Requirements for Electronic Data for Regulated Clinical Trials

"eCF Requirements"

Version:	PR2025 *(Previous MR2025.2)*
Date:	01 APR 2026
Status:	Working Document; an updated release will occur yearly
Author:	eClinical Forum Regulatory Advisory Group (REG team)
	The eClinical Forum REG team that produced this version of eCF Requirements included regulatory expertise from these companies: Astellas, Bristol-Myers Squibb, Clario, eClinical Solutions, Eli Lilly, Fasor, Kyowa Kirin, Medidata 3DS, Neptunus Data, Novartis, Oracle, Pfizer, Servier, and Viedoc Technologies.
	The team members represent regulatory expertise from these countries: Belgium, Finland, France, Germany, India, Italy, Japan, Sweden, Switzerland, United Kingdom, and United States.
Security:	**This is an eClinical Forum Public release. The most current version (MR2026) is reserved for eClinical Forum members in good standing and can be obtained by logging into the eCF website members area. Any references to MR2025 in this or other eClinical Forum documents now refer to this public release PR2025.**

Copyright eClinical Forum

Copyright eClinical Forum 2026

DOCUMENT HISTORY

Date	Revision	Author	Changes
March 2018 March 2019 March 2020 March 2021	MR2018 MR2019 MR2020 MR2021	eCF Regulatory Expert Advisory Group (REG)	This document is updated annually, based on advisory group review and interpretation of information from regulatory authorities.
20-March-2021	MR2021.1	eCF Admin	Minor corrections to Appendix 3
18-June-2021	MR2021.2	eCF Admin	Additional eCF member companies added to the title page
4-April-2022	MR2022.1	eCF REG Team	Please see page 2 of MR2022 for a list of changes to the eCF Requirements text
6-May-2022	MR2022.2	eCF Admin	Additional eCF member companies added to the title page
22-March-2023	MR2023.1	eCF REG Team	Please see page 2 of MR2023 for a list of changes to the eCF Requirements text
1-June-2023	MR2023.2	eCF Admin	Additional eCF member companies added to the title page
20-Nov-2023	MR2023.3	eCF REG Team	This is a significant release in that it incorporates additional mappings and some Criteria text updates as a result of the REG team review of the EMA Guideline on computerised systems and electronic data in clinical trials, which went into effect on 7-Sep-2023
30-Jun-2024	MR2024.1	eCF REG Team	Please see page 2 of MR2024 for a list of changes to the eCF Requirements text
1-May-2025	MR2025.1	eCF REG Team	Please see below for a list of changes to the eCF Requirements text
8-May-2025 24-July-2025	MR2025.2 MR2025.3	eCF REG Team	Corrections to the list of changes Formatting corrected; new logo

In this release (PR2025): The following User Requirements were added or modified:

UR#	PR2024 Text	PR2025
C04	System has an audit trail to include recording date/time/originator of any data creation, change, or deletion.	**The system audit trail must:** **- be indelible, readable and readily available for review and copying.** **- include date, time, originator of any data creation, change, or deletion, and when required the reason for change.**
C05 C07	The audit trail includes the reason for changes /deletions. Audit trail information is readable and readily available.	These 3 user requirements were rolled into the updated C04 above, so these 3 are now retired.

Copyright eClinical Forum

Copyright eClinical Forum 2026

UR#	PR2024 Text	PR2025
C08	System does not allow new audit trail information to over-write existing (previous) information and cannot be altered without detection.	
C16	The system has the ability to create, maintain, apply and revoke the roles, access permissions and capabilities of each user that accesses the system, such that users have access only to those system features and functions to which they have been granted access.	There are system features and processes to create, maintain, revoke, and document the history of user access, roles and privileges over time.
C18	The monitor, auditor, and inspector can within a reasonable timeframe obtain direct access to relevant clinical trial records in order to perform their regulatory duties.	The monitor, auditor, **investigator** and inspector can within a reasonable timeframe obtain direct access to relevant clinical trial records in order to perform their regulatory duties.
C21	There are system and process access control mechanisms that follow current physical and logical information security best practices.	There are system **features and processes to manage, preclude and report on security issues** following current physical and logical information security best practices.
C23	The system must have the ability to provide a history of all individuals who have access to the system and their access privileges over time.	This criteria was combined with C16 and then C23 was retired.
C26	There are sufficient system and/or process controls for backup and recovery procedures.	There are sufficient system and/or process controls for backup and recovery procedures. **Documentation can be produced for inspection by a monitor, auditor or inspector.**
C27	Documentation of the backup and recovery process can be produced for inspection by a monitor, auditor or inspector.	C27 was rolled into the updated C26 above and then C27 was retired.
C35	There are sufficient system and/or process controls to prevent or mitigate the effects of malware: viruses, worms, or other harmful software code.	This criterion was combined with C21 and then C35 was retired.
C36	There are sufficient system and/or process controls over data transfers or migrations from/to other systems, including validation of data mapping and transfer, security of data in transit, confirmation of receipt and continued availability of the audit trail.	There are sufficient system and/or process controls over data transfers **and** migrations from/to systems **to ensure the integrity of data,** and continued availability of the audit trail.
C40	There is a process to ensure the privacy of subjects, and in the event	There are **sufficient system and/or** process controls to ensure the privacy of subjects. In the event of a security incident that exposes privacy

Copyright eClinical Forum

Copyright eClinical Forum 2026

UR#	PR2024 Text	PR2025
	of a security incident that exposes privacy data, the Sponsor and/or Investigator shall notify the relevant Data Protection or other applicable authority.	data, the Sponsor and/or Investigator shall notify the relevant Data Protection or other applicable authority.
C43	There should be a process to periodically review and affirm the continued suitability of the computerised system taking into account the potential cumulative risks and impacts of changes to the system, requirements, version releases and computing environment of the system.	There **is a** process to periodically review and affirm the continued suitability of the computerised system taking into account the potential cumulative risks and impacts of changes to the system, requirements, version releases and computing environment of the system.
C44	For eTMF, the audit trail additionally captures accessing of records.	The eTMF audit trail shall additionally capture the accessing of records.
C46	New in 2025.	**A detailed diagram and description of the transmission of electronic data (data flow) should be available in the protocol or a protocol-related document.**

CONTENTS

1 About the eClinical Forum 4
2 About the eCF Requirements 5
3 eCF Requirements Release Schedule 7
Appendix 1: DISCLAIMER and LICENSE for FAIR USE of eCLINICAL FORUM MATERIALS 8
Appendix 2: Basis for the 2025.1 Release 9
Appendix 3: Documents Reviewed and Not Included as Basis for eCF Requirements 14
Appendix 4: Abbreviations and Definitions 18
Appendix 5: ECF REQUIREMENTS Public Release V2025 20

Copyright eClinical Forum

Copyright eClinical Forum 2026

1 About the eClinical Forum

The eClinical Forum (eCF) is a global not-for-profit and non-commercial, technology independent group representing members of the pharmaceutical, biotechnology, and allied industries. The eClinical Forum's mission is to serve these industries by focusing on those systems, processes and roles relevant to electronic capture, management and submission of clinical data. For further information visit the website at https://eclinicalforum.org/.

The eClinical Forum has sought out opportunities to promote electronic capture since its inception in 2000. The cross-industry forum has a broad view of research with members - Sponsors, Contract Research Organizations (CROs), Technology vendors (both clinical research and healthcare), Academia, and Investigators - and with invited outreach opportunities with global Regulatory representatives.

The eClinical Forum is firmly committed to promoting electronic data in all areas of clinical research. The eClinical Forum endeavors to ease the pain of change by providing clear rationale on implications of regulatory guidance in this area.

1.1 DISCLAIMER, COPYRIGHT and LICENSE

The information presented in these works draws upon the combined current understanding and knowledge of the eClinical Forum on this topic and is provided as an aid to understanding the environment for electronic clinical research. While the information provided has been guided and reviewed by members of the eClinical Forum representing all areas of the pharmaceutical and associated support industry, the opinions of the author(s) and the eClinical Forum do not necessarily reflect the position of individual companies. Users should assess the content and opinions in the light of their own knowledge, needs and experience as well as interpretation of relevant guidance and regulations.

The information in these works does not represent legal advice.

This work is the property of the eClinical Forum and is released under a Creative Commons license for non-commercial use. If you use any portion of this document or associated mappings (or any previous versions) in your own materials, you must credit the eClinical Forum and provide a link to this original document.

For additional License information, see Appendix 1.

Copyright eClinical Forum

Copyright eClinical Forum 2026

2 About the eCF Requirements

The eClinical Forum produces a set of eCF Requirements, which are based upon statements in documents prepared and issued and/or recognized by regulatory authorities that pertain to the design, development, implementation, and management of electronic systems that support clinical research data, as well as those statements that pertain to the handling of data that will be used in a regulated clinical trial.

This is an ongoing effort of the eClinical Forum's "Regulatory Expert Group" (REG). They have put in countless hours to ensure that this comprehensive checklist for evaluating electronic systems that will manage data used in regulated clinical research remains up-to-date against regulations and guidance from FDA /United States, EMA/European Union, PMDA/Japan, NMPA/China, MHRA/United Kingdom, and ICH (International Council on Harmonization) among others. This work is a result of the vast experience of the REG members who come from a variety of different eCF Member companies. They have spent hours debating each regulation or guidance and how to word the eCF Requirements to meet the needs in the regulatory documents.

Each eCF Requirement has as its basis one or more statements from one or more of the documents prepared and issued by FDA, EMA, PMDA, MHRA, NMPA and ICH and others. See appendix 2 for this list of reference documents. We have made every attempt to make each Requirement as succinct as possible, containing a single requirement in each. In addition, we have reviewed many documents from regulatory agencies and associations that are leaders in regulatory insights for clinical research. In some cases, we determined, while valuable documents, did not specifically call-out expectations/laws/regulations/guidance what could be used as a basis for these eCF requirements. So that you may know the completeness of our work, we have included a list of these non-mapped documents in Appendix 3.

The eClinical Forum acknowledges that documents cited in this reference are utilized and applied by regulatory authorities in a variety of ways. For example, some regional regulatory authorities codified the ICH E6 Good Clinical Practice guidance to be binding; other regulatory authorities do not consider the ICH E6 document to be a regulatory document but instead consider it to be non-binding (to industry and the regulatory authority) guidance that represents best practices. These interpretations have been taken into consideration by eClinical Forum in defining the requirements set forth in this reference. To address this conundrum, eClinical Forum has adopted the following rule in determining its requirements:

If any regulatory authority identifies a particular document as a regulatory requirement, we treat the statements in this document as a requirement.

The eClinical Forum recommends that users of this reference be guided by the regulations that impact the region(s) where electronic data and systems will be utilized and apply the eClinical Forum requirements accordingly. With the existence of a global marketplace, it is important to consider the regulatory requirements of all regions where data generated by electronic systems may be used for product marketing submissions or where clinical research is being conducted.

Copyright eClinical Forum

Copyright eClinical Forum 2026

Users should be aware that local legislation may impose additional requirements or user obligations to those stated in the following eCF requirements. For example, local legislation governing data privacy or the use of electronic/digital signatures may also need to be considered.

We commit to updating these eCF Requirements as would be needed when updates are made to the underlying documents and/or new pertinent documents are released from any of the regulatory authorities and bodies listed in Appendix 2. We anticipate releasing updated eCF Requirements once/year typically in the first quarter, in conjunction with our membership year, which begins in January. eClinical Forum member companies with paid annual membership fees are provided exclusive access to the updated eCF Requirements, while the previous year version may be released for non-member use via our website: https://eclinicalforum.org/.

The eCF Requirements can be used to determine if systems which originate and/or manage data that will become part of a regulated clinical trial are consistent with regulatory requirements and recommendations. In particular, the eCF Requirements can be used to assist with self-assessment of systems, planning for system upgrades, writing RFIs, writing system requirements, writing system test scripts, etc. Depending on the type of system being evaluated, not all eCF Requirements may apply. *It is up to the user of these eCF Requirements to review the underlying regulatory statements of any eCF Requirement to determine if it applies to the system under scrutiny.* When using to develop test cases, the user should review all statements from regulatory documents in the mappings to be sure test suites capture all items requested in these regulatory documents. In the case of evaluating Electronic Health/Medical Record systems (EHR/EMR systems), the eClinical Forum has provided an "eSource-Readiness Assessment" (eSRA), based on the eCF Requirements, to assist with this evaluation. The eClinical Forum also provides a questionnaire for evaluating eISF Systems (e-Investigator Site File Systems), also based on the eCF Requirements. They can be found on the eClinical Forum website in the "Site Sys Assmts" tab[1] and is provided to all for free. The work that is published here is an extension of work previously published as HL7 EHRCR Functional Profile (2009), ANSI EHRCR Functional Profile (2010), EuroRec EHRCR Functional Profile (2010), EHRCR User Requirements (2011), eSource-Readiness Assessment: eSRA (2015-2022), Checklist for EDC Systems in Clinical Trials using Service Providers (2016).

A note about Real World Data (RWD) - In today's digital world, foundational data quality determinants are also impacted by computerised systems, that are used to create, process, archive, or transmit data. For RWD, when not regulated by existing guidelines, a software development life cycle ensures the appropriate design, development, and testing of the software and transfers. When guidelines' directives exist, those should be implemented to validate the computerized systems using a risk-based approach that considers the importance of the RWD that is collected, maintained, retained, or transmitted.

[1] The "eSource-Readiness Assessment", or eSRA, can be downloaded for free from www.eclinicalforum.org/esra .

Copyright eClinical Forum

Copyright eClinical Forum 2026

3 eCF Requirements Release Schedule

The eCF Requirements are in a linked .pdf file such that one can easily review the Requirement and then the statements from regulatory authority documents used as a basis for the eCF Requirement. Each release is provided to eCF members with paid annual membership dues for the duration of that membership year (see rationale under "About the eCF Requirements"). It can be obtained by logging into the eCF website with member credentials and accessing the Members area.

Public releases of the previous year eCF Requirements document will be done in the first quarter of the year and can be obtained on the eCF website in the Downloads area: https://eclinicalforum.org/downloads.

The linked .pdf file is provided in Appendix 5.

FEEDBACK: If you would like to provide feedback to these eCF Requirements or ask any questions, please submit in writing to REG@eclinicalforum.org. Please provide the eCF Requirements number and text your comments are referring to, as well as your contact information.

Copyright eClinical Forum

Copyright eClinical Forum 2026

Appendix 1: DISCLAIMER and LICENSE for FAIR USE of eCLINICAL FORUM MATERIALS

This work is the property of the eClinical Forum and is released under Creative Commons – Attribution-Non-Commercial-No Derivatives 4.0. Under the terms of the license, you are free to:

- Share, copy and redistribute the material in any medium or format

The licensor cannot revoke these freedoms if you follow the license terms.

Under the following terms:

- Attribution: You must give appropriate credit, provide a link to the license, and indicate if changes are made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
- Non-Commercial: You may not use the material for commercial purposes.
- No Derivatives: If you remix, transform, or build upon the material, you may not distribute the modified material.
- No additional restrictions: You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

Notices:

You do not have to comply with the license for elements of the material in the public domain or where your use is permitted by an applicable exception or limitation.

No warranties are given. The license may not give you all the permissions necessary for your intended use. For example, other rights such as publicity, privacy, or moral rights may limit how you use the material.

Copyright eClinical Forum

Copyright eClinical Forum 2026

Appendix 2: Basis for the 2025.1 Release

This release is based on the following documents that have been prepared and issued by regulatory authorities. These eCF Requirements are always evolving as the eCF REG continues to evaluate and map new regulatory authority documents as they come into effect. It is our intent to release updated mappings yearly. Future releases will include additional regulatory authority document mappings.

The below references are not all 'regulatory documents' as one customarily understands the phrase – some of them do not directly imply literal and strict observance by the industry as do the FDA Code of Federal Regulations, EU Regulations/Directives and other national legislations. For instance, *FDA Guidance for Industry* documents and *EMA Reflection Papers* are offered as suggested best practices. In an effort to provide a homogenous template for quality designs and risk assessments, the eCF chose not to differentiate between Regulations and Best Practices in the naming convention for its statements and calls them all **eCF *Requirements***; please refer to the Regulatory mapping section for each eCF Requirement in order to specifically assess the legal implications of non-conformance in your region.

In cases where we are using an English translation of a national document, if there is a conflict, then the national/original version is used to make the final mapping determination.

