive 2001/20/EC and Directive 2005/28/EC), as well as ICH E6 Good Clinical Practice (GCP), regarding the use of computerised systems and the collection of electronic data in clinical trials.

The risk-based approach to quality management also has an impact on the use of computerised systems and the collection of electronic 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 and electronic signatures.

Further elaboration of the expectations of the EU GCP Inspectors' Working group (GCP IWG) on various topics, including those on computerised systems, can be found as GCP IWG 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, accessed, and maintained in a secure manner, to fulfil the ALCOA++ principles of being attributable, legible, contemporaneous, original, accurate, complete, consistent, enduring, available when needed 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 data 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 on the importance of data integrity principles and the creation of a working environment that enables visibility, and actively encourages reporting of omissions and erroneous results.

Lack of integrity before the expiration of the mandated retention period may render the data unusable and is equivalent to data loss/destruction.

4.2. Responsibilities

Roles and responsibilities in clinical trials should be clearly defined. 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:

- Investigators and their institutions, laboratories and other technical departments or clinics, generate and store 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 that supply, store and/or, manage and operate computerised systems (including software and hardware) and the records generated by them. Sponsors may do this directly, or via service providers, including organisations providing e.g. eCOA, eCRF, or IRT that collect and store data on behalf of sponsors.

Please refer to Annex 1 regarding the transfer/delegation to service providers of tasks related to the use of computerised systems and services.

4.3. Data and metadata

Electronic data consist of individual data points. Data become information when viewed in context. Metadata provide context for the data point. Different types of metadata exist such as: variable name, unit, field value before and after change, reason for change, trial master file (TMF) location document identifier, timestamp, 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 entering or taking an action on the data such as modifying, deleting, reviewing, etc. (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 have no meaning. Loss of metadata may result in a lack of data integrity and may render the data unusable.

4.4. Source data

The term source data refers to the original reported observation in a source document. Source documents could be e.g. hospital records, clinical and office charts, laboratory notes. Other examples are emails, spreadsheets, audio and/or video files, images, and tables in databases.

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 outline (figure 1) of the data processing stages, starting with the data capture. The correct identification of source data is important for adequate source data verification and archiving. Data at different processing stages can be considered source depending on the preceding processing steps.

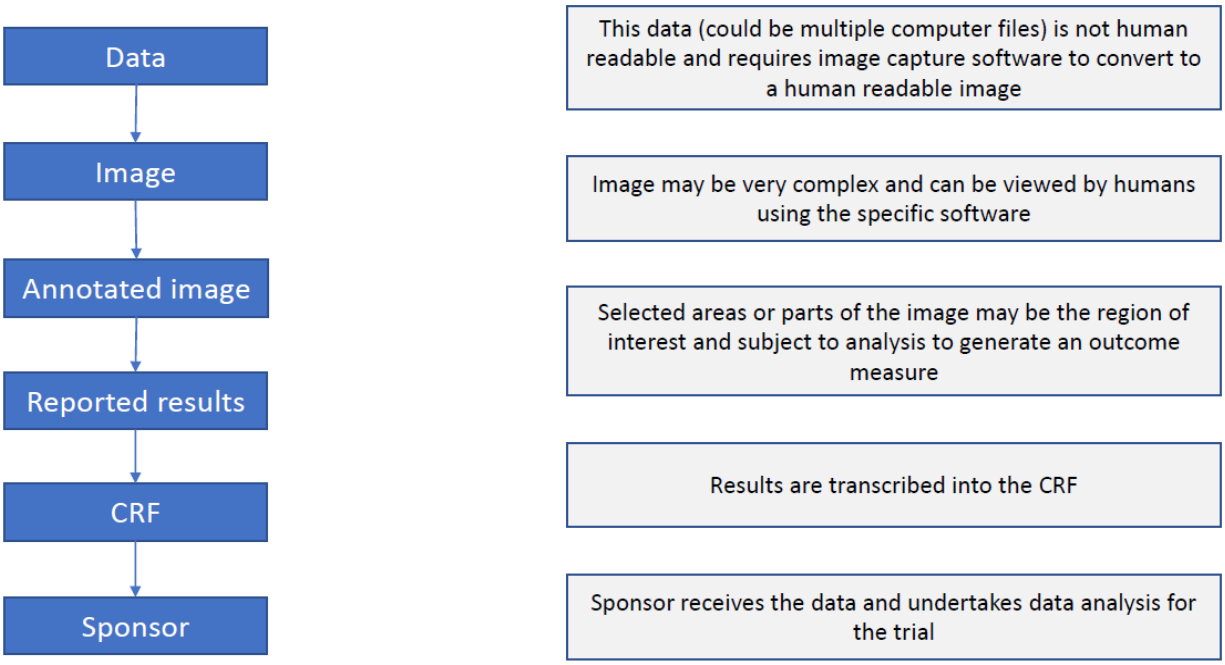

Figure 1

Data capture sometimes requires some degree of processing prior to data recording. In this process, the data generated during an observation, measurement or data collection is checked, processed, and transferred into a new format and then recorded.

The retention of unprocessed data records is not always feasible. If the processing is an integral part of the solution used and is recognisable as such in the solution characteristics, there is no need to extract and retain the unprocessed data. It should be possible to validate the correct operation of the processing.

As a general principle, the source data should be processed as little as possible and as much as necessary.

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 adherence to the ALCOA++ principles (see section 4.5.). The location where the source data is first obtained should be part of the metadata.

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 and/or system 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.

Contemporaneous
Data should be generated by a system or captured by a person at the time of the observation. The time point of the observation and the time point of the storage should be kept as part of the metadata, including the audit trail. Accurate date and time information should be automatically captured and should be linked and set by an external standard.

Original
Data should be the original first generation/capture of the observation. Certified copies can replace original data (see section 6.5. on certified copies). 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 on paper. The coding process, which consists in matching text or data collected on the data acquisition tools 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 remain 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. This includes the associated metadata and audit trail and may require preserving the original context.

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 detect and/or avoid 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 sections 6.8. and 6.10. on back-up and archiving).

Available when needed
Data should be stored throughout the data life cycle and should 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/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 E6 describes 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 acquisition tools or trial specific configurations or customisations of systems.

Risks in relation to the use of computerised systems and especially critical risks affecting the rights, safety and well-being of the trial participants or the reliability of the trial results would be those related to the assurance of data integrity. Those risks should be identified, analysed, and mitigated or accepted, where justified, throughout the life cycle of the system. Where applicable, mitigating actions include revised system design, configuration or customisation, increased system validation or revised SOPs (including appropriate training) for the use of systems and data governance culture.

In general, risks should be determined based on the system used, its complexity, operator, use of system and data involved. Critical 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 functionalities such as the generation of an IMP shipment report. The interface and interdependency between systems or system components should be taken into consideration.

All data collected or generated in the context of a clinical trial should fulfil ALCOA++ principles. Consequently, the arrangements for data governance to ensure that data, irrespective of the format in which they are generated, 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, coding and validation, monitoring plans, agreements between parties that define roles and responsibilities, systematic safeguards to ensure adherence to SOPs, training in processes and procedures, etc.

There are special risks to take into consideration when activities are transferred/delegated. These are further elaborated on in Annex 1 on agreements.

The risk-assessment should take the relevance of the system use for the safety, rights, dignity and well-being of the participant and the importance and integrity of derived clinical trial data into account 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 for other purposes than what they were developed for, or which are used outside the supplier’s specification/validation are inherently higher risk. In case of well-established computerised systems, which are used as intended 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 prior to use in the trial.

For systems deployed by the investigator/institution specifically for the purposes of clinical trials, the investigator should ensure that the requirements for computerised systems as described in this guideline are addressed and proportionately implemented. For systems deployed by the investigator/institution, the sponsor should determine during site selection whether such systems (e.g. electronic medical records and other record keeping systems for source data collection and the investigator site file) are fit for purpose.

For computerised systems deployed by the sponsor, the sponsor should ensure that the requirements of this guideline are addressed and proportionately implemented.

4.7. Data capture

The clinical trial protocol should specify data to be collected and the processes to capture them, including by whom, when and by which tools.

Data acquisition tools should be designed and/or configured or customised to capture all information required by the protocol and not more. Data fields should not be prepopulated or automatically filled in, unless these fields are not editable and are derived from already entered data (e.g. body surface area). The protocol should identify any data to be recorded directly in the data acquisition tools and identify them as source data.

A detailed diagram and description of the transmission of electronic data (data flow) should be available in the protocol or a protocol-related document. The sponsor should describe which data will be transferred and in what 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 encouraged.

The sponsor should ensure the traceability of data transformations and derivations during data processing and analysis.

4.8. Electronic signatures

Whenever ICH E6 requires a document to be signed and an electronic signature is used for that purpose, 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:

- authenticate the signatory, i.e. establish a high degree of certainty that a record was signed by the claimed signatory;
- ensure non-repudiation, i.e. that the signatory cannot later deny having signed the record;
- 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 the signature being rendered visibly invalid;
- 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, i.e. signatures executed in '*closed*' and in '*open*' systems.

For '*closed*' systems, which constitute the majority of systems used in clinical trials and which are typically provided by the responsible party or by their respective service provider, the system owner knows the identity of all users and signatories and grants and controls their access rights to the system. Regulation (EU) No 910/2014 ('*eIDAS*') on electronic identification and trust services for electronic transactions is not applicable for 'closed' systems ('*eIDAS*' article 2.2). The electronic signature functionality in these systems should be proven during system validation to meet the expectations mentioned above.

For '*open*' systems, the signatories (and users) are not known in advance. For sites located in the EU, electronic signatures should meet the requirements defined in the '*eIDAS*' regulation. Sites located in third countries should use electronic or digital signature solutions compliant with local regulations and proven to meet the expectations mentioned above.

Irrespective of the media used, in case a signature is applied on a different document or only on part of a document (e.g. signature page), there should still be an unbreakable link between the electronic document to be signed and the document containing the signature.

4.9. Data protection

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

The requirements of General Data Protection Regulation (EU) No 2016/679 (GDPR) 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 for the data to be consequently deleted) as this would cause bias to e.g. safety data (Regulation (EU) No 536/2014 recital 76 and Article 28(3)). Trial participants should be informed accordingly.

In accordance with EU data protection legislation, if personal data of trial participants from an EU Member State are processed (at rest or in transit) or 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 Regulation (EU) No 2018/1727 - 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 place only if a derogation for specific situations apply (under Article 49 of GDPR or Article 50 of EUDPR).

4.10. Validation of systems

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 the design until the 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 associated records) performed by service providers 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 computerised system and for the validation of the trial specific configuration or customisation.

Validation of the trial specific configuration or customisation should ensure that the system is consistent with the requirements of the approved clinical trial protocol and that 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 for further detail on validation.

4.11. Direct access

All relevant computerised systems should be readily available with full, direct and read-only access (this requires a unique identification method e.g. username and password) upon request by inspectors from regulatory authorities. If a computerised system is decommissioned, direct access (with a unique identification method) to the data in a timely manner should still be ensured (see section 6.12.).

5. Computerised systems

Requirements for validation are described in section 4.10. and Annex 2, the requirements for user management are described in Annex 3, while the requirements for information technology (IT) security are detailed in Annex 4 of this guideline.

5.1. Description of systems

The responsible party should maintain a list of physical and logical locations 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 security measures implemented.

5.2. Documented procedures

Documented procedures should be in place to ensure that computerised systems are used correctly. These procedures should be controlled and maintained by the responsible party.

5.3. Training

Each individual involved in conducting a clinical trial should be qualified by education, training, and experience to perform their respective task(s). This also applies to training on computerised systems. Systems and training should be designed to meet the specific needs of the system users (e.g. sponsor, investigator or service provider). Special consideration should be given to the training of trial participants when they are users.

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

All training should be documented, and the records retained and available for monitoring, auditing, and inspections.

5.4. Security and access control

To maintain data integrity and the protection of the rights of trial participants, computerised systems used in clinical trials should have security processes and features to prevent unauthorised access and unwarranted data changes and should maintain blinding of the treatment allocation where applicable.

Checks should be used to ensure that only authorised individuals have access to the system and that they are granted 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 passwords and to keep them confidential, enforcement of security systems and processes, identification and handling of security incidents, social engineering and the prevention of phishing.

See Annexes 3 and 4 for further guidance on user management and IT security.

5.5. Timestamp

Accurate and unambiguous date and time information given in coordinated universal time (UTC) or time and time zone (set by an external standard) should be automatically captured.

Users should not be able to modify the date, time and time zone on the device used for data entry, when this information is captured by the computerised system and used as a timestamp.

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 will be retrieved and transmitted. Electronic source data, including the audit trail should be directly accessible by investigators, monitors, auditors, and inspectors without compromising the confidentiality of participants' identities.

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.

6.1.1. Transcription

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 electronic data collection (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

Trial data are transferred in and between systems on a regular basis. The process for file and data transfer needs to be validated and should ensure that data and file integrity are 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 that precludes disclosure of confidential information.

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

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 trails should be continuously accessible (according to delegated roles and corresponding access rights).

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

6.1.3. Direct capture

Direct data capture 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 documented procedure should exist to transfer or transcribe information into the medical record, when relevant.

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

6.1.4. Edit checks

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

Such approaches should be guided by necessity, should not cause bias and should be traceable e.g. when data are changed as a result of an edit check notification.