Documents from the following agencies have been mapped to the eCF Requirements:

- **EU-EMA:** European Union Medicines Agency
- **US-FDA:** United Stated Food and Drug Administration
- **UK-MHRA:** United Kingdom Medicines and Healthcare products Regulatory Agency
- **J-PPC:** Japan Personal Information Protection Commission
- **J-JPMA:** Japan Manufacturers Assoc (These documents are agreed by Japanese manufacturers and accepted by PMDA)
- **J-PMDA:** Japan Pharmaceutical and Medical Devices Agency
- **C-NMPA:** China National Medical Products Administration
- **C-MPS:** China Ministry of Public Security
- **TFDA:** Taiwan Food and Drug Administration
- **ISO**: International Organization for Standardization
- **ICH:** International Council on Harmonisation

Copyright eClinical Forum

Copyright eClinical Forum 2026

Additions in this paper are highlighted in bold. Where a link to the document is available, we have included it for convenience.

Source	Date	Title/Link
C-MPS		China Electronic Signature Law - **中华人民共和国**电子签**名法**. Electronic Signature Law of the People's Republic of China • Note – we have used an unofficial English translation of this document. It is available to eCF members in the eCF Members section of our website.
C-MPS	May, 2018	Chinese Personal Information Security Specification (1-May-2018)
C-NMPA		Clinical Trial Data Management Guide (non-official translation) (Judged by eCF REG review to have the same requirements for electronic data as ICH GCP, and therefore not separately mapped)
EU-EMA		EMA GCP Q&A (Q&A: Good clinical practice (GCP) | European Medicines Agency (europa.eu). The following questions were addressed: • B8. Contractual Arrangements with Vendors; April 2020 • B9. Sponsor Validation of Vendor Systems; April 2020 • B17. How can sponsors demonstrate oversight for those activities that are delegated by written contract? (December 2022) • C1 - What are the expectations of EU Competent Authorities concerning the use of electronic trial master files (e-TMFs)
EU-EMA	Oct, 2023	EMA Data Quality Framework for EU Medicines Regulation (Oct 2023)
EU-EMA	Mar, 2023	EMA Guideline on computerised systems and electronic data in clinical trials, (7-Mar-2023)
EU-EMA	Dec, 2018	EMA Guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic) (Dec 2018)
EU-EMA	Dec, 2013	EMA Reflection paper on the use of interactive response technologies (interactive voice/web response systems) in clinical trials, with particular emphasis on the handling of expiry dates (10-Dec-2013);
EU-EMA	Nov, 2013	EMA Reflection paper on risk based quality management in clinical trials (18-Nov-2013);
EU-EMA	Apr, 2016	EU General Data Protection Regulation 2016/679
EU-EMA	Jul, 2014	EU 910/2014 on Electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

Copyright eClinical Forum

 Copyright eClinical Forum 2026

Source	Date	Title/Link
EU-EMA	Dec, 2018	Guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic) (6-Dec-2018)
EU-EMA	Apr, 2005	EU Directive 2005/28/EC: Laying down principles and detailed guidelines for good clinical practice as regards investigational medicinal products for human use, as well as the requirements for authorisation of the manufacturing or importation of such products (GCP Directive).
EU-EMA	Jun, 2011	EU Annex 11 (EU regulatory requirement) • The Rules Governing Medicinal Products in the EU -Volume 4 - GMP Annex 11: Computerised Systems (June 2011);
EU-EMA	Apr, 2014	EU Regulation 536/2014 Clinical Trials (16 April 2014) Articles 57, 58
EU-EMA	2001	Directive 2001/20/EC of the European Parliament and of the conduct of clinical trials on medicinal products for human use (Clinical Trials Directive) (superseded by Regulation (EU) 536/2014).
EU-EMA	**Sep, 2024**	**Reflection paper on the use of Artificial Intelligence (AI) in the medicinal product lifecycle**
ICH	Nov, 2016	International Council on Harmonisation Guideline for Good Clinical Practices E6 R2 (9-Nov-2016); (considered regulatory requirement in EU) – this has now been superseded by ICH E6 R3 (6-Jan-2025)
ICH	**Jan, 2025**	**ICH_E6(R3)_Step4_FinalGuideline_2025_0106.pdf**
ISO	Jul, 2020	ISO 14155:2020 - Clinical investigation of medical devices for human subjects — Good clinical practice (Judged by eCF REG review to have the same requirements for electronic data as ICH GCP, and therefore not separately mapped.)
J-JPMA	Jan, 2012	Supplement to the Guidance for Electronic Data Capture in Clinical Trials; JPMA (10-Jan-2012)
J-JPMA	Nov, 2007	Guidance for electronic trial data capturing of clinical trials (01-Nov-2007);
J-PMDA	Apr, 2005	Using electromagnetic records and electronic signatures for application for approval or licensing of drugs (1-Apr-2005)
J-PMDA	Oct, 2010	Guideline on Management of Computerized Systems for Marketing Authorization Holders and Manufacturers of Drugs and Quasi-drugs

Copyright eClinical Forum

Copyright eClinical Forum 2026

Source	Date	Title/Link
J-PMDA	Jul, 2021	EDC Management Checklist (1-Jul-2021)
J-PMDA	2022	Act on Electronic Signatures and Certifications (Revised 2022)
J-PMDA	**Mar, 2023**	**PMDA Points to note regarding using information collected as electromagnetic records in CR and PMS**
J-PPC	Jun, 2020	Act on the Protection of Personal Information (Act No. 57 of 2003;) Enforcement date: June 17, 2020; (Revised by Law No. 68 of 2022)
J-PPC	May, 2017	Act_on_the_Protection_of_Personal_Information.pdf
TFDA	**Dec, 2023**	**Taiwan - Digital health technology applied in drug clinical trials Guidelines for executing remote data collection**
TFDA	**May, 2024**	**Guidance on computerized systems and electronic data in clinical trials**
UK-MHRA	Mar, 2018	MHRA Guidance on GxP Data Integrity, March 2018
UK-MHRA	Nov, 2020	MHRA & FDA: Data Integrity in Global Clinical Trials: Discussions From Joint US Food and Drug Administration and UK Medicines and Healthcare Products Regulatory Agency Good Clinical Practice Workshop
US-FDA		21 CFR Part 312, Investigational New Drug Application;
US-FDA		21 CFR Part 11 Electronic Records and Electronics Signatures
US-FDA	Aug, 2013	FDA Guidance for Industry: Oversight of Clinical Investigations – A Risk Based Approach to Monitoring (August 2013);
US-FDA	Sep, 2013	Guidance for Industry Electronic Source Data in Clinical Investigations (September 2013);
US-FDA	Sep, 2022	FDA Guidance Mobile Medical Applications Guidance –(Sept 28, 2022);
US-FDA	1996	USA Health Insurance Portability and Accountability Act; • This document was originally mapped as part of the HL7 Functional Profile project in 2010. It was reviewed again in light of current interpretations in 2019 and some mappings to eCF Requirements were adjusted.
US-FDA	Jul, 2018	FDA Use of Electronic Health Record Data in Clinical Investigations Guidance for Industry (July 2018);

Copyright eClinical Forum

Copyright eClinical Forum 2026

Source	Date	Title/Link
US-FDA		FDA 21 CFR Part 812 Investigational Device Exemptions
US-FDA	Jun, 2017	FDA Use of Electronic Records and Electronic Signatures in Clinical Investigations under 21 CFR Part 11 – Questions and Answers; June 2017
US-FDA UK-MHRA	Mar, 2020	FDA & MHRA: Data Integrity in Global Clinical Trials: Discussions From Joint US Food and Drug Administration and UK Medicines and Healthcare Products Regulatory Agency Good Clinical Practice Workshop
US-FDA	Dec, 2016	FDA Guidance Document: Use of Electronic Informed Consent in Clinical Investigations – Questions and Answers Guidance for Institutional Review Boards, Investigators, and Sponsors (Dec 2016)
US-FDA	Dec, 2023	FDA Digital Health Technologies for Remote Data Acquisition in Clinical Investigations (Dec 2023)
US-FDA	Dec, 2023	Real-World Data: Assessing Registries To Support Regulatory Decision-Making for Drug and Biological Products (Dec 2023)
US-FDA	**Oct, 2024**	**Electronic Systems, Electronic Records, and Electronic Signatures in Clinical Investigations: Questions and Answers; Guidance for Industry**
WHO	**2021**	**TRS 1033 - Annex 4: WHO Guideline on data integrity**

Copyright eClinical Forum

Copyright eClinical Forum 2026

Appendix 3: Documents Reviewed and Not Included as Basis for eCF Requirements

The eClinical Forum REG has reviewed many documents that, while providing value to the industry, do not provide specific basis for criteria for evaluating systems for clinical research. To provide a complete picture of the careful thought that has gone into the eCF Requirements, we offer this list of documents that eCF REG has reviewed and not used as a basis for eCF Requirements.

Upon consideration, the following types of documents are not used as a basis for the eCF Requirements.

- Documents pertaining to submission requirements
- Webinar slides and presentation notes from Regulatory Authorities
- Methodologies that are not legally mandated (e.g., ISO, GAMP, PDA, BSA, ACDM)
- Documents that are not freely available (i.e., available only via purchase)

In addition to documents in the above categories, the following documents were reviewed by REG and determined to be not appropriate for the eCF Requirements; however, they may be useful resources.

Source	Date	Title/Link
EU-EMA	May, 2020	EMA Guidance on remote GCP inspections during the COVID19 pandemic (18-May-2020)
US-FDA	Dec, 2009	Guidance for Industry Patient-Reported Outcome Measures: Use in Medical Product Development to Support Labeling Claims
US-FDA	Sep, 2024	Providing Regulatory Submissions in Electronic Format — Certain Human Pharmaceutical Product Applications and Related Submissions Using the eCTD Specifications Guidance for Industry
US-FDA	Apr, 2005	Providing Regulatory Submissions in Electronic Format — Content of Labeling; Guidance for Industry
US-FDA	Aug, 2003	Guidance for Industry Part 11, Electronic Records; Electronic Signatures — Scope and Application
US-FDA	Dec, 2017	Software as a Medical Device (SAMD): Clinical Evaluation; Guidance for Industry and Food and Drug Administration Staff; December 8, 2017
US-FDA	Sep, 2022	Policy for Device Software Functions and Mobile Medical Applications
US-FDA	Revision Apr, 2020	21 CFR 50, Protection of Human Subjects

Copyright eClinical Forum

Copyright eClinical Forum 2026

Source	Date	Title/Link
US-FDA	Revision Apr, 2020	21 CFR 56, Institutional Review Boards
US-FDA	Revision Apr, 2020	21CFR part 314.50 Application for FDA approval to market new drug
US-FDA	Sep, 2019	Changes to Existing Medical Software Policies Resulting from Section 3060 of the 21stCentury Cures Act Guidance for Industry
US-FDA	Apr, 2023	A Risk-Based Approach to Monitoring of Clinical Investigations Questions and Answers Guidance for Industry
US-FDA	Dec, 2023	Data Standards for Drug and Biological Product Submissions Containing Real-World Data | FDA
US-FDA	Apr, 2023	Risk-based approach to monitoring of clinical investigations Q&A
US-FDA	Dec, 2023	Data Standards for Drug and Biological Product Submissions Containing Real-World Data | FDA
US-FDA	Sep, 2024	Conducting Clinical Trials With Decentralized Elements | FDA
US-FDA	Aug, 2023	Considerations for the Use of Real-World Data and Real-World Evidence To Support Regulatory Decision-Making for Drug and Biological Products | FDA
US-FDA	May, 2007	Guidance for Industry: Computerized Systems Used in Clinical Investigations (May 2007);
UK-MHRA	Sep, 2018	Joint statement on seeking consent by electronic methods
UK-MHRA	Jul, 2015	MHRA Blog on Trial Master File
J-PMDA	Apr, 2015	Technical Conformance Guide on Electronic Study Data Submissions (PFSB/ELD/OMDE Notification No. 0427001, April 27, 2015)
J-PMDA	Oct, 2010	Questions and Answers (Q and A) regarding the Guideline on Management of Computerized Systems for Marketing Authorization Holders and Manufacturers of Drugs and Quasi-drugs (PFSB/CNB Administrative Notification October 21, 2010)
J-PMDA	June, 2014	Basic Principles on Electronic Submission of Study Data for New Drug Applications (PFSB/ELD Notification 0620-6, June 20, 2014)

Copyright eClinical Forum

Copyright eClinical Forum 2026

Source	Date	Title/Link
J-PMDA	July, 2013	Basic Rules of the Risk-Based Approach to Monitoring Clinical Trials (PFSB/ELD Notification, 1 July 2013)
J-PMDA	Apr, 2015	Notification on Practical Operations of Electronic Study Data Submissions (PFSB/ELD Notification 0427-1, April 27, 2015)
J-PMDA	Oct, 2010	Guideline on Management of Computerized Systems for Marketing Authorization Holders and Manufacturers of Drugs and Quasi-drugs
J-PMDA	Apr, 2015	Technical Conformance Guide on Electronic Study Data Submissions (PFSB/ELD/OMDE Notification No. 0427001, April 27, 2015)
J-PMDA	Jul, 2014	The Basic Rules for Using Electromagnetic records for Clinical Study-Related Documents
Brazil ANVISA	Apr, 2020	Guide for Computerized System Validation
Non-Reg	Dec, 2019	SCDM: Good Clinical Data Management Practices
Non-Reg	May, 2023	ECRIN (European Clinical Research Infrastructure Network) Requirements for Certification
Non-Reg	Mar, 2017	International Society of Pharmaceutical Engineering – GAMP Guide: Records and Data Integrity
Non-Reg	Sep, 2007	PIC/s Good Practices for Computerised Systems in Regulated 'GXP' Environments
Non-Reg	Jul, 2021	PIC/S Guidance on Data Integrity
ISO	Jul, 2020	ISO 14155:2020 - Clinical investigation of medical devices for human subjects — Good clinical practice
OECD	Dec, 2024	OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring | OECD
US-FDA	Sep, 2022	Policy for Device Software Functions and Mobile Medical Applications, SEP 2022
EU-EMA		EMA: eSubmission information web page
US-FDA	Apr, 2022	Guidance for Industry-Providing Submissions in Electronic Format — Postmarketing Safety Reports for Vaccines DRAFT June 2014

Copyright eClinical Forum

Copyright eClinical Forum 2026

Source	Date	Title/Link
US-FDA	Apr, 2022	Providing Regulatory Submissions in Electronic and Non-Electronic Format—Promotional Labeling and Advertising Materials for Human Prescription Drugs
US-FDA	Jun, 2009	Providing Regulatory Submissions in Electronic Format – Drug Establishment Registration and Drug Listing; Guidance for Industry
US-FDA	Sep, 2024	Providing Regulatory Submissions in Electronic Format - Human Pharmaceutical Product Applications and Related Submissions Using the eCTD Specifications; Guidance for Industry
US-FDA	Feb, 2014	Providing Regulatory Submissions in Electronic Format--Receipt Date; Guidance for Industry
US-FDA	Jul, 2013	Providing Submissions in Electronic Format – Postmarket Non-Expedited ICSRs Technical Questions and Answers' Guidance for Industry
US-FDA	Apr, 2022	Providing Submissions in Electronic Format — Postmarketing Safety Reports
US-FDA	Jun, 2021	Providing Submissions in Electronic Format -- Standardized Study Data; Guidance for Industry
US-FDA	Jun, 2023	Electronic Submissions Presentations
US-FDA	Jan, 2014	FDA D33Training: Final Guidance on Electronic Source Data in Clinical Investigations
ICH		ICH: ESTRI Index (M2, E2B, M8): Electronic Standards for the Transmission of Regulatory Information
J-PMDA	Jun, 2014	Question and Answer Guide Regarding "Basic Principles on electronic Submission of Study Date for New Drug Applications" (PFSB/ELD Administrative Notice June 20, 2014)
J-PMDA	Apr, 2015	Question and Answer Guide Regarding "Notification on Practical Operations of Electronic Study Data Submissions" (PFSB/ELD Administrative Notice April 27, 2015)
ICH	Oct, 2021	ICH E8 R1 General Consideration for Clinical Studies

Copyright eClinical Forum

Copyright eClinical Forum 2026

Appendix 4: Abbreviations and Definitions

Abbreviations

Abbreviation	Meaning
CFR	Code of Federal Regulations (US)
CRF	Case Report Form
CRO	Contract Research Organization
DAT	Data Acquisition Tool
DHT	Digital Health Technology
EDC	Electronic Data Capture
EHR	Electronic Health Record
EMR	Electronic Medical Records
eTMF	electronic Trial Master File
eSRA	e-Site System Readiness Assessment
GCP	Good Clinical Practice
RWD	Real World Data
RWE	Real World Evidence

Definitions

Term	Definition
Audit trail / Audit log	A secure, computer generated, time-stamped electronic record that allows reconstruction of the course of events relating to the creation, modification, and deletion of an electronic record.
Case Record	An original entry (or certified copy thereof) which is under the exclusive control of the Investigator and is submitted as part of the Case Report to the Sponsor and IRB/IEC. Examples of Case/data records are CRF entries, outcome assessments, patient questionnaire responses, laboratory results, ECG tracings, etc..
Certified Copy	A copy (irrespective of the type of media used) of the original record that has been verified (i.e., by a dated signature or by generation through a validated

Copyright eClinical Forum

Copyright eClinical Forum 2026

Term	Definition
	process) to have the same information, including data that describe the context, content, and structure, as the original.
Clinical trial	Any investigation in human subjects intended to discover or verify the clinical, pharmacological, and/or other pharmacodynamic effects of an investigational product(s), and/or to identify any adverse reactions to an investigational product(s), and/or to study absorption, distribution, metabolism, and excretion of an investigational product(s) with the object of ascertaining its safety and/or efficacy. The terms clinical trial and clinical study are synonymous.
Core system	A core system includes the application(s) that do not include the trial-specific configurations. It is what comes "out-of-the-box" with every study before any study-specific elements are added.
Contract Research Organization (CRO)	A person or an organization (commercial, academic or other) contracted by the sponsor to perform one or more of a sponsor's trial related duties and functions. For the purpose of this document, the CRO acts as an extension of the sponsor.
Data Originator	A person, a computer system, a device, or a lab instrument that is authorized to enter, change, or transmit data elements (also sometimes known as an author).
EDC System	An Electronic Data Capture (EDC) system consists of a user interface, i.e., web pages and reports, programming logic (e.g., computer programs, scripts) and a repository of data (e.g., database) using services from Infrastructure Systems.
EMR / EHR	Electronic Medical Record, Electronic Health Record – for purposes of completing an eSRA assessment of your healthcare system, these terms are interchangeable
EHRCR	The global EHRCR Functional Profile Project is a collaborative effort to expand and adapt the functionality of EHR and associated systems, networks, and processes to support clinical research. The project is aimed at developing a Functional Profile that identifies critical capabilities for the conduct of clinical research utilizing EHR systems and establishes conformance to the HL7 EHR Functional Model and the Q-Rec EHR Certification Criteria. HL7 Health Level-7 refers to a set of international standards for transfer of clinical and administrative data between hospital information systems.
IoMT	Internet of Medical Things. The Internet of Medical Things (IoMT) is the collection of medical devices and applications that connect to healthcare IT systems through online computer networks. Medical devices equipped with Wi-Fi allow the machine-to-machine communication that is the basis of IoMT. ... IoMT is also known as healthcare IoT.

Copyright eClinical Forum

Copyright eClinical Forum 2026

Term	Definition
Investigator	A person responsible for the conduct of the clinical trial at a trial site. If a trial is conducted by a team of individuals at a trial site, the investigator is the responsible leader of the team and may be called the principal investigator.
IT, Site IT	Information Technology. IT should include a Data Privacy Officer and Records Retention staff particularly during set-up and maintenance of clinical research systems.
Metadata	The contextual information required to understand a given data element. Metadata is structured information that describes, explains or otherwise makes it easier to retrieve, use or manage data.
Research Protocol	(Also called Clinical Trial Protocol) A document that describes the objective(s), design, methodology, statistical considerations, and organization of a trial. The protocol usually also gives the background and rationale for the trial, but these could be provided in other protocol referenced documents. Throughout the ICH GCP Guidance, the term protocol refers to protocol and protocol amendments.
Sponsor	An individual, company, institution or organization that takes responsibility for the initiation, management and or/financing of a clinical trial.
Transient Data Collector	Devices, in that they acquire data, temporarily store it in files, but as part of normal workflow, pass the data onto databases before the process task is complete
Trusted Third Party	Third party entities who collect data on behalf of an investigator and maintain independence from sponsor control.
Unsuccessful vs Unauthorized access attempt	An “unsuccessful” access attempt refers to a legitimate user forgetting their access information (e.g., their username or password). An “unauthorized” access attempt refers to a non-user attempting to gain access (e.g., through hacking).

Copyright eClinical Forum

Appendix 5: ECF REQUIREMENTS Public Release V2025

See next page.

Copyright eClinical Forum 2026

eCF Requirement Report

Please see *Disclaimer and License For Fair Use Of eClinical Forum Materials*

ID	Description	Version	Mapping Version
C01	System has the ability to store and retrieve data items in a way that is **attributable** to a trial/data subject.	4	33
C02	Specified **de-identified** data can be extracted for clinical research.	2	23
C03	System has capability of storing data related to **subject consent** and should not allow data collection until the subject consent is confirmed.	3	14
C04	The system **audit trail** must: - be indelible, readable and readily available for review and copying. - include date, time, originator of any data creation, change or deletion, and when required the reason for change.	6	130
C10	There is a process to ensure that case **records** and any subsequent modifications are **reviewed and approved** by the investigator.	5	21
C11	There is a system and/or process to ensure the **investigator has control** of and continuous access to all essential records (data and documents) generated by the investigator/institution/patient before, during and after the trial.	6	46
C13	Controls exist such that the ability to **change system settings** is limited to authorized personnel.	4	16
C14	System uses a **standard time** reference such that the local time can be derived.	5	16
C16	There are system features and processes to create, maintain, revoke, and document the history of **user access, roles and privileges** over time.	4	107
C17	There is a policy and training that instructs users **not to share** their **access** mechanisms (e.g. usernames and passwords, or access keys) or to leave their account open for others to use. A shared account (or group account) is not appropriate.	6	34
C18	The monitor, auditor, investigator and inspector can within a reasonable timeframe obtain **direct access** to relevant clinical trial records in order to perform their regulatory duties.	5	51
C19	System limits the number of **log-in attempts** and records unsuccessful attempts.	3	14
C20	System records and notifies a system administrator of **unauthorized** access **log-in attempts**.	2	21
C21	There are system features and processes to manage, preclude and report on **security issues** following current physical and logical **information security** best practices.	7	71
C22	System feature to allow **automatic logoff** or other access lock (such as password protected screen saver) after a set period of time of inactivity.	3	8
C24	System has the ability to produce a **human-readable** copy of data (which includes associated audit trails and any decoded data) in appropriate file formats that facilitate review, searching and analysis.	4	23
C25	Copies of electronic records must be **certified copies** if they are being used for regulatory purposes	4	29
C26	There are sufficient system and/or process controls for **backup and recovery** procedures. Documentation can be produced for **inspection** by a monitor, auditor or inspector.	4	38
C28	Process and/or system controls ensure that regulated data used for clinical research, including source data and metadata are enduring, continue to be available, readable and understandable and are retained in an **archive** for the legal period.	4	85
C29	There are sufficient process controls for the system covering **Business Continuity** to manage disruptive incidents.	4	21
C30	There are sufficient process controls based on industry standards, covering **Disaster Recovery** Procedures.	6	22
C31	There is a process to demonstrate that individuals who develop, maintain, or use the system should be qualified by having appropriate **education, training**, and experience necessary to perform their assigned task.	3	72
C32	The development, hosting, deployment and change control of a computerised system has objective evidence that system components are traceable to requirements and have been **validated** based on risk, using good **software lifecycle** practices.	8	142
C36	There are sufficient system and/or process controls over **data transfers and migrations** from/to systems to ensure the integrity of data, and continued availability of the audit trail.	8	87
C37	When **service providers** are used to provide GxP-related services, **formal agreements** must exist and include clear statements of the roles and responsibilities, management and oversight of the service provider (and their GxP-related providers).	7	63
	Signed electronic records shall contain information associated with the **signing** that clearly indicates all of the following:		

Copyright eClinical Forum

C39	- The **name** of the signer - The **date** and time when the signature was executed - The **meaning** (such as creation, confirmation or approval) - Electronic signatures are permanently linked to their respective record - If the record is subsequently altered, then the signature no longer applies	7	33
C40	There are sufficient system and/or process controls to ensure the **privacy of subjects**. In the event of a **security incident** that exposes privacy data, the Sponsor and/or Investigator shall notify the relevant Data Protection or other applicable authority.	6	21
C41	There is a process to evaluate and mitigate the **risk** and impact **of changes** to the computerised system taking into account changes to protocol (i.e. amendments and addendums), users, & roles on an ongoing basis.	5	52
C43	There is a process to periodically review and affirm the **continued suitability** of the computerised system taking into account the potential cumulative risks and impacts of changes to the system, requirements, version releases and computing environment of the system.	7	55
C44	The eTMF **audit trail** shall additionally capture the **accessing** of records.	4	4
C45	There are processes to **address** incidents for the computerised system that identify, assess, resolve, and close: actions, **software anomalies** (bugs), **IT issues**, and **Help desk** issues.	2	10
C46	A detailed diagram and description of the transmission of electronic data (data flow) should be available in the protocol or a protocol-related document.	1	7

Copyright eClinical Forum

Regulatory mapping for eCF Requirement ID C01

System has the ability to store and retrieve data items in a way that is **attributable** to a trial/data subject.

Regulation	Paragraph	Description
FDA 21 CFR Part 11 Q and A	Q20b	If a participant manually enters data into the DHT (e.g., when using an electronic patient-reported outcome mobile application or when performing a task-based measure, such as a cognitive test), the participant should be identified as the data originator.
FDA 21 CFR Part 312	62b	An investigator is required to prepare and maintain adequate and accurate case histories that record all observations and other data pertinent to the investigation on each individual administered the investigational drug or employed as a control in the investigation. Case histories include the case report forms and supporting data including, for example, signed and dated consent forms and medical records including, for example, progress notes of the physician, the individual's hospital chart(s), and the nurses' notes. The case history for each individual shall document that informed consent was obtained prior to participation in the study.
Japanese APPI	Article 33	The person may request disclosure of retained personal data from a business operator handling personal information by providing an electromagnetic record of the retained personal data that identifies the person concerned or by other methods specified by the rules of the Personal Information Protection Commission.
FDA CSUCI	F2a	The computerized system should be designed in such a way that retrieved data regarding each individual subject in a study is attributable to that subject.
EMA Computerised Systems	4.1.a	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.
EMA Computerised Systems	4.1.b	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.
EMA Computerised Systems	4.5.a	Data should be attributable to the person and/or system generating the data.
EMA Computerised Systems	4.5.f	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).
EMA Computerised Systems	6.1.3	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).
EMA eTMF Guideline	4.1.3b	The documentation in the investigator TMF includes some source documents containing personal data that enable the data subjects to be directly identified (i.e. direct identifiers of trial subjects).
EU Directive 2005 28	2.1.5	All clinical trial information shall be recorded, handled, and stored in such a way that it can be accurately reported, interpreted and verified, while the confidentiality of records of the trial subjects remains protected.
FDA eSource Guidance	Background	Source data includes all information in original records and certified copies of original records of clinical findings, observations, or other activities in a clinical investigation used for reconstructing and evaluating the investigation. Access to source data is critical to the review and inspections of clinical investigations. The review of source data by both the FDA and sponsor is important to ensure adequate protection of the rights, welfare, and safety of human subjects and the quality and integrity of the clinical investigation data. Source data should be attributable, legible, contemporaneous, original, and accurate (ALCOA) and must meet the regulatory requirements for recordkeeping. Capturing source data electronically and transmitting it to the eCRF should: - Eliminate unnecessary duplication of data - Reduce the possibility for transcription errors - Encourage entering source data during a subjects visit, where appropriate - Eliminate transcription of source data prior to entry into an eCRF - Facilitate remote monitoring of data - Promote real-time access for data review - Facilitate the collection of accurate and complete data
EU GDPR	Article 15	The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed.
ICH E6 GCP R3 Good Clinical	III.2.12.10d	Where equipment for data acquisition is provided to trial participants by the investigator, ensure that traceability is maintained and that participants are provided with appropriate training.

Copyright eClinicalForum

Practice		
ICH E6 GCP R3 Good Clinical Practice	III.2.12.8	Data reported to the sponsor should be identified by an unambiguous participant code that can be traced back to the identity of the participant by the investigator/institution.
ICH E6 GCP R3 Good Clinical Practice	III.3.16.1s	The sponsor should use an unambiguous trial participant identification code that allows identification of all the data reported for each participant.
ICH GCP	2.10	All clinical trial information should be recorded, handled, and stored in a way that allows its accurate reporting, interpretation and verification. ADDENDUM - This principle applies to all records referenced in this guideline, irrespective of the type of media used.
ICH GCP	4.9.0	The investigator/institution should maintain adequate and accurate source documents and trial records that include all pertinent observations on each of the site's trial subjects. Source data should be attributable, legible, contemporaneous, original, accurate, and complete. Changes to source data should be traceable, should not obscure the original entry, and should be explained if necessary (e.g., via an audit trail).
ICH GCP	4.9.7	Upon request of the monitor, auditor, IRB/IEC, or regulatory authority, the investigator/institution should make available for direct access all requested trial related records.
ICH GCP	5.5.5	The sponsor should use an unambiguous subject identification code (see 1.58) that allows identification of all the data reported for each subject.
JPMA EDC Guidance	4.2.2	Clinical data captured can be displayed on screen or printed on paper as forms or inventory for each clinical case.
JPMA EDC Supplement	1.2a	...it is required to prepare necessary equipment (e.g. devices) and environment (e.g. internet line, telephone line) for data entry by subjects, make operational procedures for transmitting subject data to the operational database, operational procedures for providing the collected subject data to investigators. and sponsors, and also procedures for data retention after completion of the clinical trial and location of storage.
NMPA PISS	7.4	Personal information controllers should provide personal information subjects with access to the following information: a) the personal information or type of information it holds about the subject; b) the source of the above personal information and the purpose for which it was used; c) The identity or type of the third party who has obtained the above personal information.
Taiwan Computerized Systems	4.1.a	In order for the data to fully support related outcome and decision-making, ALCOA++ principles of being attributable, legible, contemporaneous, original, accurate, complete, consistent, enduring, available when needed and traceable should be applied to achieve data integrity.
Taiwan Computerized Systems	4.5.a	Data should be attributable to the person, system and/or equipment generating the data.
Taiwan Computerized Systems	4.5.f	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).
Taiwan Computerized Systems	6.1.3	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).

Copyright eClinical Forum

Regulatory mapping for eCF Requirement ID C02

Specified **de-identified** data can be extracted for clinical research.

Regulation	Paragraph	Description
FDA 21 CFR Part 312	60	...investigator is responsible for protecting the rights, safety, and welfare of the subject.
FDA 21 CFR Part 312	68	An investigator shall upon request from any properly authorized officer or employee of FDA, at reasonable times, permit such officer or employee to have access to, and copy and verify any records or reports made by the investigator pursuant to 312.62. The investigator is not required to divulge subject names unless the records of particular individuals require a more detailed study of the cases, or unless there is reason to believe that the records do not represent actual case studies, or do not represent actual results obtained.
21 CFR Part 56	111.a.7	Where appropriate, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data.
EMA eTMF Guideline	4.1.3c	In general, information (data/documents) shared with the sponsor/CRO or uploaded into a database or filing system that is managed by the sponsor/CRO, should only contain data of trial subjects, which has been pseudonymised.
EMA eTMF Guideline	4.1.3h	Remote access by sponsor or CRO personnel to the investigator TMF should only be possible to the documents where personal data that enable the data subjects to be directly identified (i.e. direct identifiers of trial subjects) is not present or has been pseudonymised.
EU Directive 2005 28	2.1.5	All clinical trial information shall be recorded, handled, and stored in such a way that it can be accurately reported, interpreted and verified, while the confidentiality of records of the trial subjects remains protected.
EU GDPR	Article 20.2	In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.
EU GDPR	Article 20.3	The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
EU GDPR	Article 25.1	The controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation.
ICH GCP	2.11	The confidentiality of records that could identify subjects should be protected, respecting the privacy and confidentiality rules in accordance with the applicable regulatory requirement(s).
NMPA Clinical Trial DM Guide	5.14.2	Personal privacy protection measures in the design of the database should be considered at the technical level, without affecting the integrity of the data and does not violate the principles of GCP does not include as much as possible under the conditions of the protected health information, such as: the database should not be included under Full name of those tested, but should record the full name abbreviations. In Chinese name, for example, should use the first letter of the subjects surname and first name initials.
NMPA PISS	6.2	After collecting personal information, the personal information controller should immediately perform de-identification processing and take technical and management measures to store the de-identified data separately from the information that can be used to recover the identified individuals, and ensure the follow-up individuals. Individuals are not re-identified in information processing.

Copyright eClinical Forum

Regulatory mapping for eCF Requirement ID C03

System has capability of storing data related to **subject consent** and should not allow data collection until the subject consent is confirmed.