The sponsor should not make automatic or manual changes to data entered by the investigator or trial participants unless authorised by the investigator.

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. In computerised systems, the audit trail should be secure, computer generated and timestamped.

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 deactivated 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 be stored within the system itself. The responsible investigator, sponsor, and inspector should be able to review and comprehend the audit trail and therefore audit trails should be in a human-readable format.

Audit trails should be visible at data-point level in the live system, and it should be possible to export the entire audit trail as a dynamic data file to allow for the identification of systematic patterns or concerns in data across trial participants, sites, etc. The audit trail should show the initial entry and the changes (value - previous and current) specifying what was changed (field, data identifiers) by whom (username, role, organisation), when (date/timestamp) and, where applicable, why (reason for change).

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 A5.1.1.4 for further details.

For certain types of systems (e.g. ePRO) the data entered may not be uploaded immediately but may be temporarily stored 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. The timestamp of data entry in the capture tool (e.g. eCRF) and timestamp 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 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. eCRF page).

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

Access logs, including username and user role, are in some cases considered to be 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 be generally 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 the 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 to 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 the audit trail of their 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 data acquisition tools under their supervision (electronic records).

The sponsor should seek investigator endorsement of their data at predetermined milestones. The signature of the investigator or authorised member of the investigator's staff is considered as the documented confirmation that the data entered by the investigator and submitted to the sponsor are attributable, legible, original, accurate, and complete and contemporaneous. Any member of the staff authorised for sign-off should be qualified to do so in order to fulfil the purpose of the review as described below. National law could require 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 in 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 serious adverse events (SAEs), adjudication of important events and endpoint data, data and safety monitoring board (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 eCRF as source is particularly important.

Therefore, it will rarely be sufficient to just provide 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 for a marketing authorisation application, all submitted data need to be signed off by the investigator or their 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 their designated representative, the design of the data acquisition tool should be laid out to support the signing of the data at the defined time points.

Furthermore, it is important that the investigator review 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 investigator is a general requirement to ensure participant safety as well as data quality and integrity. Oversight can be demonstrated by various means, one of them being the 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 (see section 6.5.).

Copies should contain a faithful representation of the data and the contextual information. Source documents and data should allow accurate copies to be made. The method of copying should be practical and should ensure that the resulting copy is complete and accurate. It should include the relevant

metadata and such metadata should be complete and accurate. See also section 5 of the '*Guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic)*' (EMA/INS/GCP/856758/2018), 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. a PDF document) or dynamic (e.g. a 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 (JS) among other programming languages). Either way, the result of the copy process should be verified either automatically by a validated process or manually to ensure that the same information is present — including data that describe the context, content, and structure — as in the original.

In case of dynamic files e.g. when a database is decommissioned and copies of data and metadata are provided to sponsors, the resulting file should also capture the dynamic aspects of the original file. In case of files, which are the result of an interpreter, special care needs to be taken to not only consider the informative content of such a file, but also to capture and preserve aspects that are the result of the interactions of the used interpreter(s) and system settings during the display. For example, window size, browser type, operating system employed and the availability of software dependencies (e.g. enabled active web content) can influence the structure and content displayed. Special considerations should be taken whenever copies are to replace original source documents.

6.6. Control of data

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 to enable investigators to make decisions related to eligibility, treatment, care for the participants, etc. and to ensure that the investigator can fulfil their legal responsibility to retain an independent copy of the data for the required retention period. This includes data from external sources, such as central laboratory data, centrally read imaging data and ePRO data.

Exceptions should be justified in the protocol e.g. if sharing this information with the investigator would jeopardise the blinding of 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 service provider that is not considered to be independent from the sponsor or if the sponsor (instead of the service provider) is distributing the data to the investigator. 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 a service provider.

Instead of a system maintained by an independent service provider, the sponsor may take other adequate technical measures that preclude sole control. E.g. the verifiability of data (transactions) by an independent (distributed) tamper-proof ledger may provide comparable security to a system maintained by an independent service provider. This should be justified and documented.

Data entered to data acquisition 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 a service provider. 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 the audit trail should be made available to the investigator in a complete and comprehensive way. In the situation where a service provider 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 from the investigators. The period between the 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 revoked 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 through a service provider, agreements should ensure the level of investigator control mentioned above.

Investigators delegating hosting of such data to service providers themselves should ensure that the intended use is covered by local legal requirements and the in-house rules of the institution.

For investigator-initiated trials, where the data are hosted somewhere in the sponsor/institution organisation, the degree of independence should be justified and pre-specified in agreements e.g. that it is a central IT department, not otherwise involved in the operational aspects of the trial, hosting the data and providing copies to the participating investigators.

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 service provider 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). It is common for these services that they provide the responsible party on-demand availability of computerised system resources over the internet, without having the need or even the possibility to directly manage these services.

If a cloud solution is used, the responsible party should ensure that the service provider providing the cloud is qualified.

When using cloud computing, the responsible parties 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 ICH E6 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 their own validation of the computerised system, the cloud provider should make a test environment available that is identical to the production environment.

6.8. Backup 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 of loss. 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. Backups 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 tests from the backup 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 that endanger data security. Such plans should be regularly reviewed. Disaster mitigation and recovery plans should be part of the contractual agreement, if applicable.

6.9. Contingency plans

Agreements and procedures should be in place to allow trial continuation and prevent loss of data critical to participant safety and trial results.

6.10. Migration of data

Migration as opposed to the 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. the 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 the design or purchase of a new system and of subsequent data migration from an old system, validation of the data migration process should have no less focus than the validation of the system itself.

The validation 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, the 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 complex, depending on the different platforms and systems involved. Regardless of the 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 the 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 the audit trail and the data for continuous access by all stakeholders. A detailed explanation is expected, if no such method has been established to allow the migration of data and the audit trail. Arrangements should ensure that the link between data and metadata can be established. If several parties are involved, agreements should be in place to ensure this.

6.11. 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. An inventory of all essential data and documents and corresponding retention periods should be maintained. It should be clearly defined which data are 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 ensured that the file and any software required (depending on the media used for storage) remain accessible, throughout the retention period. This could imply e.g. migration of data (see section 6.9.).

Suitable archiving systems should be in place to safeguard 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. Please refer to section 4.11 direct access.

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.

6.12. Database decommissioning

After the finalisation of the trial, database(s) might be decommissioned. It is recommended that the time of decommissioning is decided taking into consideration e.g. whether the clinical trial will be used for a marketing authorisation application in the near future in which case it is recommended to keep the database(s) live. Please refer to figure 2 for a proposed approach. 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 service provider) that archived formats provide the possibility to restore the database(s). This includes the restoration 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) are 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 service provider is involved, this should be addressed in the contractual arrangements. Static formats of dynamic data will not be considered adequate. See definitions section on static and dynamic formats.