Regulation	Paragraph	Description
FDA 21 CFR Part 312	62b	An investigator is required to prepare and maintain adequate and accurate case histories that record all observations and other data pertinent to the investigation on each individual administered the investigational drug or employed as a control in the investigation. Case histories include the case report forms and supporting data including, for example, signed and dated consent forms and medical records including, for example, progress notes of the physician, the individual's hospital chart(s), and the nurses' notes. The case history for each individual shall document that informed consent was obtained prior to participation in the study.
21 CFR Part 812	140.a.3	(a) Investigator records. A participating investigator shall maintain the following accurate, complete, and current records relating to the investigators participation in an investigation:... (3) Records of each subjects case history and exposure to the device. Case histories include the case report forms and supporting data including, for example, signed and dated consent forms and medical records including, for example, progress notes of the physician, the individuals hospital chart(s), and the nurses notes.
Japanese APPI	Article 18	A business operator handling personal information shall not handle personal information beyond the scope necessary to achieve the purpose of use specified in accordance with the provisions of the preceding article, without obtaining the prior consent of the person.
Japanese APPI	Article 27	A business operator handling personal information shall not provide personal data to a third party without obtaining the prior consent of the person.
Japanese APPI	Article 28	A business operator handling personal information shall be a foreign country (meaning a country or region outside Japan… Excluding those specified by the rules of the Personal Information Protection Commission as foreign countries that have a system regarding the protection of personal information that is recognized to be at the same level as Japan in terms of protection...) ...a business operator handling personal information is required to take pursuant to the provisions of this Section regarding the handling of personal data... the consent of the person to the effect that the provision to a third party in a foreign country is permitted must be obtained in advance.
EU Directive 2001 20	16	The person participating in a clinical trial must consent to the scrutiny of personal information during inspection by competent authorities and properly authorised persons, provided that such personal information is treated as strictly confidential and is not made publicly available.
FDA A Risk-Based Approach to Monitoring	III.B.2.a	Verification of subjects informed consent is a critical activity that should be monitored.
FDA A Risk-Based Approach to Monitoring	IV.a	Verification that informed consent was obtained appropriately
FDA Real World Data	III.Ce	Sponsors should address whether the registry has privacy and security controls in place to ensure that the confidentiality and security of data are preserved.
EU GDPR	Recital 42	Where processing is based on the data subject consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation.
ICH E6 GCP R3 Good Clinical Practice	II.2.1	Freely given informed consent should be obtained and documented from every participant prior to clinical trial participation.
ICH E6 GCP R3 Good Clinical Practice	III.2.8.7	Prior to trial participation, the informed consent form should be signed and dated by the participant or by the participant’s legally acceptable representative and, where appropriate, by an impartial witness and by the investigator or delegated investigator site staff who conducted the informed consent discussion.
ICH GCP	2.9	Freely given informed consent should be obtained from every subject prior to clinical trial participation.
ICH GCP	4.8.8	Prior to a subjects participation in the trial, the written informed consent form should be signed and personally dated by the subject or by the subject's legally acceptable representative, and by the person who conducted the informed consent discussion.
NMPA PISS	5.5a	When collecting sensitive personal information, you should obtain explicit consent from the subject of your personal information. It should be ensured that the express consent of the subject of personal information is a concrete, clear and unambiguous expression of wishes that is voluntarily given on a fully informed basis.

Copyright eClinical Forum

Regulatory mapping for eCF Requirement ID C04

The system **audit trail** must:
- be indelible, readable and readily available for review and copying.
- include date, time, originator of any data creation, change or deletion, and when required the reason for change.

Regulation	Paragraph	Description
FDA 21 CFR Part 11	10b	(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.
FDA 21 CFR Part 11	10e	(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.
FDA 21 CFR Part 11 Q and A	Q11d	...it is nonetheless important to have audit trails or other physical, logical, or procedural security measures in place to ensure the trustworthiness and reliability of the electronic records.
FDA 21 CFR Part 11 Q and A	Q12	To ensure the trustworthiness and reliability of electronic records, audit trails must capture electronic record activities including all changes made to the electronic record, the individuals making the changes, and the date and time of the changes and should include the reasons for the changes.
FDA 21 CFR Part 11 Q and A	Q20a	As part of an audit trail, each electronic data element should be associated with an authorized data originator.
Japanese APPI	Article 23	A business operator handling personal information must take necessary and appropriate measures to prevent leakage, loss or damage of the personal data it handles and to otherwise manage the security of personal data.
FDA CSUCI	D2a	It is important to keep track of all changes made to information in the electronic records that document activities related to the conduct of the trial (audit trails).
FDA CSUCI	D2b	The use of audit trails or other security measures helps to ensure that only authorized additions, deletions, or alterations of information in the electronic record have occurred and allows a means to reconstruct significant details about study conduct and source data collection necessary to verify the quality and integrity of data.
FDA CSUCI	D2c	Computer-generated, time-stamped audit trails or other security measures can also capture information related to the creation, modification, or deletion of electronic records and may be useful to ensure compliance with the appropriate regulation.
FDA CSUCI	D2f	Computer-generated, time-stamped electronic audits trails are the preferred method for tracking changes to electronic source documentation.
FDA CSUCI	D2g	Audit trails or other security methods used to capture electronic record activities should describe when, by whom, and the reason changes were made to the electronic record.
FDA CSUCI	D2h	Original information should not be obscured though the use of audit trails or other security measures used to capture electronic record activities.
PMDA EDC Management Sheet version 2	49 and 54	Outline of audit trails on creation / modification of retained information - Does the system have full audit trail capability? - Does the system clearly identify who created the data? - Does the system clearly identify which data was automatically calculated/derived - Does the system clearly determine who is responsible for the data loaded from other systems? - Does the system clearly identify who modified the data? - Does the system retain (i.e. not to obscure) the information before modification? - Does the system provide sponsors with the view of the audit trails? - Does the system provide staff at the medical institutions with the view of the audit trails? (During the conduct of clinical trials and after completion of clinical trials)
PMDA EDC Management Sheet version 2	66	Does the system ensure the readability of retained information? (During the conduct of clinical trials and after completion of clinical trials)
PMDA EDC Management Sheet version	68	Does the system ensure the readability of retained information? (After completion of clinical trials)

Copyright eClinical Forum

2		
EMA Computerised Systems	4.1.b	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.
EMA Computerised Systems	4.3	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).
EMA Computerised Systems	4.5.b2	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.
EMA Computerised Systems	4.5.f	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).
EMA Computerised Systems	5.5	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.
EMA Computerised Systems	6.1.3	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).
EMA Computerised Systems	6.2.1.a	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.
EMA Computerised Systems	6.2.1.b	...for an audit trail to be deactivated by "admin users", this should automatically create an entry into a log file (e.g. audit trail).
EMA Computerised Systems	6.2.1.c	Entries in the audit trail should be protected against change, deletion, and access modification (e.g. edit rights, visibility rights).
EMA Computerised Systems	6.2.1.d	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.
EMA Computerised Systems	6.2.1.f	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).
EMA Computerised Systems	6.2.1.i	Changes to data should only be performed when justified. Justification should be documented.
EMA Computerised Systems	A3.3.b	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.
EMA Computerised Systems	A5.1.1.1	The (ePRO) timestamp should record the time of the data entry and not only the time of the data submission/transmission.
EMA Computerised Systems	A5.1.1.2.b	In addition to the general requirements on audit trails, 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.
EMA eTMF Guideline	4.1.2e	The primary eTMF is a system for managing documents that should contain the controls listed below: an audit trail in place to identify date/time/user details for creation and/or uploading deletion of and changes to a document (explanation of the deletion or modification, if necessary);
EMA eTMF Guideline	4.2b	The sponsor and/or investigator/institution should implement risk-based quality checks (QC) or review processes to ensure the TMF is being maintained up-to-date and that all essential documents are appropriately filed in the TMF. Areas to consider during QC and review include the following: - review of the audit trail (for eTMF).
EMA eTMF Guideline	5	Particular attention should be paid when documents are stored on electronic, magnetic, optical or other non-indelible media. In such cases suitable controls should be implemented to ensure that these documents are complete and cannot be altered without appropriate authorisation and the creation of an audit trail.
EMA IRT Reflection Paper	2.2.3g	A readily accessible audit trail - audit trails should be available for all data including any alterations to the data either as a result of interacting with the system or manual interventions.

Copyright eClinical Forum

MHLW ERES (Japan)	3.1.1.2	Distinction of the creator of maintained information shall be definite. And also when modify the maintained information, previously recorded information shall be stored, and distinction of the modifier shall be definite. Audit trail shall be recorded by automatically, and recorded audit trail is desirable to be confirmed by predetermined procedure.
MHLW ERES (Japan)	3.1.2	Readability of electromagnetic records The contents of electromagnetic records shall be output (output to display, output to paper and copy to electronic storage media) as human readable format.
MHLW ERES (Japan)	3.1.3	Storability electromagnetic records Electromagnetic records shall be maintained with keeping its authenticity and readability.
EU Annex 11	12.4	Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.
EU Annex 11	9	Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.
EU Directive 2005 28	2.4.17	The sponsor and the investigator shall retain the essential documents relating to a clinical trial for at least five years after its completion.They shall retain the documents for a longer period, where so required by other applicable requirements or by an agreement between the sponsor and the investigator. Essential documents shall be archived in a way that ensures that they are readily available, upon request, to the competent authorities.The medical files of trial subjects shall be retained in accordance with national legislation and in accordance with the maximum period of time permitted by the hospital, institution or privatepractice.
EU Clinical Trials Regulation 536 2014	58f	Any alteration to the content of the clinical trial master file shall be traceable.
EU Electronic Identification Regulation 910-2014	26.d	An advanced electronic signature shall meet the following requirements: (d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.
FDA EHR Guidance	V.B.3	Audit trails are available to track changes to data.
FDA EHR Guidance	V.C.1	Each electronic data element should be associated with a data originator.
FDA EHR Guidance	V.C.2.b	Modified and corrected data elements should have data element identifiers that reflect the date, time, data originator, and the reason for the change.
FDA EHR Guidance	V.C.2.c	Modified and corrected data should not obscure previous entries.
FDA eSource Guidance	A3	The eCRF should include the capability to record who entered or generated the data and when it was entered or generated. Changes to the data must not obscure the original entry, and must record who made the change, when, and why.
FDA and MHRA Data Integrity Discussions	P3a	Audit trails for data entry should have an automatic function to show what data element was changed, what the change was, who changed it, when and why it was changed, and not obscure the original entry and any previous changes.
FDA and MHRA Data Integrity Discussions	P3b	It is important that audit trails can be easily accessed and reviewed during the study, as part of a dynamic system, and once the data are archived, which may be in a static format.
FDA and MHRA Data Integrity Discussions	P9a	Audit trails should be available to allow reconstruction of all changes to the study data.
FDA Real World Data	III.Cc	Conformance with 21 CFR part 11, as applicable, including maintenance of access controls and audit trails to demonstrate the provenance of the registry data and to support traceability of the data
FDA Real World Data	III.Cf	Implement and maintain version control by documenting the date, time, and originator of data entered in the registry; performing preventative and/or corrective actions to address changes to the data (including flagging erroneous data without deleting the erroneous data, while inserting the corrected data for subsequent use); and describing reasons for any changes to data without obscuring previous entries
EU GDPR	Article 19	The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Articles 16, 17(1) and 18 to each recipient to whom the personal data have been disclosed.
EU GDPR	Article 28h	(Processor) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

Copyright eClinical Forum

EU GDPR	Recital 82	In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility.
USA HIPAA	164.312b	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
USA HIPAA	164.312c1	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.
ICH E6 GCP R3 Good Clinical Practice	II.9.4	Clinical trials should incorporate efficient and robust processes for managing records (including data) to help ensure that record integrity and traceability are maintained and that personal information is protected.
ICH E6 GCP R3 Good Clinical Practice	III.2.12.2b	Source records should be attributable, legible, contemporaneous, original, accurate and complete. Changes to source records should be traceable, should not obscure the original entry and should be explained if necessary (via an audit trail).
ICH E6 GCP R3 Good Clinical Practice	III.2.12.6	Changes or corrections in the reported data should be traceable, should be explained (if necessary) and should not obscure the original entry.
ICH E6 GCP R3 Good Clinical Practice	III.3.11.4.5.1c	Informing the investigator or other parties and individuals involved in the trial conduct of entry errors or omissions in source record(s) and/or data acquisition tools and ensuring that corrections, additions or deletions are made as appropriate, dated and explained (if necessary) and that approval of the change is properly documented.
ICH E6 GCP R3 Good Clinical Practice	III.3.16.2c	The sponsor should ensure the traceability of data transformations and derivations during data processing and analysis.
ICH E6 GCP R3 Good Clinical Practice	III.3.16.2e	Such data changes should be authorised by the investigator and reflected in an audit trail.
ICH E6 GCP R3 Good Clinical Practice	III.4.2.1b	Acquired data from any source, including data directly captured in a computerised system (e.g., data acquisition tool), should be accompanied by relevant metadata.
ICH E6 GCP R3 Good Clinical Practice	III.4.2.2aii	Evaluating the system for the types and content of metadata available to ensure that: Systems are designed to permit data changes in such a way that the initial data entry and any subsequent changes or deletions are documented, including, where appropriate, the reason for the change.
ICH E6 GCP R3 Good Clinical Practice	III.4.2.2aiii	Evaluating the system for the types and content of metadata available to ensure that: Systems record and maintain workflow actions in addition to direct data entry/changes into the system.
ICH E6 GCP R3 Good Clinical Practice	III.4.2.2b	Ensuring that audit trails, reports and logs are not disabled. Audit trails should not be modified except in rare circumstances (e.g., when a participant’s personal information is inadvertently included in the data) and only if a log of such action and justification is maintained.
ICH E6 GCP R3 Good Clinical Practice	III.4.2.2c	Ensuring that audit trails and logs are interpretable and can support review.
ICH E6 GCP R3 Good Clinical Practice	III.4.2.4	There should be processes to correct data errors that could impact the reliability of the trial results. Corrections should be attributed to the person or computerised system making the correction, justified and supported by source records around the time of original entry and performed in a timely manner.
ICH GCP	4.9.0	The investigator/institution should maintain adequate and accurate source documents and trial records that include all pertinent observations on each of the site's trial subjects. Source data should be attributable, legible, contemporaneous, original, accurate, and complete. Changes to source data should be traceable, should not obscure the original entry, and should be explained if necessary (e.g., via an audit trail).
ICH GCP	4.9.3	Any change or correction to a CRF should be dated, initialled, and explained (if necessary) and should not obscure the original entry (i.e. an audit trail should be maintained); this applies to both written and electronic changes or corrections (see 5.18.4(n)). Sponsors should provide guidance to investigators and/or the investigators' designated representatives on making such corrections. Sponsors should have written procedures to assure that changes or corrections in CRFs made by sponsor's designated representatives are documented, are necessary, and are endorsed by the investigator. The investigator should retain records of the changes and corrections.

Copyright eClinical Forum

ICH GCP	5.5.3c	When using electronic trial data handling and/or remote electronic trial data systems,the sponsor should: c) Ensure that the systems are designed to permit data changes in such a way that the data changes are documented and that there is no deletion of entered data (i.e.maintain an audit trail, data trail, edit trail).
ICH GCP	5.5.4	If data are transformed during processing, it should always be possible to compare the original data and observations with the processed data.
JPMA EDC Guidance	4.1.1.1f	Audit trail shall be recorded automatically. (i.e. The EDC system is designed to permit data changes in such a way that the data changes are documented and that there is no deletion of entered data.)
JPMA EDC Guidance	4.1.1.1g	Audit trail shall not be modified by anyone.
JPMA EDC Guidance	4.1.1.2a	The ability to investigate of operator, content and timing of input/modify of data.
JPMA EDC Guidance	4.1.1.2b	The ability to prevent alteration, divulgation and repudiation of fact of operation.
JPMA EDC Guidance	4.1.1.3.6c	The ability to identify of operator ID and input time of each data by log (i.e. audit trail). - Note that signature shall not be requested for every data input. - But, the operator shall be identified for every data input.
JPMA EDC Guidance	4.1.1.3.6g	The ability to confirm the audit trail on the display by the investigator.
JPMA EDC Guidance	4.1.1.3c	In case of source document does not exist (i.e. data of electronic CRF is source document), employ controls to identify the data creator clearly, such as functionality of control of access rights to the EDC system.
JPMA EDC Supplement	1.2e	First, in case of an ePRO system using an IVRS or IWRS, data in the server is regarded as source data, as it is directly recorded PRO (original). Therefore, the data must include an input trail and, in case of correction, an edit trail.
JPMA EDC Supplement	1.2f	In case of an ePRO system using an entry device, data saved in the device is the original record created by the subject, and is thus regarded as the source data. Therefore, the Usage of Electromagnetic Records and Electronic Signatures in the Application for Drug Approval or Licensing must be complied for the device itself. In other words, requirements for authenticity, readability and retainability must be fulfilled under precondition that the device has been validated. These requirements include recording of an audit trail in case the data saved in the device are changeable.
JPMA EDC Supplement	1.4c	Ensure that the systems are so designed as to permit data correction in such a way that the data correction are documented and that all records of correction of entered data remain undeleted as logs distinguishable to the inputter as well as to the corrector (i.e. to maintain audit trail, input trail, and edit trail);
JPMA EDC Supplement	1.5.1.1c	An audit trail can be retained automatically. Together with the entered data, the date and time of entry and the person who enters the data can be recorded. If the system is also designed to permit data correction, then the data corrections are documented and that all records of correction of entered data remain undeleted as unchangeable logs distinguishable to the inputter as well as to the corrector, automatically.
JPMA EDC Supplement	1.5.1.2a	An audit trail shall enable identification of the persons who entered the data, the entered data and the time of entry. In case of correction, the persons who corrected, the correction details and the time of correction must be identifiable.
MHRA GXP Data Integrity Guidance	6.13a	The audit trail is a form of metadata containing information associated with actions that relate to the creation, modification or deletion of GXP records. An audit trail provides for secure recording of life-cycle details such as creation, additions, deletions or alterations of information in a record, either paper or electronic, without obscuring or overwriting the original record. An audit trail facilitates the reconstruction of the history of such events relating to the record regardless of its medium, including the 'who, what, when and why' of the action.
MHRA GXP Data Integrity Guidance	6.13b	Where computerised systems are used to capture, process, report, store or archive raw data electronically, system design should always provide for the retention of audit trails to show all changes to, or deletion of data while retaining previous and original data. It should be possible to associate all data and changes to data with the persons making those changes, and changes should be dated and time stamped (time and time zone where applicable). The reason for any change, should also be recorded. The items included in the audit trail should be those of relevance to permit reconstruction of the process or activity.
MHRA GXP Data Integrity Guidance	6.13c	Audit trails (identified by risk assessment as required) should be switched on. Users should not be able to amend or switch off the audit trail. Where a system administrator amends, or switches off the audit trail a record of that action should be retained.
NMPA Clinical Trial DM Guide	3.3.1.d	Clinical trial data management system validation include the following aspects: - Ensure data integrity, including the prevention of deleted or lost data
NMPA Clinical Trial DM Guide	3.3.2.a	CRF data for any changes or correction should be dated and signed name and explain why (if required), and should make the original records are still visible.
NMPA Clinical Trial DM Guide	3.3.2.b	Inspection of clinical trial data track (Audit Trail), from the first data entry so that every change, delete or add, must be retained in the clinical trials database system to ensure that the data from the original data to declare the whole process transparency. Inspection should include changing tracks the date, time, change the people, change reasons, the data value before the change, the changed data values. This inspection trajectory of system protection, does not allow any artificial modification and editing. Inspection records should be archived and trajectory queries.

CDISC Clinical Forum

NMPA Clinical Trial DM Guide	5.13.b	Ensure data accessibility refers to the user when needed, such as login and retrieve data from, and the data in the database can be transmitted in a timely manner as needed.
NMPA PISS	10.5b	An automated audit system should be established to monitor and record personal information processing activities.
NMPA PISS	10.5d	Unauthorized access, tampering or deletion of audit records should be prevented.
NMPA PISS	7.4	Personal information controllers should provide personal information subjects with access to the following information: a) the personal information or type of information it holds about the subject; b) the source of the above personal information and the purpose for which it was used; c) The identity or type of the third party who has obtained the above personal information.
NMPA PISS	8.1e	The personal information controller should accurately record and save the circumstances of the commissioned personal information.
PMDA Points to Note in CR and PMS	4.C.3	When collecting data directly from information and communication devices, the sponsor shall ensure reliability by including an audit trail . The audit trail should be available for presentation at the time of the conformity study, if necessary.
Taiwan Computerized Systems	4.3.b	Metadata also permit data to be attributable to an individual entering or taking an action on the data such as modifying, deleting, reviewing, etc.
Taiwan Computerized Systems	4.5.b2	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 permanent 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, such as Coordinated Universal Time (UTC) or central server.
Taiwan Computerized Systems	4.5.f	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).
Taiwan Computerized Systems	5.5	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 computerized system and used as a timestamp.
Taiwan Computerized Systems	6.1.3	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).
Taiwan Computerized Systems	6.2.1.a	An audit trail should be enabled for the original creation and subsequent modification of all electronic data. In computerized systems, the audit trail should be secure, computer generated and timestamped.
Taiwan Computerized Systems	6.2.1.b	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).
Taiwan Computerized Systems	6.2.1.c	Entries in the audit trail should be protected against change, deletion, and access modification (e.g. edit rights, visibility rights).
Taiwan Computerized Systems	6.2.1.d	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.
Taiwan Computerized Systems	6.2.1.f	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, organization), when (date/timestamp) and, where applicable, why (reason for change).
Taiwan Computerized Systems	6.2.1.i	Changes to data should only be performed when justified. Justification should be documented.
Taiwan Computerized Systems	8.2.1.1.1	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.
Taiwan Computerized Systems	8.2.1.1.2.b	In addition to the general requirements on audit trails, 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.

Copyright eClinical Forum

Regulatory mapping for eCF Requirement ID C10

There is a process to ensure that case **records** and any subsequent modifications are **reviewed and approved** by the investigator.

Regulation	Paragraph	Description
EMA Computerised Systems	4.1.b	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.
EMA Computerised Systems	6.3	The sponsor should seek investigator endorsement of their data at predetermined milestones. The signature of the investigator or authorised member of the investigators 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.
EMA Computerised Systems	A6.4	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 input. The system should allow the investigator to document the assessment and acknowledgement of information entered into the system by others.
FDA EHR Guidance	V.C.2.d	Clinical investigators should review and electronically sign the completed eCRF for each study participant before data are archived or submitted to FDA.
FDA EHR Guidance	V.C.2.e	If modifications are made to the eCRF after the clinical investigator has already signed the eCRF, the changes should be reviewed and approved by the clinical investigator.
FDA eSource Guidance	B1a	Clinical Investigator(s) Review and Electronic Signature To comply with the requirement to maintain accurate case histories clinical investigator(s) should review and electronically sign the completed eCRF for each subject before the data are archived or submitted to FDA. Use of electronic signatures must comply with part 11 (21 CFR part 11).
FDA eSource Guidance	B2	Modifications and Corrections During Clinical Investigator(s) Review of the eCRF To comply with the requirement to maintain accurate case histories, data elements might call for modification or correction during clinical investigator(s) review. Either the clinical investigator(s) or an originator can enter the revised data element. Modified and/or corrected data elements must have data element identifiers that reflect the date, time, originator, and reason for the change, and must not obscure previous entries. If changes are made to the eCRF after the clinical investigator(s) has already signed, the changes should be reviewed and electronically signed by the clinical investigator(s).
FDA and MHRA Data Integrity Discussions	P9b	Sponsors and clinical investigators should ensure that all changes to the investigator's study data are documented and authorized by investigators or delegated study personnel at the site.
FDA and MHRA Data Integrity Discussions	P9c	Any changes to study data entered into the EDC system should also be authorized by the investigator.
ICH E6 GCP R3 Good Clinical Practice	III.2.12.1	In generating, recording and reporting trial data, the investigator should ensure the integrity of data under their responsibility, irrespective of the media used.
ICH E6 GCP R3 Good Clinical Practice	III.3.16.1o	The sponsor should seek investigator endorsement of their reported data at predetermined important milestones.
ICH E6 GCP R3 Good Clinical Practice	III.3.16.2e	Such data changes should be authorised by the investigator and reflected in an audit trail.
ICH GCP	4.9.0	The investigator/institution should maintain adequate and accurate source documents and trial records that include all pertinent observations on each of the site's trial subjects. Source data should be attributable, legible, contemporaneous, original, accurate, and complete. Changes to source data should be traceable, should not obscure the original entry, and should be explained if necessary (e.g., via an audit trail).

Copyright eClinical Forum

ICH GCP	4.9.1	The investigator should ensure the accuracy, completeness, legibility, and timeliness of the data reported to the sponsor in the CRFs and in all required reports.
JPMA EDC Guidance	4.1.1.3.6d	The investigator shall check and confirm the created or modified electronic CRF and put electronic or handwriting signature on it.
JPMA EDC Guidance	4.1.1.3.6f	If there are some amendments after investigator signed, the investigator shall check and confirm the modified electronic CRF and put electronic or handwriting signature on it again.
JPMA EDC Guidance	4.1.1.4e	Clearly identified signature time and intended electronic records and if electronic records are modified, electronic signature shall be executed on the modified records.
MHRA GXP Data Integrity Guidance	6.15	The approach to reviewing specific record content, such as critical data and metadata, cross- outs (paper records) and audit trails (electronic records) should meet all applicable regulatory requirements and be risk-based.
NMPA Clinical Trial DM Guide	5.6	Erroneous data in the data cleaning process will be corrected. Data sheets or data verification challenge file as a data record of the changes must be signed by the investigator.
Taiwan Computerized Systems	6.3	The investigators are responsible for data entered into eCRFs and other data acquisition tools under their supervision (electronic records), and should review and sign-off these data. The signature of the investigator or authorized 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 authorized for sign-off should be qualified to do so.
Taiwan Computerized Systems	8.3.4	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 input. The system should allow the investigator to document the assessment and acknowledgement of information entered into the systems.

Copyright eClinical Forum

Regulatory mapping for eCF Requirement ID C11

There is a system and/or process to ensure the **investigator has control** of and continuous access to all essential records (data and documents) generated by the investigator/institution/patient before, during and after the trial.

Regulation	Paragraph	Description
EMA Computerised Systems	6.1.4	The sponsor should not make automatic or manual changes to data entered by the investigator or trial participants unless authorised by the investigator.
EMA Computerised Systems	6.2.1.h	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.
EMA Computerised Systems	6.6.a	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.
EMA Computerised Systems	6.6.b	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.
EMA Computerised Systems	A5.1.1.3	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.
EMA Computerised Systems	A5.1.1.4	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.
EMA Computerised Systems	A5.2.3	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.
EMADCT	6.5	Utilising multiple systems and parties adds complexity and requires an adequate oversight and implementation of adequate measures by the sponsor. To this end, the sponsor should: Ensure control of and continuous and complete access by the investigator to both source data generated either on-site or off-site as well as source data reported to the sponsor (e.g. central lab data).
EMA eTMF Guideline	3.1a	The investigator/institution is responsible for all essential documents generated by the investigator/institution and should therefore have control of them at all times. In cases in which the investigator is employed by an institution that is the trial sponsor, the sponsor may delegate the task for maintaining all or part of the sponsor TMF to the investigator. In this circumstance, it is possible to combine the delegated part of the sponsor TMF and investigator TMF for that investigator/institution, which avoids the duplication of documentation; however, the responsibility for the sponsor TMF remains with the sponsor. The same applies when the investigator and the sponsor are the same person. When there is co-sponsorship of a trial, there should be arrangements in place for the maintenance of the TMF based upon the responsibilities that each co- sponsor holds.
EMA eTMF Guideline	4.1.3a	A complete investigator TMF should be available before, during and after the trial, and accessible under the control of the investigator/institution, independent from the sponsor.
EMA eTMF Guideline	4.1.3d	The uploading of any investigator/institution-generated essential documents onto a sponsor/CRO-maintained eTMF system bears the risk that the investigator has no control of and no continuous access to its documents. If an eTMF is to be used for such documents, the contractual arrangements for the system and the hosting of the data should identify the investigator/institution, as owner of/responsible party for these documents.
EMA eTMF Guideline	4.1.3e	The investigator/institution is responsible for the suitability of the investigator TMF. Regardless of what arrangements are put in place for an eTMF, these should ensure that this responsibility can be fulfilled and that the investigator/institution maintains continuous access to and control of the files and their documents. When a third party eTMF is used, there should be assurance that the investigator/institution can fulfil their responsibility.
EMA eTMF Guideline	6.2	The investigator/institution should make the sponsor aware of the storage arrangements for their essential documents and conversely the sponsor should inform the investigator/institution in writing of the need for document archiving. The ultimate responsibility for the documents to be retained by the investigator/institution resides with the investigator/institution. If the investigator/institution becomes unable to be responsible for their essential documents (e.g. relocation, retirement, closure of institution, etc.) the sponsor agreement with the investigator/institution should stipulate that the sponsor is notified (preferably upfront) in writing of this change and informed to whom the responsibility will be/has been transferred. The new individual/institution responsible should be independent of the sponsor and should be free of any conflict of interest.

Copyright © Clinical Forum

FDA EHR Guidance	V.C.2.a	After data are transmitted to the eCRF, the clinical investigator or delegated study personnel should be the only individuals authorized to make modifications or corrections to the data.
FDA and MHRA Data Integrity Discussions	10a	The use of a third party to prevent sponsor sole control would be undermined if the third party transfers the data to the sponsor for final distribution to investigators and the third party deletes the data.
FDA and MHRA Data Integrity Discussions	P10	The investigator should control all source data, CRFs, and other site essential documents as the sponsor should not have exclusive control of the study data.
FDA and MHRA Data Integrity Discussions	P9d	Sponsors should not be making edits in the eCRF without the investigator's authorization.
ICH E6 GCP R3 Good Clinical Practice	III.2.12.11	The investigator/institution should have control of all essential records generated by the investigator/institution before and during the conduct of the trial.
ICH E6 GCP R3 Good Clinical Practice	III.2.12.2a	The investigator/institution should maintain adequate source records that include pertinent observations on each of the trial participants under their responsibility.
ICH E6 GCP R3 Good Clinical Practice	III.3.16.1i	The sponsor should not make changes to data entered by the investigator or trial participants unless justified, agreed upon in advance by the investigator and documented.
ICH E6 GCP R3 Good Clinical Practice	III.3.16.1j	The sponsor should allow correction of errors to data, including data entered by participants, where requested by the investigators/participants. Such data corrections should be justified and supported by source records around the time of original entry.
ICH E6 GCP R3 Good Clinical Practice	III.3.16.1k	The sponsor should ensure that the investigator has timely access to data collected in accordance with the protocol during the course of the trial, including relevant data from external sources (e.g., central laboratory data, centrally read imaging data and, if appropriate, ePRO data).
ICH E6 GCP R3 Good Clinical Practice	III.3.16.1l	The sponsor should not have exclusive control of data captured in data acquisition tools in order to prevent undetectable changes.
ICH E6 GCP R3 Good Clinical Practice	III.3.16.1m	The sponsor should ensure that the investigator has access to the required data for retention purposes.
ICH GCP	4.9.4	The investigator/institution should maintain the trial documents as specified in Essential Documents for the Conduct of a Clinical Trial (see 8.) and as required by the applicable regulatory requirement(s). The investigator/institution should take measures to prevent accidental or premature destruction of these documents.
ICH GCP	8.1	ADDENDUM The sponsor and investigator/institution should maintain a record of the location(s) of their respective essential documents including source documents. The storage system used during the trial and for archiving (irrespective of the type of media used) should provide for document identification, version history, search, and retrieval. Essential documents for the trial should be supplemented or may be reduced where justified (in advance of trial initiation) based on the importance and relevance of the specific documents to the trial. The sponsor should ensure that the investigator has control of and continuous access to the CRF data reported to the sponsor. The sponsor should not have exclusive control of those data. When a copy is used to replace an original document (e.g., source documents, CRF), the copy should fulfill the requirements for certified copies. The investigator/institution should have control of all essential documents and records generated by the investigator/institution before, during, and after the trial.
JPMA EDC Supplement	1.2a	...it is required to prepare necessary equipment (e.g. devices) and environment (e.g. internet line, telephone line) for data entry by subjects, make operational procedures for transmitting subject data to the operational database, operational procedures for providing the collected subject data to investigators. and sponsors, and also procedures for data retention after completion of the clinical trial and location of storage.
JPMA EDC Supplement	1.2b	The entered data are stored in the vendor server as source documents. During this process, the vendor ensures reliability of the source documents as a trusted third party.

Copyright eClinical Forum

JPMA EDC Supplement	1.2c	During the trial, both the site and sponsor representatives can view the ePRO data in the vendor server via web as necessary.
JPMA EDC Supplement	1.5.2b	If it is necessary to evaluate safety and efficacy and/or to conduct monitoring with the data collected by an ePRO system, such data should be viewable at any time throughout the trial period.
JPMA EDC Supplement	1.5.3	Throughout the specified period of record keeping, the authenticity and readability of the electromagnetic records must be ensured.
Taiwan Computerized Systems	6.2.1.h	A procedure should be in place to address the situation when a data originator (e.g. investigator or trial participant) realizes that she/he has submitted incorrect data by mistake and wants to correct the recorded data.
Taiwan Computerized Systems	6.6.a	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.
Taiwan Computerized Systems	6.6.b	The sponsor should not have exclusive control of the data entered in a computerized 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.
Taiwan Computerized Systems	8.2.1.1.3	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 minimize the risk of missed adverse events or missing data.
Taiwan Computerized Systems	8.2.1.1.4	A procedure should be in place to address and document if a data originator (investigator or trial participant) realizes that they have submitted incorrect data by mistake and want to correct the recorded data.
Taiwan Computerized Systems	8.2.2.3	Where clinical data is entered into the IRT system and integrated in the electronic data collection (EDC) system, the additional functionality and GCP requirement concerning data acquisition tools (eCRFs) should be addressed in the IRT system requirements and UAT e.g. investigator control of site entered data, authorization of data changes by the investigator, authorization of persons entering/editing data in the system by the investigator.