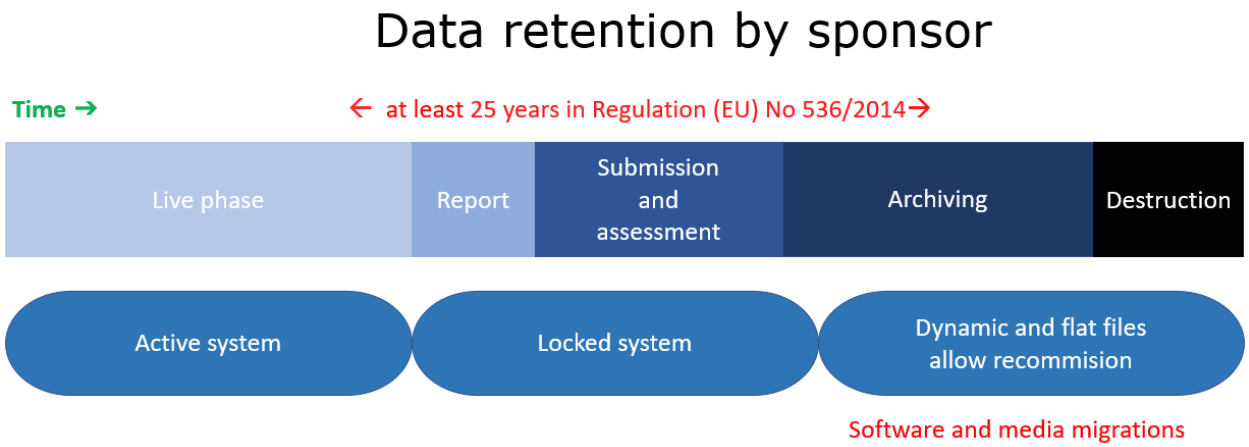
Data retention by sponsor
Time →
← at least 25 years in Regulation (EU) No 536/2014→
Live phase
Report
Submission and assessment
Archiving
Destruction
Active system
Locked system
Dynamic and flat files allow recommision
Software and media migrations

Figure 2

Annex 1 Agreements

The legally responsible parties are the sponsors and investigators. They contract/delegate an increasing number of tasks in clinical trials, contracting is frequent 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 developed by others. The responsible parties can delegate tasks to a service provider, but nevertheless the full responsibility for the data integrity, security and confidentiality resides with them.

Agreements can cover a variety of tasks such as system and trial specific configuration and customisation, provision of a 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. A risk-based approach can be used in relation to agreements as well as for computerised systems in general. It is recognised that a trial specific agreement is not required, if a product is purchased and used as intended without the involvement of the manufacturer of the system; however, such use will require a risk assessment by the responsible party to assess whether such a non-trial specific system is fit for its intended use.

The responsible party should ensure that the distribution of tasks in a trial 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 distribution of activities as part of the clinical trial application process, where applicable. This should be carefully documented in the protocol and related documents, procedures, agreements, and other documents as relevant. It is important to consider who is providing and controlling the computerised system being used.

Clear written agreements should be in place and appropriately signed by all involved parties prior to the provision of services or systems. Agreements should be maintained/updated as appropriate. Sub-contracting and conditions for sub-contracting and the responsible party's oversight of sub-contracted activities should be specified.

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

If appropriate agreements cannot be put in place due to the inability or reluctance of a service provider to allow access to important documentation (e.g. system requirements specifications) or the service provider is unwilling to support pre-qualification audits or regulatory inspections, systems from such a service provider should not be used in clinical trials.

The responsible party should ensure that service providers (including vendors of computerised systems) have the knowledge and the processes to ensure that they can perform their tasks in accordance with ICH E6, as appropriate to their tasks. Standards to be followed, e.g. clinical trial legislation and guidance should be specified in the agreement, where relevant. A number of tasks involve accessing, reviewing, collecting and/or analysing data, much of which is personal/pseudonymised data. In addition, in specific cases involving contact with (potential) trial participants, data protection legislation needs to be followed, in addition to the clinical trial legislation and guidance.

The approved protocol, implicitly, defines part of the specification for system configuration or customisation (e.g. for interactive response technologies (IRT) systems and data acquisition tools) and there should be consistency between the protocol and the wording of the agreement. 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, where relevant.

It should be clear from agreements which tasks are delegated also in relation to retaining essential documentation for performed activities. In the context of clinical trials, 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 (e.g. emails on important decisions and meeting minutes) related to the individual clinical trial (including e.g. relevant helpdesk tickets or meeting minutes) should be retained for the full retention period. It should be clear from the agreement 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 the availability of documentation irrespective of whether the documentation is held by the sponsor/investigator or a service provider 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.

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

It should be specified in agreements 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 that the vendor site shall accept these. The responsible party should also ensure that their service providers act on/respond appropriately to findings from audits and inspections.

The sponsor has a legal responsibility under Regulation (EU) No 536/2014 to report serious breaches, including important data and security breaches, to authorities within seven days. To avoid undue delay in sponsor reporting from the time of discovery e.g. by a vendor, agreements and related documents should specify which information should be escalated immediately to ensure regulatory compliance.

As set out in ICH E6, to ensure that the investigator, rather than the sponsor, maintains control over their data, it should be specified in agreements how investigators' access to and control over data are 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 what formats. Types of output could include e.g. data collected via data acquisition tools including metadata, queries, history and status of changes to users and their access rights, and the description of format for delivery of the complete database to sponsors.

Arrangements on the decommissioning of the database(s) should be clear, including the possibility to restore the database(s), for instance, for inspection purposes.

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

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

Agreements should ensure reliable, continued and timely access to the data in case of bankruptcy, shutdown, disaster of the vendor, discontinuation of service by the vendor or for 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 about computerised systems and data protection legislation, but also on GCP requirements, quality systems, etc. as appropriate to the tasks they perform.

This guideline should be read together with the notice to sponsors regarding computerised systems (EMA/INS/GCP/467532/2019) published on the EMA website.

Annex 2 Computerised systems validation

A2.1 General principles

The responsible party should ensure that systems used in clinical trials have been appropriately validated and demonstrated to meet the requirements defined in ICH E6 and in this guideline.

Systems should be validated independently of whether they are developed on request by the responsible party, are commercially or freely available, or are provided as a service.

The responsible party may rely on validation documentation provided by the vendor of a system if they have assessed the validation activities performed by the vendor and the associated documentation as adequate; however, they may also have to perform additional validation activities based on a documented assessment. In any case, the responsible party remains ultimately responsible for the validation of the computerised systems used in clinical trials.