Copyright eClinical Forum

Regulatory mapping for eCF Requirement ID C13

Controls exist such that the ability to **change system settings** is limited to authorized personnel.

Regulation	Paragraph	Description
FDA 21 CFR Part 11	10d	(d) Limiting system access to authorized individuals.
FDA 21 CFR Part 11	10g	(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.
FDA 21 CFR Part 11	10k	(k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.
FDA CSUCI	D2e	Should it be decided that audit trails or other appropriate security measures are needed to ensure electronic record integrity, personnel who create, modify, or delete electronic records should not be able to modify the documents or security measures used to track electronic record changes.
FDA CSUCI	D3b	The ability to change the date or time should be limited to authorized personnel, and such personnel should be notified if a system date or time discrepancy is detected.
EMA Computerised Systems	A3.3.b	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.
EMA Computerised Systems	A4.19	The integrity of data should be protected against unauthorised back-end changes made directly on a database by a database administrator.
EU Clinical Trials Regulation 536 2014	58f	Any alteration to the content of the clinical trial master file shall be traceable.
MHLWCS	6.4.1	The Operation Manager should conduct the followings activities in accordance with the Operations Management Code, etc.; (1) To configure access privileges of persons in charge of input, modification, deletion, etc. of data and to take preventive actions against unauthorized accesses.
MHRA GXP Data Integrity Guidance	5.1a	At the point of use, having access to appropriately controlled/synchronised clocks for recording timed events to ensure reconstruction and traceability, knowing and specifying the time zone where this data is used across multiple sites.
NMPA Clinical Trial DM Guide	3.3.3.a	Clinical trial data management system must have a sound management system privileges. Paper-based or electronic data management are needed to develop SOPs for access control and management. Data management system for different people with different permissions or roles that only authorized personnel are allowed to operate (record, modify, etc.), and shall take appropriate methods to monitor and prevent non-licensed person operation.

Copyright eClinical Forum

Regulatory mapping for eCF Requirement ID C14

System uses a **standard time** reference such that the local time can be derived.

Regulation	Paragraph	Description
FDA 21 CFR Part 11	10e	(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.
FDA 21 CFR Part 11 Q and A	Q14	Controls should be in place to ensure that the system date and time are correct.
FDA CSUCI	D3e	Computerized systems are likely to be used in multi-center clinical trials and may be located in different time zones. For systems that span different time zones, it is better to implement time stamps with a clear understanding of the time zone reference used. We recommend that system documentation explain time zone references as well as zone acronyms or other naming conventions.
EMA Computerised Systems	4.5.b2	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.
EMA Computerised Systems	A5.1.1.2.f	Important actions should be time-stamped in an unambiguous way.
EMA Computerised Systems	A5.1.3.1	The application should use an external source for date and time and should not rely on information from the users device.
EMA eTMF Guideline	4.1.2k	Metadata applied to documents should be formally defined to ensure consistency across all documents. This should include the predefined document date (e.g. date of creation) and when appropriate, time, based on standard time zone, so that the files can be displayed in chronological order.
MHLW ERES (Japan)	2.6	Audit Trail means a series of operational records with accurate time stamp (date recorded by computer automatically).
EU Annex 11	12.4	Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.
ICH E6 GCP R3 Good Clinical Practice	III.4.2.2d	Ensuring that the automatic capture of date and time of data entries or transfer are unambiguous (e.g., coordinated universal time (UTC)).
MHRA GXP Data Integrity Guidance	5.1a	At the point of use, having access to appropriately controlled/synchronised clocks for recording timed events to ensure reconstruction and traceability, knowing and specifying the time zone where this data is used across multiple sites.
Taiwan Computerized Systems	4.5.b2	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 permanent 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, such as Coordinated Universal Time (UTC) or central server.
Taiwan Computerized Systems	8.2.1.1.2.f	Important actions should be time-stamped in an unambiguous way, e.g. data entries, transfer times and volume (bytes).
Taiwan Computerized Systems	8.2.1.3.1	The application should use an external source for date and time and should not rely on information from the users device.

Copyright eClinical Forum

Regulatory mapping for eCF Requirement ID C16

There are system features and processes to create, maintain, revoke, and document the history of **user access, roles and privileges** over time.

Regulation	Paragraph	Description
FDA 21 CFR Part 11	10d	(d) Limiting system access to authorized individuals.
FDA 21 CFR Part 11	10g	(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.
FDA 21 CFR Part 11 Q and A	Q11a	Logical and physical access controls should be integral to electronic systems used in clinical investigations to limit system access to authorized users, particularly for systems that provide access to multiple users or systems that are accessed through networks.
Japanese APPI	Article 24	A personal information handling business operator shall, when having its employees handle personal data, exercise necessary and appropriate supervision over said employees to ensure the safety management of said personal data.
FDA CSUCI	D1a	Access must be limited to authorized individuals (21 CFR 11.10(d). This requirement can be accomplished by the following recommendations. We recommend that each user of the system have an individual account.
FDA CSUCI	D1e	The system should not allow an individual to log onto the system to provide another person access to the system.
FDA CSUCI	E4	You should maintain a cumulative record that indicates, for any point in time, the names of authorized personnel, their titles, and a description of their access privileges. That record should be kept in the study documentation, accessible for use by appropriate study personnel and for inspection by FDA investigators.
PMDA EDC Management Sheet version 2	47	A list of individuals authorized to access the system is: - During the trial: - Upon completion of the trial (to be submitted at the time of inspection)
EMA Computerised Systems	4.2.a	Roles and responsibilities in clinical trials should be clearly defined.
EMA Computerised Systems	5.4.a	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.
EMA Computerised Systems	6.1.4	The sponsor should not make automatic or manual changes to data entered by the investigator or trial participants unless authorised by the investigator.
EMA Computerised Systems	6.2.1.b	...for an audit trail to be deactivated by "admin users", this should automatically create an entry into a log file (e.g. audit trail).
EMA Computerised Systems	6.2.1.j	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.
EMA Computerised Systems	A3.1.a	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.
EMA Computerised Systems	A3.2	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.
EMA Computerised Systems	A3.3.a	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.
EMA		Users with privileged access should be sufficiently independent from and not be involved in the management and conduct of the

Copyright eClinicalForum

Computerised Systems	A3.3.b	clinical trial and in the generation, modification, and review of data.
EMA Computerised Systems	A3.3.c	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.
EMA Computerised Systems	A3.3.d	Unblinded information should only be accessible to pre-identified user roles.
EMA Computerised Systems	A3.4	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.
EMA Computerised Systems	A5.1.1.7.b	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.
EMA Computerised Systems	A5.2.1.3	Unblinded information should only be provided and accessible to pre-identified user roles.
EMA Computerised Systems	A5.3.4	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.
EMA Computerised Systems	A6.7	Robust procedures on user management should be implemented.
EMA Computerised Systems	A6.8.a	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.
EMADCT	6.4	Utilising multiple systems and parties adds complexity and requires an adequate oversight and implementation of adequate measures by the sponsor. To this end, the sponsor should: Ensure access to trial data is controlled by defined user rights and methods of access for all relevant parties involved. Unauthorised access should be prevented using appropriate security measurers e.g. firewalls.
EMA eTMF Guideline	3.1	In organising the TMF, it is essential to segregate some documents that are generated and/or held by the sponsor only, from those that are generated and/or held by the investigator/institution only (e.g. subject identification code list filed in the investigator TMF only and master randomisation list filed in the sponsor TMF only).
EMA eTMF Guideline	3.1b	Role-based permissions should be established for activities being undertaken, such as restricted access to files/documents (e.g. randomisation codes and unblinded adverse event data).
EMA eTMF Guideline	4.1	The TMF should be managed securely at all times to ensure completeness and to prevent accidental or premature loss, unauthorised alteration or destruction of documents. Access to the TMF should be based on a role and permission description that is defined by the sponsor and/or investigator/institution. The sponsor TMF and investigator/institution TMF may contain some information that could unblind personnel who need to remain blinded during the trial conduct. This should be appropriately controlled, e.g. storage of the documentation in another system or repository and/or by a role and permission description that is defined by the sponsor and/or investigator/institution.
EMA eTMF Guideline	4.1.2a	The primary eTMF is a system for managing documents that should contain the controls listed below: user accounts; secure passwords for users.
EMA eTMF Guideline	4.1.2f	The primary eTMF is a system for managing documents that should contain the controls listed below: role-based permissions for activities being undertaken, such as restricted access to files/documents (e.g. randomisation codes and unblinded adverse event data);
EMA eTMF Guideline	4.1.3h	Remote access by sponsor or CRO personnel to the investigator TMF should only be possible to the documents where personal data that enable the data subjects to be directly identified (i.e. direct identifiers of trial subjects) is not present or has been pseudonymised.
EMA eTMF Guideline	4.2a	The sponsor and/or investigator/institution should implement risk-based quality checks (QC) or review processes to ensure the TMF is being maintained up-to-date and that all essential documents are appropriately filed in the TMF. Areas to consider during QC and review include the following: - documents only accessible according to the assigned roles and permissions.
EMA eTMF Guideline	5	Particular attention should be paid when documents are stored on electronic, magnetic, optical or other non-indelible media. In such cases suitable controls should be implemented to ensure that these documents are complete and cannot be altered without appropriate authorisation and the creation of an audit trail.
EMA eTMF Guideline	6.1a	With respect to the sponsor TMF, Article 58 of the Regulation states that the sponsor shall appoint individuals within its organisation to be responsible for archives. Access to archives shall be restricted to those individuals.

Clinical eClinical Forum

EMA IRT Reflection Paper	2.2.3a	Access permissions - personnel with these access rights at the site should be qualified for these delegated activities. These permissions should be included in the project specification. It is important that the permissions be clear with respect to their ability to see what trial medication is being taken by a subject (blinded versus unblinded). Access permissions might include but not be limited to the following staff: - pharmacy staff; - principal investigator; - site research team, including any study coordinator, research nurse or sub-investigator; - contract research associate (CRA), where applicable; - sponsor staff, including project managers, clinical supplies staff.
MHLW ERES (Japan)	3.1.1.1	Rules and procedures of maintaining securities of the system are documented and practicing them appropriately.
MHLW ERES (Japan)	5	Persons who uses electromagnetic records and electronic signatures for materials and raw-materials of applications for approval or licensing of drugs, and for registration of conformity certification bodies shall prepare documents described persons in charge, managers, organizations, equipments and training for using electromagnetic records and electronic signatures.
EU Annex 11	12.3	Creation, change, and cancellation of access authorisations should be recorded.
EU Annex 11	2	There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.
EU Clinical Trials Regulation 536 2014	58d	The sponsor shall appoint individuals within its organisation to be responsible for archives. Access to archives shall be restricted to those individuals.
FDA DHT for RDA in CI	IV.Bb	Sponsors should describe how access to the DHT or the data collected from it is controlled to ensure privacy and security. The description should include methods for access control, when feasible, to ensure that only appropriate individuals are able to use the DHT or enter information.
FDA EHR Guidance	V.B.1	Policies and processes for the use of EHR systems at the clinical investigation site are in place, and there are appropriate security measures employed to protect the study data.
FDA EHR Guidance	V.B.2	Access to electronic systems is limited to authorized users.
FDA Electronic Informed Consent Q&A	Q10a	The electronic system that supports the eIC must be secure with restricted access (see 21 CFR 11.10 and 11.30) and should include methods to ensure confidentiality regarding the subjects identity, study participation, and personal information after informed consent has been obtained.
FDA eSource Guidance	D	Data Access Sponsors, CROs, data safety monitoring boards, and other authorized personnel can view the data elements in the eCRF before and after the clinical investigator(s) has electronically signed the completed eCRF. We encourage viewing the data to allow early detection of study-related problems (e.g., safety concerns, protocol deviations) and problems with conducting the study (e.g., missing data, data discrepancies). The sponsor should have a list (e.g., in a data management plan) of the individuals with authorized access to the eCRF. Only those individuals who have documented training and authorization should have access to the eCRF data. Individuals with authorized access should be assigned their own identification (log-on) codes and passwords. Log-on access should be disabled if the individual discontinues involvement during the study.
FDA and MHRA Data Integrity Discussions	P9e	Because audit trails rely on username assignment, individuals should work only under their own username and password, or other access controls, and not share these with others.
FDA Real World Data	III.Cc	Conformance with 21 CFR part 11, as applicable, including maintenance of access controls and audit trails to demonstrate the provenance of the registry data and to support traceability of the data
FDA Real World Data	III.Ce	Sponsors should address whether the registry has privacy and security controls in place to ensure that the confidentiality and security of data are preserved.
FDA Real World Data	III.Dd	...the sponsor should consider whether... The procedures and access controls in place protect the privacy of patient data
EU GDPR	Article 25.2	Controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose are processed.
EU GDPR	Article 29	The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.
EU GDPR	Article 36.3a	When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with: (a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings.
EU GDPR	Article 5.1c	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).

Copyright eClinical Forum

USA HIPAA	164.304a	Availability means the property that data or information is accessible and useable upon demand by an authorized person.
USA HIPAA	164.306a3	Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
USA HIPAA	164.308a3iiA	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
USA HIPAA	164.514d2	(i) A covered entity must identify: (A) Those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and (B) For each such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access. (ii) A covered entity must make reasonable efforts to limit the access of such persons or classes identified in paragraph (d)(2)(i)(A) of this section to protected health information consistent with paragraph (d)(2)(i)(B) of this section.
ICH E6 GCP R3 Good Clinical Practice	III.2.12.10a	For systems deployed by the investigator/institution, ensure that appropriate individuals have secure and attributable access.
ICH E6 GCP R3 Good Clinical Practice	III.2.12.9	For systems deployed by the investigator/institution that maintain and retain trial data/information, the investigator/institution should ensure that such data are protected from unauthorised access, disclosure, dissemination or alteration and from inappropriate destruction or accidental loss.
ICH E6 GCP R3 Good Clinical Practice	III.3.16.1r	Prior to provision of the data for final analysis and, where applicable, before unblinding the trial, edit access to the data acquisition tools should be restricted.
ICH E6 GCP R3 Good Clinical Practice	III.3.16.1v	The sponsor should ensure that trial data are protected from unauthorised access, disclosure, dissemination or alteration and from inappropriate destruction or accidental loss.
ICH E6 GCP R3 Good Clinical Practice	III.3.16.1xiii	Maintain a record of the individual users who are authorised to access the system, their roles and their access permissions
ICH E6 GCP R3 Good Clinical Practice	III.3.16.1xiv	Ensure that access permissions granted to investigator site staff are in accordance with delegations by the investigator and visible to the investigator.
ICH E6 GCP R3 Good Clinical Practice	III.4.2.2ai	Evaluating the system for the types and content of metadata available to ensure that: (i) Computerised systems maintain logs of user account creation, changes to user roles and permissions and user access.
ICH E6 GCP R3 Good Clinical Practice	III.4.3.8a	Access controls are integral to computerised systems used in clinical trials to limit system access to authorised users and to ensure attributability to an individual. The security measures should be selected in such a way that they achieve the intended security.
ICH E6 GCP R3 Good Clinical Practice	III.4.3.8b	Procedures should be in place to ensure that user access permissions are appropriately assigned based on a user's duties and functions, blinding arrangements and the organisation to which users belong. Access permissions should be revoked when they are no longer needed. A process should be in place to ensure that user access and assigned roles and permissions are periodically reviewed, where relevant.
ICH E6 GCP R3 Good Clinical Practice	III.4.3.8c	Authorised users and access permissions should be clearly documented, maintained and retained. These records should include any updates to user roles, access permissions and time of access permission being granted (e.g., time stamp).
ICH GCP	5.5.3b	When using electronic trial data handling and/or remote electronic trial data systems,the sponsor should: b) Maintains SOPs for using these systems. ADDENDUM The SOPs should cover system setup, installation, and use. The SOPs should describe system validation and functionality testing, data collection and handling, system maintenance, system security measures, change control, data backup, recovery, contingency planning, and decommissioning. The responsibilities of the sponsor, investigator, and other parties with respect to the use of these computerized systems should be clear, and the users should be provided with training in their use.
JPMA EDC Guidance	4.1.1.1a	User management and access rights grant are conducted according to the predetermined rule appropriately.
JPMA EDC Guidance	4.1.1.3.6a	The account list which mentions personnel access rights shall be created and operated instead of handwriting signature list.

Copyright eClinical Forum

JPMA EDC Guidance	4.1.1.3c	In case of source document does not exist (i.e. data of electronic CRF is source document), employ controls to identify the data creator clearly, such as functionality of control of access rights to the EDC system.
JPMA EDC Guidance	4.1.1.4a	Employ account management rule for electronic signature, and operate it properly.
JPMA EDC Supplement	1.4d	Maintain a security system for the data;
JPMA EDC Supplement	1.4f	Prepare and maintain a list of the individuals who are authorized to make data correction;
JPMA EDC Supplement	1.5.1.1a	User management and authority setting must be appropriately undertaken, as per the pre-set rules.
JPMA EDC Supplement	3.2.1c	To establish procedure to confirm that correct authority is granted to appropriate accounts.
MHRA GXP Data Integrity Guidance	5.1d	User access rights that prevent (or audit trail, if prevention is not possible) unauthorised data amendments. Use of external devices or system interfacing methods that eliminate manual data entries and human interaction with the computerised system, such as barcode scanners, ID card readers, or printers.
MHRA GXP Data Integrity Guidance	6.16	Full use should be made of access controls to ensure that people have access only to functionality that is appropriate for their job role, and that actions are attributable to a specific individual.
NMPA Clinical Trial DM Guide	3.3.1.c	Clinical trial data management system validation include the following aspects: - System access control, and user management
NMPA Clinical Trial DM Guide	3.3.1.e	Clinical trial data management system validation include the following aspects: - Prevent unauthorized data and document changes
NMPA Clinical Trial DM Guide	3.3.3.a	Clinical trial data management system must have a sound management system privileges. Paper-based or electronic data management are needed to develop SOPs for access control and management. Data management system for different people with different permissions or roles that only authorized personnel are allowed to operate (record, modify, etc.), and shall take appropriate methods to monitor and prevent non-licensed person operation.
NMPA PISS	4f	Ensuring security principles - have the security capabilities that match the security risks you face, and take adequate management measures and techniques to protect the confidentiality, integrity, and availability of your personal information.
NMPA PISS	7.1d	If it is necessary to authorize a specific person to handle personal information because of the need of work, it shall be examined and approved by the person responsible for personal information protection or the personal information protection agency, and recorded in the book.
PRC Electronic Signature Law	13a	Electronic signatures are considered reliable, when all of the following conditions are satisfied: (1) Data that create electronic signatures are owned only by the signer when they are being used for electronic signatures; (2) Data that create electronic signatures may only be controlled by the electronic signer at the time he is creating the signatures
Taiwan Computerized Systems	4.2.a	Roles and responsibilities in clinical trials should be clearly defined.
Taiwan Computerized Systems	5.4.a	To maintain data integrity and the protection of the rights of trial participants, computerized systems used in clinical trials should have security processes and features to prevent unauthorized access and unwarranted data changes and should maintain blinding of the treatment allocation where applicable. Checks should be used to ensure that only authorized 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 authorization 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.
Taiwan Computerized Systems	6.2.1.b	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).
Taiwan Computerized Systems	6.2.1.j	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.
Taiwan Computerized Systems	8.2.1.1.7.b	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.
Taiwan Computerized Systems	8.2.2.1.3	Unblinded information should only be provided and accessible to pre-identified user roles.
Taiwan Computerized	8.2.3.4	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.

Copyright eClinical Forum

Systems		
Taiwan Computerized Systems	8.3.7	Robust procedures on user management should be implemented.
Taiwan Computerized Systems	8.3.8.a	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.

Copyright eClinical Forum

Regulatory mapping for eCF Requirement ID C17

There is a policy and training that instructs users **not to share** their **access** mechanisms (e.g. usernames and passwords, or access keys) or to leave their account open for others to use. A shared account (or group account) is not appropriate.

Regulation	Paragraph	Description
FDA 21 CFR Part 11	200a	(a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. (2) Be used only by their genuine owners;
FDA 21 CFR Part 11 Q and A	Q20d	When fingerprints or other biometrics are used by data originators in place of username and password combinations, controls should be designed to ensure that the biometrics cannot be used by anyone other than the data originator.
FDA 21 CFR Part 11 Q and A	Q21b	Clinical trial personnel, participants, and other individuals should use their own usernames and passwords and not share them with others or use access controls belonging to others.
FDA CSUCI	D1d	Individuals should work only under their own password or other access key and not share these with others.
PMDA EDC Management Sheet version 2	42	Procedures for maintaining of security: Policy / Guidance for maintaining security
PMDA EDC Management Sheet version 2	44	Procedures for maintaining of security: Written procedures for users handling of the ID/password
PMDA EDC Management Sheet version 2	45	Procedures for maintaining of security: Written procedure for security training for users
EMA Computerised Systems	5.4.a	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.
EMA Computerised Systems	5.4.b	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.
EMA Computerised Systems	A4.16	Passwords should be kept confidential, sharing of passwords is unacceptable and a violation of data integrity.
EMA Computerised Systems	A5.1.1.7.a	The trial participants passwords should only be known to the trial participant.
EMA Computerised Systems	A6.7	Robust procedures on user management should be implemented.
EMA eTMF Guideline	4.1.2a	The primary eTMF is a system for managing documents that should contain the controls listed below: user accounts; secure passwords for users.
MHLW	4.2	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

Copyright eClinical Forum

ERES (Japan)		
EU Annex 11	12.1	Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.
FDA Electronic Informed Consent Q&A	Q6b	Electronic signatures based on biometrics must be designed to ensure that they cannot be used by anyone other than their genuine owners.
EU GDPR	Article 25.2	Controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose are processed.
EU GDPR	Article 32.2	In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
USA HIPAA	164.308a5i	Implement a security awareness and training program for all members of its workforce (including management).
USA HIPAA	164.308a5iiD	Procedures for creating, changing, and safeguarding passwords.
JPMA EDC Guidance	4.1.1.1c	Operation shall be adequate and compliance shall be ensured by training. (i.e. Prevent from spoofing, stealing password and so on.)
JPMA EDC Guidance	4.1.1.2c	The ability to prevent unauthorized access. (take a measure of malware and security hole, management and prevent of leaking of ID and password, user management).
JPMA EDC Supplement	1.4d	Maintain a security system for the data;
MHLWCS	6.4.1	The Operation Manager should conduct the followings activities in accordance with the Operations Management Code, etc.; (1) To configure access privileges of persons in charge of input, modification, deletion, etc. of data and to take preventive actions against unauthorized accesses.
NMPA Clinical Trial DM Guide	3.3.3.c	The electronic management system, user can only work with their own password, the password can not be shared, nor let other people access to login
NMPA PISS	10.4e	Personal information security professional training and assessment should be carried out on relevant personnel in personal information processing positions on a regular basis (at least once a year) or in the event of major changes in the privacy policy to ensure that relevant personnel are proficient in privacy policies and related procedures.
PRC Electronic Signature Law	13a	Electronic signatures are considered reliable, when all of the following conditions are satisfied: (1) Data that create electronic signatures are owned only by the signer when they are being used for electronic signatures; (2) Data that create electronic signatures may only be controlled by the electronic signer at the time he is creating the signatures
PRC Electronic Signature Law	15	The signer of electronic signatures shall keep custody of the data that create the electronic signatures. If the electronic signer learns that the data that created the electronic signatures are already deciphered or might be deciphered, he shall inform every involved party in a timely manner and terminate the use of the data.
Taiwan Computerized Systems	5.4.a	To maintain data integrity and the protection of the rights of trial participants, computerized systems used in clinical trials should have security processes and features to prevent unauthorized access and unwarranted data changes and should maintain blinding of the treatment allocation where applicable. Checks should be used to ensure that only authorized 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 authorization 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.
Taiwan Computerized Systems	5.4.b	There should be documented training on the importance of security e.g. sharing passwords is not allowed, enforcement of security systems and processes, identification and handling of severe violations.
Taiwan Computerized Systems	8.2.1.1.7.a	The trial participant’s passwords should only be known to him/herself.
Taiwan Computerized Systems	8.3.7	Robust procedures on user management should be implemented.

Copyright eClinical Forum

Regulatory mapping for eCF Requirement ID C18

The monitor, auditor, investigator and inspector can within a reasonable timeframe obtain **direct access** to relevant clinical trial records in order to perform their regulatory duties.

Regulation	Paragraph	Description
FDA 21 CFR Part 312	58a	FDA inspection. A sponsor shall upon request from any properly authorized officer or employee of the Food and Drug Administration, at reasonable times, permit such officer or employee to have access to and copy and verify any records and reports relating to a clinical investigation conducted under this part.
FDA 21 CFR Part 312	68	An investigator shall upon request from any properly authorized officer or employee of FDA, at reasonable times, permit such officer or employee to have access to, and copy and verify any records or reports made by the investigator pursuant to 312.62. The investigator is not required to divulge subject names unless the records of particular individuals require a more detailed study of the cases, or unless there is reason to believe that the records do not represent actual case studies, or do not represent actual results obtained.
21 CFR Part 812	145b	Records inspection. A sponsor, IRB, or investigator, or any other person acting on behalf of such a person with respect to an investigation, shall permit authorized FDA employees, at reasonable times and in a reasonable manner, to inspect and copy all records relating to an investigation.
21 CFR Part 812	145c	Records identifying subjects. An investigator shall permit authorized FDA employees to inspect and copy records that identify subjects, upon notice that FDA has reason to suspect that adequate informed consent was not obtained, or that reports required to be submitted by the investigator to the sponsor or IRB have not been submitted or are incomplete, inaccurate, false, or misleading.
Japanese APPI	Article 143	The Commission shall… request the submission of necessary reports or materials, or ask its staff to provide the relevant personal information handling business operator, etc. may enter the office or other necessary places of the parties concerned, ask questions about the handling of personal information, etc., or inspect books and documents and other properties.
EMA Computerised Systems	4.11	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.
EMA Computerised Systems	6.a	Electronic source data, including the audit trail should be directly accessible by investigators, monitors, auditors, and inspectors without compromising the confidentiality of participants identities.
EMA Computerised Systems	A1.b	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.
EMA Computerised Systems	A2.1.a1	...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.
EMA Computerised Systems	A5.1.a	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.
EMA Computerised Systems	A6.8.a	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.
EMA eTMF Guideline	2	The TMF should provide for document identification, version history, search and retrieval; also, as stated in both Directive 2005/28/EC (Article 17) and the Regulation (Articles 57 and 58) it shall be archived in a way that ensures that it is readily available and directly accessible upon request, to the competent authorities of the Member States.
EMA eTMF Guideline	3.2c	The clinical trial contract/agreement and other documents and procedures agreed between all parties should outline the arrangements for the TMF in some detail, such as: - how the TMF would be made available to the competent authorities; - arrangements for oversight of the TMF performed by the sponsor and how this would be achieved (e.g. audit reports and/or monitoring).
EMA eTMF Guideline	4.1.1	At all times the storage area for the TMF documents (such as paper or electronic media archives and server rooms) should be appropriate to maintain the documents in a manner that they remain complete and legible throughout the trial conduct and the required period of retention and can be made available to the competent authorities of the Member States, upon request.
EMA eTMF	4.2c	In addition, the sponsor should ensure the TMF is readily available and directly accessible to the competent authority, e.g. for

Copyright eClinical Forum

Guideline		inspection purposes.
EMA Q&A eTMF 1	b	Inspectors/auditors should have direct access to the e-TMF and the documents held in the e-TMF (the live system, not a copy) to allow direct searching.
EU Clinical Trials Regulation 536 2014	57	The clinical trial master file shall at all times contain the essential documents relating to that clinical trial which allow verification of the conduct of a clinical trial and the quality of the data generated, taking into account all characteristics of the clinical trial, including in particular whether the clinical trial is a low-intervention clinical trial. It shall be readily available, and directly accessible upon request, to the Member States.
EU Clinical Trials Regulation 536 2014	58b	The content of the clinical trial master file shall be archived in a way that ensures that it is readily available and accessible, upon request, to the competent authorities.
FDA EHR Guidance	V.2	Sponsors should also ensure that study monitors have suitable access to all relevant subject information pertaining to a clinical investigation, as appropriate.
FDA EHR Guidance	VI.1	All relevant information in the EHR pertaining to the clinical investigation must be made available to FDA for review upon request.
FDA Electronic Informed Consent Q&A	Q16	FDA regulations require that FDA be granted access to records and reports made by the investigator, including site-specific versions of the eIC, the materials submitted to IRBs for review and approval, all amendments to the site-specific eICs, and all subject-specific signed eICs.
FDA eSource Guidance	A2c	Transcription of Data From Paper or Electronic Sources to the eCRF Data elements can be transcribed into the eCRF from paper or electronic source documents. The authorized person transcribing the data from the source documents is regarded as the data originator. For these data elements, the electronic or paper documents from which the data elements are transcribed are the source. These data must be maintained by the clinical investigator(s) and available to an FDA inspector if requested (e.g., an original or certified copy of a laboratory report, instrument printout, progress notes of the physician, the study subjects hospital chart(s), nurses notes).
FDA eSource Guidance	A2d	Direct Transmission of Data From the Electronic Health Record to the eCRF Data elements originating in an EHR can be transmitted directly into the eCRF automatically. Unlike a direct transmission to an eCRF from instruments or medical devices, EHRs can use intervening processes (e.g., algorithms for the selection of the appropriate data elements). For this reason the EHR is the source, and the pertinent data for the subjects in the clinical study should be made available for review during an FDA inspection. The ability of sponsors and/or monitors to access health records of study subjects in clinical information systems relevant to the clinical investigation should not differ from their ability to access health records recorded on paper.
FDA Real World Data	III.E	Sponsors seeking to use registry data to support a drugs effectiveness and/or safety in a marketing application should ensure that patient-level data are provided to FDA in accordance with applicable legal and regulatory requirements. If the registry data are owned and controlled by third parties, sponsors should ensure that relevant patient-level data can be provided to FDA and that metadata and source records necessary to verify the RWD are made available for inspection, as applicable.
EU GDPR	Article 28h	(Processor) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.
USA HIPAA	164.512d1	A covered entity may disclose protected health information to a health oversight agency for oversight activities authorized by law...
ICH E6 GCP R3 Good Clinical Practice	B.11	The sponsor should ensure that it is specified in the protocol or other documented agreement that the investigator(s)/institution(s)/service provider(s) will permit trial-related monitoring, audits, regulatory inspection(s) and, in accordance with applicable regulatory requirements, review by the institutional review board/independent ethics committee (IRB/IEC), providing direct access to source records.
ICH E6 GCP R3 Good Clinical Practice	II.9.5b	These essential records should be available to regulatory authorities, monitors, auditors and IRBs/IECs (as appropriate) upon request to enable appropriate evaluation of the trial conduct in order to ensure the reliability of trial results.
ICH E6 GCP R3 Good Clinical Practice	III.2.12.14	Upon request of the monitor, auditor, IRB/IEC or regulatory authority, the investigator/institution should make available for direct access all requested trial-related records.
ICH E6 GCP R3 Good Clinical Practice	III.2.12.3	The investigator should be provided with timely access to data by the sponsor and be responsible for the timely review of data.
ICH E6 GCP R3 Good Clinical Practice	III.2.3.5	The investigator/institution should permit monitoring and auditing by the sponsor, inspection by the appropriate regulatory authority(ies) and, in accordance with applicable regulatory requirements, review by IRB/IEC(s).
ICH E6 GCP		

Copyright EClinical Forum

R3 Good Clinical Practice	III.3.11.4.1c	Monitoring may include remote and secure, direct read-only access to source records, other data acquisition tools and essential record retention systems.
ICH E6 GCP R3 Good Clinical Practice	III.3.16.4a	The sponsor should ensure that it is specified in the protocol or other documented agreement that the investigator(s)/institution(s) provide direct access to source records for trial-related monitoring, audits, regulatory inspection and, in accordance with applicable regulatory requirements, IRB/IEC review.
ICH E6 GCP R3 Good Clinical Practice	III.3.6.3d	The sponsor should obtain the investigator's/institution's and, where applicable, service provider's agreements: (d) To permit monitoring and auditing by sponsors, inspections by regulatory authorities (domestic and foreign) and, in accordance with applicable regulatory requirements, review by IRBs/IECs, including providing direct access to source records and facilities, including to those of service providers.
ICH GCP	4.9.7	Upon request of the monitor, auditor, IRB/IEC, or regulatory authority, the investigator/institution should make available for direct access all requested trial related records.
ICH GCP	5.1.2	The sponsor is responsible for securing agreement from all involved parties to ensure direct access to all trial related sites, source data/documents, and reports for the purpose of monitoring and auditing by the sponsor, and inspection by domestic and foreign regulatory authorities.
JPMA EDC Guidance	4.1.1.3.5	In the institutes, authority and investigators are able to check the data of CRF at anytime within the retention period.
NMPA PISS	7.1c	Separate roles should be set for the roles of security managers, data operators, and auditors.
Taiwan Computerized Systems	4.11	All relevant computerized systems should be readily available with full and direct access (this requires a unique identification method e.g. username and password). If a computerized system is decommissioned, direct access (with username and password) to the data in a timely manner should still be ensured.
Taiwan Computerized Systems	6.a	Electronic source data, including the audit trail should be directly accessible by investigators, monitors, auditors, and inspectors without compromising the confidentiality of participants identities.
Taiwan Computerized Systems	8.1.1.b	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.
Taiwan Computerized Systems	8.2.1.a	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.
Taiwan Computerized Systems	8.3.8.a	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.