If the responsible party wants to use the vendor's validation documentation, the responsible party should ensure that it covers the responsible party's intended use as well as its defined needs and requirements. The responsible party should be thoroughly familiar with the vendor's quality system and validation activities, which can usually be obtained through an in-depth systematic examination (e.g. an audit). This examination should be performed by qualified staff with sufficient time spent on the activities and with cooperation from the vendor. It should go sufficiently deep into the actual activities, and a suitable number of relevant key requirements and corresponding test cases should be reviewed, and this review should be documented. The examination report should document that the vendor's validation process and documentation is satisfactory. Any shortcomings should be mitigated by the responsible party, e.g. by requesting or performing additional validation activities.

Some service providers may release new or updated versions of a system at short notice, leaving insufficient time for the responsible party to validate it or to review any validation documentation supplied by the service provider. In such a situation, it is particularly important for the responsible party to evaluate the vendor's process for validation prior to release for production, and to strengthen their own periodic review and change control processes. New functionalities should not be used by the responsible party until they have validated them or reviewed and assessed the vendor's documentation.

If the responsible party relies on the vendor's validation documentation, inspectors should be given access to the full documentation and reporting of the responsible party’s examination of the vendor. If this examination is documented in an audit report, this may require providing access to the report. The responsible party, or where applicable, the service provider performing the examination activities on their behalf, should have a detailed understanding of the validation documentation.

As described in Annex 1 on agreements, the validation documentation should be made available to the inspectors in a timely manner, irrespective of whether it is provided by the responsible party or the vendor of the system. Contractual arrangements should be made to ensure continued access to this documentation for the legally defined retention period even if the sponsor discontinues the use of the system or if the vendor discontinues to support the system or ceases its activities.

In case the vendor’s validation activities and documentation are insufficient, or if the responsible party cannot rely on the vendor to provide documentation, the responsible party should validate the system.

Any difference between the test and the production configuration and environment should be documented and its significance assessed and justified.

Interfaces between systems should be clearly defined and validated e.g. transfer of data from one system to another.

A2.2 User requirements

Critical system functionality implemented and used in a clinical trial should be described in a set of user requirements or use cases, e.g. in a user requirements specification (URS). This includes all functionalities, which ensure trial conduct in compliance with ICH E6 and which include capturing, analysing, reporting and archiving clinical trial data in a manner that ensures data integrity. User requirements should include, but may not be limited to operational, functional, data integrity, technical, interface, performance, availability, security, and regulatory requirements. The above applies independently of the sourcing strategy of the responsible party or the process used to develop the system.

Where relevant, user requirements should form the basis for system design, purchase, configuration, and customisation; but in any case, they should constitute the basis for system validation.

The responsible party should adopt and take full ownership of the user requirements, whether they are documented by the responsible party, by a vendor or by a service provider. The responsible party should review and approve the user requirements in order to verify that they describe the functionalities needed by users in their particular clinical trials.

User requirements should be maintained and updated as applicable throughout a system's lifecycle when system functionalities are changed.

A2.3 Trial specific configuration and customisation

The configuration and customisation of a system for use in a specific trial should be pre-specified, documented in detail and verified as consistent with the protocol, with the data management plan and other related documents. Trial specific configuration and customisation should be quality controlled and tested as applicable before release for production. It is recommended to involve users in the testing activities. The same process applies to modifications required by protocol amendments.

If modifications to a system are introduced due to a protocol amendment, e.g. to collect additional information, it should be determined whether they should be applied to all trial participants or only to those concerned by the amendment.

If new functionalities or interfaces need to be developed, or new code added, they should be validated before use.

A2.4 Traceability of requirements

Traceability should be established and maintained between each user requirement and test cases or other documents or activities, such as standard operating procedures, as applicable. This traceability may have many forms and the process may be automated by software. It should be continuously updated as requirements are changed to ensure that where applicable, for every requirement, there is a corresponding test case or action, in line with the risk evaluation.

A2.5 Validation and test plans

Validation activities should be planned, documented, and approved. The validation plan should include information on the validation methodology, the risk-based approach taken and if applicable, the division of tasks between the responsible party and a service provider. Prior to testing, the risk assessment should define which requirements and tests are related to critical system functionality.

Test cases should be pre-approved. They may have many formats and while historically consisting of textual documents including tables with multiple columns corresponding to the elements below, they may also 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:

- the version of the software being tested;
- any pre-requisites or conditions prior to conducting the test;
- a description of the steps taken to test the functionality (input);
- the expected result (acceptance criteria).

Test cases should require the tester to document the actual result as seen in the test step, the evidence if relevant and, if applicable, the conclusion of the test step (pass/fail). Where possible, the tester should not be the author of the test case. In case of test failure, the potential impact should be assessed and subsequent decisions regarding the deviations should be documented.

A2.6 Test execution and reporting

Test execution should follow approved protocols and test cases (see section A2.5), the version of the software being tested should be documented, and where applicable and required by test cases and test procedures, evidence (e.g. screen shots) should be captured to document test steps and results. Where relevant, the access rights (role) and the identification of the person or automatic testing tool performing tests should be documented.

Where previously passed scripts are not retested along with the testing of fixes for previous failing tests, this should be risk assessed and the rationale should be documented.

Deviations encountered during system validation should be recorded and brought to closure. Any failure to meet requirements pre-defined to be critical should be solved or mitigating actions should be implemented prior to deployment. All open deviations and any known issues with the system at the time of release should be assessed and subsequent decisions should be documented in the validation report and, if applicable, in the release notes. The validation report should be approved by the responsible party before release for production.

A2.7 Release for production

The responsible party should sign off the release prior to initial use.

Training materials, user guides and any other resources required for users should be available at the time of release.

A2.8 User helpdesk

There should be a mechanism to report, record, and solve defects and issues raised by the users e.g. via a helpdesk. Defects and issues should be fixed in a timely manner.

A2.9 Periodic review

Validation of a system should be maintained throughout the full system life cycle. Periodic 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 (non-exhaustive list) should be evaluated and concluded, both individually and in combination:

- changes to hardware/infrastructure;
- changes to operating system/platform;
- changes to the application;
- changes to security procedures;
- changes to backup and restore tools and procedures;
- configurations or customisations;
- deviations (or recurrence thereof);
- performance incidents;
- security incidents;
- open and newly identified risks;
- new regulation;
- review of system accesses;
- updates of agreements with the service provider.

These elements should be reviewed whether the system is hosted by the responsible party or by a service provider.

A2.10 Change control

There should be a formal change control process. Requests for change should be documented and authorised and should include details of the change, risk-assessment (e.g. for data integrity, current functionalities and regulatory compliance), impact on the validated state and testing requirements. For trial specific configurations and customisations, the change request should include the details of the protocol amendment if applicable.

As part of the change control process, all documentation should be updated as appropriate (e.g. requirements, test scripts, training materials, user guide) and a report of the validation activities prepared and approved prior to release for production. The system should be version controlled.

The responsible party 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. The investigator should be clearly informed of any change to a form (e.g. electronic case report form [eCRF] or electronic clinical outcome assessment [eCOA] page) and it should be clear when such changes were implemented.

The documentation relating to the validation of previous or discontinued system versions used in a clinical trial 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).

Annex 3 User management

A3.1 User management

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

Access to the system should only be granted to trained site users when all the necessary approvals for the clinical trial have been received and all documentation is in place (e.g. signed protocol and signed agreement with the investigator). This also applies to any updates to the system, e.g. changes resulting from a protocol amendment should only be made available to users once it is confirmed that the necessary approvals have been obtained, except where necessary to eliminate an immediate hazard to trial participants.

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 to 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 E6.

Users with privileged or '*admin access*' 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 deactivating 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)]). There is a risk that these privileges can be misused. Consequently, 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 the relevant 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 have the fewest privileges and access rights for them to undertake their required duties for as short a time as necessary.

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 E6 principles as data should be attributable.

A3.6 Unique usernames

User access should be unique within the system and across the full life cycle of the system. User account names should be traceable to a named owner and accounts intended for interactive use and those assigned to human users should be readily distinguishable from machine accounts.

Annex 4 Security

A4.1 Ongoing security measures

The responsible party should maintain a security system that prevents unauthorised access to the data. 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, servers, communication infrastructure 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.

The responsible party should ensure an adequate level of security for data centres as well as for local hardware such as universal serial bus (USB) drives, hard disks, tablets, or laptops.

At a data centre hosting clinical trial data, physical access should be limited to the necessary minimum and should generally 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 Internet protocol providers. In case of co-location (see section 6.7 Cloud solutions), the servers should be locked up and physically protected (e.g. in cages) to prevent access from other clients. Media (e.g. hard disks) should be securely erased or destroyed before disposal.

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 data centres. A disaster recovery plan should be in place and tested.

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 security patched in a timely manner according to vendor recommendations, should be effectively isolated from computer networks and the internet, where relevant.

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 an unsupported state.

Unsupported platforms and operating systems, for which no security patches are available, are exposed to a higher risk of vulnerability. Validation 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 the 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 Bi-directional devices

The use of bi-directional devices (e.g. USB devices), which come from or have been used outside the organisation, should be strictly controlled as they may intentionally or unintentionally introduce malware and impact data integrity, data availability, and rights of trial participants.

A4.7 Anti-virus software

Anti-virus software should be installed and activated on systems used in clinical trials. The anti-virus software should be continuously updated with the most recent virus definitions in order to identify, quarantine, and remove known computer viruses. This should be monitored.

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.

A4.9 Intrusion detection and prevention

An effective intrusion detection and prevention 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 unusual or risky user activities (e.g. shift in activity pattern) should be in place.

A4.11 Security incident management

Organisations managing clinical trial data should have and work according to a procedure that defines and documents security incidents, rates the criticality of incidents, and where applicable, implements 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 service provider, the agreement 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, in accordance with Regulation (EU) No 536/2014.

A4.12 Authentication method

The method of authentication in 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. A minimum acceptable method would be user identification and a password. The need for more stringent authentication methods should be determined based on a risk assessment of the criticality of the data and applicable legislation (including data protection legislation), and generally should include two-factor authentication.

User accounts should be automatically locked after a pre-defined number of successive failed authentication attempts, either for a defined period of time, or until they are re-activated by a system administrator after appropriate security checks.

Biometric approaches are currently not specifically addressed by ICH E6. If using biometrics to authenticate the creation of a signature, the investigator and sponsor should ensure that these fulfil the above-mentioned requirements and local legal requirements.

A4.13 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 medical 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, 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 identification 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)

A4.14 Password managers

A secure and validated password manager, with a unique, robust user authentication each time it is used to log into a web site or system, can help to create and use different, complex passwords for each site or system. However, attention should be paid to insufficiently secured password managers.

Password managers built into web browsers may save and automatically fill in user identification and passwords, regardless of whether an independent secure password manager is used or not. This poses a risk if uncontrolled equipment is used (e.g. personal equipment, shared equipment or user accounts), as user access control cannot be enforced; a risk that needs to be effectively mitigated. A policy or contractual arrangement would not be considered adequate to provide a sufficient level of security in such situations.

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

A4.15 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 validation.

A4.16 Password confidentiality

Passwords should be kept confidential, sharing of passwords is unacceptable and a violation of data integrity. Passwords initially received from the system or from a manager or system administrator should be changed by the user on their first connection to the system. This should be mandated by the system.

A4.17 Inactivity logout

Systems should include an automatic inactivity logout, which logs out a user after a defined period of inactivity. 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. password entry).

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.

A4.19 Protection against unauthorised back-end changes

The integrity of data should be protected against unauthorised back-end changes made directly on a database by a database administrator. A method to prevent such changes could be by setting the application up to encrypt its data on the database or by storing data un-encrypted with an encrypted copy. In either case, the database administrator should not be identical to the administrator of the application.

Annex 5 Additional consideration to specific systems

All computerised systems used in clinical trials should fulfil the requirements and general principles described in the previous sections. 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. For electronic trial master files (eTMFs), please refer to the respective guideline[1].

A5.1 Electronic clinical outcome assessment

Electronic clinical outcome assessment (eCOA) employs technology in addition to other data acquisition tools for the reporting of outcomes by investigators, trial participants, care givers and observers. 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 systems 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 investigator e.g. via portals, display of source data on the server, generation of alerts and reports. These processes should be controlled and clearly described in the protocol (high-level) and protocol-related documents, and all parts of the processes should be validated.

Collecting data electronically 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 such measures might be of benefit to some trial participants and patient groups, it may be inconvenient for or even result in the exclusion of others. This should be considered when using any data acquisition tool and the choice should be justified.

A5.1.1 Electronic patient reported outcome

A5.1.1.1 System design

Electronic patient reported outcome (ePRO) should be designed to meet the specific needs of the end users. It is recommended to involve representatives of intended site staff and of the intended trial participant population, where relevant, in the development and testing.

One of the advantages of using an ePRO system is that the timestamps of data entry are recorded. The timestamp should record the time of the data entry and not only the time of the data submission/transmission.

Trial participants should be able to view their own previously entered data, unless justified and unless it is against the purpose of the clinical trial design or the protocol. Therefore, the period that data are viewable by the participant should be considered when designing/configuring the ePRO. Decisions about the '*view-period*' should be based on considerations regarding risk for bias on data to be entered. If viewing 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. This is especially the case if the planned entry is event-driven. In addition, this prevents an unnecessary burden to site staff, as they will be contacted by trial participants in case of doubt less often.

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

[1] Guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic) (EMA/INS/GCP/856758/2018).

It should be considered to include a scheduling/calendar component with alerts or reminders to assist compliance.

A5.1.1.2 Data collection and data transfer

The same ICH E6 standards apply to data collected via ePRO as to 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 on 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 according to a pre-defined procedure and at pre-defined times. The data saved on the device are considered source data. After the data are transferred to the server via a validated procedure, the original data can be removed from the device as the data on the server are considered certified copies. The sponsor should identify the source data in the protocol and protocol-related documents and should document the time and locations of source data storage.

In addition to the general requirements on audit trails (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 the data saved on the device are changed before the data are submitted.

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, device battery 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 the transmission of data from ePRO devices is 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

Unlike data collected in the electronic case report form (eCRF), ePRO data are not managed (although available for review) by the investigator and are often hosted by a service provider. The investigator is overall 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 their 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 and document if a data originator (e.g. investigator or trial participant) realises that they have submitted incorrect data by mistake and want to correct the recorded data.

Data changes for ePRO typically differ from that of other data acquisition tools because trial participants typically do not have the possibility to correct the data in the application. Hence, procedures need to be in place in order to implement changes when needed. This depends on the design of tools and processes and 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. Data clarification procedures introduced by the sponsor or service provider, whether or not described in the protocol should not prohibit changes in trial participant data when justified e.g. if the trial participant realises that the data have 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 a 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.

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 on paper or by 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 number of changes to ePRO data are 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 Accountability of devices

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.

A5.1.1.6 Contingency processes

Contingency processes should be in place to prevent loss of data critical for participant safety or trial results. 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.

A5.1.1.7 Username and password

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

The username and password should not be used in a manner that would breach a trial participant's confidentiality.

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.

A5.1.1.8 Training

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

A5.1.1.9 User support

Support to the trial participant and the trial site staff should be readily available (e.g. support via phone or email) 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 and for ePROs. 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

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 of or willing to use BYOD.

A5.1.3.1 Technical and operational considerations

When using BYOD, a variety of devices, operating systems and where applicable web browsers commonly used, should be considered for the application. It should be ensured that it is not exclusive to one model or operating system.

The sponsor should describe the minimum technical specifications for participants' devices (e.g. operating system, web browser and storage capacity). These should take into account which operating systems are still supported by the manufacturer and if bug fixes and security patches have been released, when relevant.

The sponsor should ensure the quality and integrity of the data across all accepted models and versions.

The sponsor has no control over the implementation of updates to the operating system or over the applications on the trial participant's device. These aspects should be taken into consideration in their risk evaluation and subsequent validation activities.

The application should use an external source for date and time and should not rely on information from the user's device.

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 any authentication methods to secure their device, access control should be at the application level. Section A.4.14 on the use of password managers also applies.

Risks linked to known application and operating system vulnerabilities should be minimised.

The hardware, operating system and applications 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.

Data capture by BYOD may require the device to be identified to ensure data attributability. 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 built-in capabilities 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. 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 that are necessary for the purposes of the data processing and not access any other information on the person's device. For example, location data should only be collected if it is necessary for the clinical trial activities and the trial participant must be informed about it in the patient information and agree to it in the consent form.

Providers may have end-user licensing agreements or terms of service that allow the sharing of data. This may be in conflict with ICH E6 and (local) legal requirements or require information to be provided to the participant and may require specific informed consent. In some cases, the application may not be suitable for use. If an application 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.

The sponsor should be aware that explicit consent may be required related to the above. The informed consent should describe the type of information that will be collected via ePRO and how that information will be used.

A5.1.3.3 Installation and support

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

Independently of 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 via targeted training, which may include user manuals, one-to-one training, and multimedia tools. 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 Uninstallation

It should be possible to uninstall software or applications without leaving residues on BYOD devices, e.g. entries in the registry, incorrect mappings or file fragments. The user should be able to uninstall at any time without expertise or assistance. The uninstallation process should not compromise the device.

A5.2 Interactive response technology system

A5.2.1 Testing of functionalities

In addition to the content of the sections A2.6, A2.10, of this guideline, sponsors should also consider the issues mentioned below when writing test scripts for user acceptance tests (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 such inaccurate assignments 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 that the allocation is occurring from the correct randomisation table.

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. A backup process should also be in place in case the online-technology emergency unblinding is unavailable.

It should be verified that a site's ability for emergency unblinding is effectively available before administering IMP to a trial participant.

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 data acquisition tool. For example, the data used for stratification may also be contained in the data acquisition tool. Where clinical data is entered into the IRT system and integrated in the electronic data collection (EDC) system (electronic data transfer to EDC) the additional functionality and ICH E6 requirement concerning data acquisition tools (eCRFs) should be addressed in the IRT system requirements and UAT e.g. investigator control of site entered data, authorisation of data changes by the investigator, authorisation of persons entering/editing data in the system 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 fitness for purpose of the created randomization list should be documented. The version of the service used, and where applicable, the seed should be maintained.

Ad hoc randomization via a web-service is not recommended as randomization distribution is unknown, the sponsor is not in control of the process e.g. 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 is retained.

A5.3 Electronic informed consent

Ethics committees will review all material related to the informed consent process. Before the implementation of an electronic consent procedure is considered, the sponsor should ensure that the electronic consent procedure is GCP compliant and legally acceptable in accordance with the requirements of the independent ethics committees concerned and of the national regulatory authorities.

The principles of consent as set out in legislation and guidance should be the same regardless of whether the process involves a computerised system. A hybrid approach could be considered, where national requirements preclude cern parts of an electronic informed consent procedure. At present, in some countries failure to provide '*written on paper*' proof of a 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) firstly to convey information related to the clinical trial to the trial participant and secondly to 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.

The method of obtaining an informed consent should ensure the broadest possible access to clinical trials. 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.

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 principal investigator. The interview should take into account the individual disposition (e.g. comorbidities, patient references, etc.) of the potential participant (or legal representative). 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 is 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 to the ethics committee for approval so that it captures the functionality of the system and the experience of the potential trial participant using it. Direct system access should be provided to the ethics committee upon request in a timely manner.

Provision of the information electronically may improve the trial participants' understanding of what taking part in the clinical trial will involve. Computerised systems could facilitate features to assess the

participant's understanding e.g. via questions at key points, which self-evaluate 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 participant's informed consent should ensure that the informed consent form is 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 document consent should follow national legislation with regard to e.g. acceptability of electronic signatures (see section 4.8.), and in some countries '*wet ink*' signature will be required.

There should be no ambiguity about the time of signature. The system should use timestamps for the audit trail for the action of signing and dating by the trial participant and investigator or qualified person who conducted the informed consent interview, which cannot be manipulated by system settings. Any alterations of 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 available to the investigator. 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.

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 to personal identifiable information in the electronic system should only be permitted for the corresponding participant, legal representative, investigator, monitor, auditor, or inspector. Any unjustified accesses, which lead to the disclosure of non-pseudonymised information, are likely to be viewed as an 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 applicable national and EU regulatory requirements.

A5.3.6 Trial participant access

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 a physical hard copy or electronic copy in a format that can be downloaded. The copy should be available immediately to the trial participant.

A5.3.7 Investigator responsibilities

The investigator should take appropriate measures to verify the identity of the potential trial participant (see section A5.3.3) and ensure that the participant has understood the information given. The informed consent documents are essential documents 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 investigator's ability to ensure that trial participants' confidentiality is protected with appropriate access and retention controls in the system. The investigator should ensure an appropriate process for the copy of the informed consent documentation (information sheet and signed consent form) to 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 and revoke access to the electronic informed consent system to monitors, auditors and regulatory authority inspectors.

A5.3.8 Version control and availability to sites

The electronic informed consent information (electronic trial participant information and informed consent form) may be subject to updates and changes during the course of the trial. Regardless of the nature of the change or update, the new version containing relevant information has to receive the favourable opinion/approval of the ethics committee(s) prior to its use. Additional information should be made available to the ethics committee(s) 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) should be enabled and used for the 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's part of the trial master file

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 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 their 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.

Annex 6 Clinical systems

As stated in sections 2. and 4.6., computerised systems implemented at the trial site are also within the scope of this guideline, and the general approach towards computerised systems used in clinical practice is that the decision to use a system in a clinical trial should be risk proportionate and justified pre-trial.

This section is dedicated to specific and additional considerations regarding electronic medical records and other systems implemented at sites, which are primarily used in clinical practice but are also generating clinical trial data.

For computerised systems built specifically for data collection in clinical trials please refer to the relevant sections of this guideline.

A6.1 Purchasing, developing, or updating computerised systems by sites

The investigator/institution should have adequate facilities for a clinical trial. This also applies to the computerised systems of the institution if considered to be used for clinical trial purposes. It is recommended that institutions planning to perform clinical trials consider whether system functionality is fit for the clinical trial purpose. This should also be considered prior to the introduction of a new electronic medical record or equipment planned to be used in clinical trials (e.g. scanners, X-ray, electrocardiograms), or prior to changes to existing systems.

To ensure that system requirements related to GCP compliance (e.g. audit trail for an electronic medical record) are addressed, experienced clinical trial practitioners should be involved by the institution in the relevant steps of the procurement and validation processes.

As many systems are designed with different configuration options, it should be ensured that the systems are configured in a GCP compliant manner.

A6.2 Site qualification by the sponsor

As part of the site qualification, the sponsor should assess the systems in use by the investigator/institution to determine whether the systems are fit for their intended use in the clinical trial (e.g. include an audit trail). The assessment should cover all computerised systems used in the clinical trial and should include consideration of the rights, safety, dignity and wellbeing of trial participants and the quality and integrity of the trial data.

If the systems do not fulfil the requirements, the sponsor should consider whether to select the investigator/institution. The use of systems not fulfilling requirements should be justified, either based on planned implementation of effective mitigating actions or a documented impact assessment of residual risks.

A6.3 Training

If the use of the systems in the context of a specific trial is different from the use in clinical practice e.g. different scanning procedures, different location of files, different requirements regarding documentation etc., trial specific training is required.

A6.4 Documentation of medical oversight

The investigator should be able to demonstrate their medical oversight of the clinical trial when electronic medical records are used. Where all or part of the entries into the medical records are made by a research nurse/dedicated data entry staff it can be difficult to reconstruct the investigator's input. The system

should allow the investigator to document the assessment and acknowledgement of information entered into the system by others.

A6.5 Confidentiality

Pseudonymised copies of electronic medical records may be provided to sponsors, or service providers working on their behalf, outside the clinical environment e.g. if needed for endpoint adjudication or safety assessments according to the protocol. National regulations need to be followed by the sites. In such cases there should be:

- procedures in place at the site to redact copies of medical records, in order to protect the trial participants' identity, before transfer;
- security measures in place, which are relevant to the process, including pseudonymisation and redaction;
- a copy of the pseudonymised records and a proof of the transfer made at the site;
- organisational and technical procedures in place on the receiving side to ensure that the requirements of the data protection regulation are met.

Due to the sensitive nature of information documented in medical records, the extent to which sponsors request these data should be ethically and scientifically justified and limited to specific critical information. Any planned collection of redacted copies of medical records by the sponsor should be described in the protocol, or related documents, and should be explicit in the patient information.

A6.6 Security

Security measures that prevent unauthorised access to data and documents should be maintained.

Please refer to section 5.4. regarding more details on the general requirements for security systems, which are equally applicable to research institutions.

A6.7 User management

Robust procedures on user management should be implemented (see Annex 3).

For systems deployed by the investigator/institution, the investigator should ensure that individuals have secure and attributable access appropriate to the tasks they are delegated to in the trial.

Robust processes for access rights are particularly important in trials where parts of the information could unblind the treatment. Such information should only be accessible to unblinded staff.

A6.8 Direct access

Sponsor representatives (monitors and auditors) and inspectors should have direct, read-only access to all relevant data for all trial participants as determined by the monitors, auditors or inspectors while taking the collected data and the clinical trial protocol into account. This may require access to several different sections or modules of the respective (medical) record e.g. imaging. This requires the use of a unique identification method e.g. username and password.

The access of monitors, auditors and inspectors should be restricted to the trial participants (including potential participants screened but not enrolled in the trial) and should include access to audit trails.

If the site has accepted to provide remote access, appropriate security measures and procedures should be in place to support such access without jeopardising patient rights and data integrity and national legislation.

A6.9 Trial specific data acquisition tools

The electronic medical record contains information, which is crucial for the management of patients and are designed to fulfil legal requirements.

Any trial specific data acquisition tools implemented cannot replace the medical record and their use should not result in a depletion of relevant information in the medical record.

Monitoring activities should not be limited to information in the data acquisition tools and should also consider relevant information in the medical record.

Please also refer to the published qualification opinion on eSource Direct Data Capture (DDC) EMA/CHMP/SAWP/483349/2019.

A6.10 Archiving

Appropriate archiving should be in place to ensure long term readability, reliability, retrievability of electronic data (and metadata), in line with regulatory retention requirements. Please also refer to section 6.11. Requirements for the retention of clinical trial data and documents are frequently different from requirements for other data and documents held by the investigators. It should be ensured that there is no premature destruction of clinical trial data in case of e.g. institution relocation or closure. It is the responsibility of the sponsor to inform the hospital, institution or practice as to when these documents will no longer need to be retained.

There are specific requirements for backup, etc. of electronic data, which can be seen in section 6.8 and which are equally applicable to research institutions. Please also refer to the guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic) EMA/INS/GCP/856758/2018.