Copyright ECClinical Forum

Regulatory mapping for eCF Requirement ID C19

System limits the number of **log-in attempts** and records unsuccessful attempts.

Regulation	Paragraph	Description
Japanese APPI	Article 23	A business operator handling personal information must take necessary and appropriate measures to prevent leakage, loss or damage of the personal data it handles and to otherwise manage the security of personal data.
FDA CSUCI	D1c	The system should be designed to limit the number of log-in attempts and to record unauthorized access log-in attempts.
EMA Computerised Systems	A4.12.b	User accounts should be automatically locked after a pre-defined number of successive failed authentication attempts.
USA HIPAA	164.308a5iiC	Procedures for monitoring log-in attempts and reporting discrepancies.
JPMA EDC Guidance	4.1.1.2c	The ability to prevent unauthorized access. (take a measure of malware and security hole, management and prevent of leaking of ID and password, user management).
JPMA EDC Supplement	1.4d	Maintain a security system for the data;
JPMA EDC Supplement	1.5.1.2b	The system must be designed to prevent and/or detect unauthorized access. For example, the system has a function that demands an access code in case of loss of a device, or a specific equipment or program to download data from the device, etc.
MHLWCS	6.4.1	The Operation Manager should conduct the followings activities in accordance with the Operations Management Code, etc.; (1) To configure access privileges of persons in charge of input, modification, deletion, etc. of data and to take preventive actions against unauthorized accesses.
NMPA PISS	10.3	Personal information controllers should establish appropriate data security capabilities and implement necessary management and technical measures to prevent leakage, damage, and loss of personal information in accordance with the requirements of relevant national standards.

Copyright eClinical Forum

Regulatory mapping for eCF Requirement ID C20

System records and notifies a system administrator of **unauthorized** access **log-in attempts**.

Regulation	Paragraph	Description
FDA 21 CFR Part 11	300d	(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.
Japanese APPI	Article 23	A business operator handling personal information must take necessary and appropriate measures to prevent leakage, loss or damage of the personal data it handles and to otherwise manage the security of personal data.
FDA CSUCI	D1c	The system should be designed to limit the number of log-in attempts and to record unauthorized access log-in attempts.
EMA Computerised Systems	A4.1	The responsible party should maintain a security system that prevents unauthorised access to the data.
EMA Computerised Systems	A4.9	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.
EMA Computerised Systems	A6.6	Security measures that prevent unauthorised access to data and documents should be maintained.
EU Annex 11	12.1	Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.
FDA EHR Guidance	V.B.2	Access to electronic systems is limited to authorized users.
USA HIPAA	164.308a5iiC	Procedures for monitoring log-in attempts and reporting discrepancies.
JPMA EDC Guidance	4.1.1.2c	The ability to prevent unauthorized access. (take a measure of malware and security hole, management and prevent of leaking of ID and password, user management).
JPMA EDC Guidance	4.1.1.2d	The ability to detect any unauthorized access. (monitoring of access, alert, access logs).
JPMA EDC Supplement	1.4d	Maintain a security system for the data;
JPMA EDC Supplement	1.5.1.2b	The system must be designed to prevent and/or detect unauthorized access. For example, the system has a function that demands an access code in case of loss of a device, or a specific equipment or program to download data from the device, etc.
MHLWCS	6.4.1	The Operation Manager should conduct the followings activities in accordance with the Operations Management Code, etc.; (1) To configure access privileges of persons in charge of input, modification, deletion, etc. of data and to take preventive actions against unauthorized accesses.
NMPA Clinical Trial DM Guide	3.3.3.a	Clinical trial data management system must have a sound management system privileges. Paper-based or electronic data management are needed to develop SOPs for access control and management. Data management system for different people with different permissions or roles that only authorized personnel are allowed to operate (record, modify, etc.), and shall take appropriate methods to monitor and prevent non-licensed person operation.
NMPA PISS	10.3	Personal information controllers should establish appropriate data security capabilities and implement necessary management and technical measures to prevent leakage, damage, and loss of personal information in accordance with the requirements of relevant national standards.
Taiwan Computerized Systems	8.3.6	Security measures that prevent unauthorized access to data and documents should be maintained.

Copyright eClinical Forum

Regulatory mapping for eCF Requirement ID C21

There are system features and processes to manage, preclude and report on **security issues** following current physical and logical **information security** best practices.

Regulation	Paragraph	Description
FDA 21 CFR Part 11	100a	(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.
FDA 21 CFR Part 11	100b	(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.
FDA 21 CFR Part 11	10j	(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.
FDA 21 CFR Part 11	300b	(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).
FDA 21 CFR Part 11 Q and A	Q11a	Logical and physical access controls should be integral to electronic systems used in clinical investigations to limit system access to authorized users, particularly for systems that provide access to multiple users or systems that are accessed through networks.
FDA 21 CFR Part 11 Q and A	Q11b	The selection and application of access controls should be based on an appropriately justified and documented risk assessment to protect the authenticity, integrity, and confidentiality of the data or information.
FDA 21 CFR Part 11 Q and A	Q11c	Security safeguards (e.g., firewalls; antivirus, anti-malware, and anti-spyware software) should be in place and updated, as appropriate, to prevent, detect, and remedy the effects of computer viruses; replicating malware computer programs (i.e., worms); and other potentially harmful software code on clinical investigation data, software, and hardware.
FDA 21 CFR Part 11 Q and A	Q11d	...it is nonetheless important to have audit trails or other physical, logical, or procedural security measures in place to ensure the trustworthiness and reliability of the electronic records.
FDA 21 CFR Part 11 Q and A	Q21a	DHTs should be designed to prevent unauthorized changes to the data stored on the DHT. Access controls (e.g., personal identification numbers, biometrics, multi-factor authentication) should be in place for a mobile application that relies on user entry of data to ensure that entries come from the participants, clinical trial personnel, or other individuals authorized to enter the data (e.g., health care providers, parents, or other caregivers).
Japanese APPI	Article 23	A business operator handling personal information must take necessary and appropriate measures to prevent leakage, loss or damage of the personal data it handles and to otherwise manage the security of personal data.
FDA CSUCI	D1f	We also recommend that passwords or other access keys be changed at established intervals commensurate with a documented risk assessment.
FDA CSUCI	E5	We also recommend that controls be implemented to prevent, detect, and mitigate effects of computer viruses, worms, or other potentially harmful software code on study data and software.
PMDA EDC Management Sheet version 2	41	Measures for maintaining security: Authentication - ID/password - One-time password - Biometrics authentication (fingerprint, retina, vein) - Other ( )
PMDA EDC Management Sheet version 2	43	Procedures for maintaining of security: Written procedures of requesting user registration, granting ID/password, reviewing users, removing the registered users
EMA Computerised Systems	5.4.a	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.
EMA Computerised Systems	A4.1	The responsible party should maintain a security system that prevents unauthorised access to the data.

Copyright eClinical Forum

EMA Computerised Systems	A4.12.a	The method of authentication in a system should positively identify users with a high degree of certainty. ...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.
EMA Computerised Systems	A4.14	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.
EMA Computerised Systems	A4.15	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.
EMA Computerised Systems	A4.3	...firewall rules should be defined. These should be defined as strict as practically feasible, only allowing necessary and permissible traffic. ...firewall rules and settings should be periodically reviewed.
EMA Computerised Systems	A4.4	Relevant security patches for platforms and operating systems should be applied in a timely manner, according to vendor recommendations.
EMA Computerised Systems	A4.6	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.
EMA Computerised Systems	A4.7	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.
EMA Computerised Systems	A4.8	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.
EMA Computerised Systems	A4.9	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.
EMA Computerised Systems	A5.1.3.2.a	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.
EMA Computerised Systems	A5.1.3.2.b	Risks linked to known application and operating system vulnerabilities should be minimised.
EMA Computerised Systems	A5.1.3.2.c	Access to the application and trial participant data may be protected with multiple barriers (e.g. unlock mobile phone, open application, access data).
EMA Computerised Systems	A6.6	Security measures that prevent unauthorised access to data and documents should be maintained.
EMA Computerised Systems	A6.8.a	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.
EMA Computerised Systems	A6.8.b	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.
MHLW ERES (Japan)	3.1.1.1	Rules and procedures of maintaining securities of the system are documented and practicing them appropriately.
FDA DHT for RDA in CI	IV.A.3	Safeguards should be in place to manage cybersecurity risks, prevent unauthorized access to the DHT and the data it collects, and ensure privacy and security.
FDA DHT for RDA in CI	IV.F.1	Sponsors should consider cybersecurity threats that could potentially impact the functionality of the DHT, resulting in a clinical risk to participants (e.g., corrupting the output of a continuous glucose monitor). Accordingly, sponsors should consider FDA information on cybersecurity to ensure that data can be securely stored and transmitted.
FDA Real World Data	III.Ce	Sponsors should address whether the registry has privacy and security controls in place to ensure that the confidentiality and security of data are preserved.
FDA Real		

Copyright eClinical Forum

World Data	III.Dd	...the sponsor should consider whether... The procedures and access controls in place protect the privacy of patient data
EU GDPR	Article 32.1d	A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
EU GDPR	Article 32.2	In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
USA HIPAA	164.308a5iiB	Procedures for guarding against, detecting, and reporting malicious software.
ICH E6 GCP R3 Good Clinical Practice	III.2.12.10e	Ensure that incidents in the use and operation of computerised systems, which in the investigator's/institution's judgement may have a significant and/or persistent impact on the trial data or system security, are reported to the sponsor and, where applicable, to the IRB/IEC.
ICH E6 GCP R3 Good Clinical Practice	III.3.16.1v	The sponsor should ensure that trial data are protected from unauthorised access, disclosure, dissemination or alteration and from inappropriate destruction or accidental loss.
ICH E6 GCP R3 Good Clinical Practice	III.3.16.1w	The sponsor should have processes and procedures in place for reporting to relevant parties, including regulatory authorities, incidents (including security breaches) that have a significant impact on the trial data.
ICH E6 GCP R3 Good Clinical Practice	III.3.16.1xi	Have a record of the important computerised systems used in a clinical trial. This should include the use, functionality, interfaces and validation status of each computerised system, and who is responsible for its management should be described. The record should also include a description of implemented access controls and internal and external security measures.
ICH E6 GCP R3 Good Clinical Practice	III.4.3.3a	The security of the trial data and records should be managed throughout the data life cycle.
ICH E6 GCP R3 Good Clinical Practice	III.4.3.3b	The responsible party should ensure that security controls are implemented and maintained for computerised systems. These controls should include user management and ongoing measures to prevent, detect and/or mitigate security breaches. Aspects such as user authentication requirements and password management, firewall settings, antivirus software, security patching, system monitoring and penetration testing should be considered.
JPMA EDC Guidance	4.1.1.2c	The ability to prevent unauthorized access. (take a measure of malware and security hole, management and prevent of leaking of ID and password, user management).
JPMA EDC Supplement	1.4d	Maintain a security system for the data;
JPMA EDC Supplement	1.5.1.2b	The system must be designed to prevent and/or detect unauthorized access. For example, the system has a function that demands an access code in case of loss of a device, or a specific equipment or program to download data from the device, etc.
MHLWCS	6.4.3	The Operation Manager should conduct the followings activities in accordance with the Operations Management Code, etc.; (3) To limit accesses to the hardware installation areas as necessary. (4) To document and retain records on information security management.
NMPA Clinical Trial DM Guide	3.3.3.d	The electronic management system, password should be changed regularly
NMPA Clinical Trial DM Guide	5.12.b	Related computer must have the corresponding effective antivirus settings, including firewall, kill virus software.
NMPA PISS	10.3	Personal information controllers should establish appropriate data security capabilities and implement necessary management and technical measures to prevent leakage, damage, and loss of personal information in accordance with the requirements of relevant national standards.
PMDA Points to Note in CR and PMS	4.C.5.A	The investigator shall take measures to connect the investigator or the clinical trial collaborator to the subject, etc., in order to prevent a third party from participating when the investigator or the study collaborator evaluates the efficacy and safety of the drug via a video call system. ... In addition, the investigator and other investigators and clinical trial collaborators should consider the privacy of the subjects, etc., such as making sure that the voice is not leaked and heard by other patients.
Guidelines for RDC	3.6.1	Trial clients should consider network security, which may affect DHT functionality and / or infringe on subject privacy. Therefore, trial clients should ensure that DHT can store and transmit data securely.
Taiwan Computerized	5.4.a	To maintain data integrity and the protection of the rights of trial participants, computerized systems used in clinical trials should have security processes and features to prevent unauthorized access and unwarranted data changes and should maintain blinding of the treatment allocation where applicable. Checks should be used to ensure that only authorized 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 authorization of

Copyright eClinical Forum

Systems		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.
Taiwan Computerized Systems	8.2.1.3.2.a	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.
Taiwan Computerized Systems	8.2.1.3.2.b	Risks linked to known application and operating system vulnerabilities should be minimized.
Taiwan Computerized Systems	8.2.1.3.2.c	Access to the application and trial participant data may be protected with multiple barriers (e.g. unlock mobile phone, open application, access data).
Taiwan Computerized Systems	8.3.6	Security measures that prevent unauthorized access to data and documents should be maintained.
Taiwan Computerized Systems	8.3.8.a	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.
Taiwan Computerized Systems	8.3.8.b	If the site has accepted to provide remote access, appropriate security measures and procedures should be in place to support such access without jeopardizing patient rights and data integrity and national legislation.

Copyright eClinical Forum

Regulatory mapping for eCF Requirement ID C22

System feature to allow **automatic logoff** or other access lock (such as password protected screen saver) after a set period of time of inactivity.

Regulation	Paragraph	Description
FDA CSUCI	D1g	When someone leaves a workstation, the person should log off the system. Alternatively, an automatic log off may be appropriate for long idle periods. For short periods of inactivity, we recommend that a type of automatic protection be installed against unauthorized data entry (e.g., an automatic screen saver can prevent data entry until a password is entered).
EMA Computerised Systems	A4.17	Systems should include an automatic inactivity logout, which logs out a user after a defined period of inactivity.
FDA Real World Data	III.Ce	Sponsors should address whether the registry has privacy and security controls in place to ensure that the confidentiality and security of data are preserved.
JPMA EDC Guidance	4.1.1.2c	The ability to prevent unauthorized access. (take a measure of malware and security hole, management and prevent of leaking of ID and password, user management).
JPMA EDC Supplement	1.4d	Maintain a security system for the data;
NMPA Clinical Trial DM Guide	3.3.3.b	The electronic management system, the system should have a personal account for each user, system requirements before you start data manipulation login account, exit the system after completion
NMPA Clinical Trial DM Guide	3.3.3.e	The electronic management system, leave your workstation should terminate the connection to the host computer is idle for a long time to implement self-disconnect after short pause work, there should be automatic protection procedures to prevent unauthorized data manipulation, such as the use of the screen before entering the password protection.

Copyright eClinical Forum

Regulatory mapping for eCF Requirement ID C24

System has the ability to produce a **human-readable** copy of data (which includes associated audit trails and any decoded data) in appropriate file formats that facilitate review, searching and analysis.

Regulation	Paragraph	Description
FDA 21 CFR Part 11	10b	(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.
FDA 21 CFR Part 11 Q and A	Q5	FDA may request copies of these records (e.g., screenshots or paper printouts) and data in a human-readable form.
FDA CSUCI	C3	When source data are transmitted from one system to another (e.g., from a personal data assistant to a sponsors server), or entered directly into a remote computerized system (e.g., data are entered into a remote server via a computer terminal that is located at the clinical site), or an electrocardiogram at the clinical site is transmitted to the sponsors computerized system, a copy of the data should be maintained at another location, typically at the clinical site but possibly at some other designated site.
FDA CSUCI	C4	Copies should be made contemporaneously with data entry and should be preserved in an appropriate format, such as XML, PDF or paper formats.
PMDA EDC Management Sheet version 2	68	Does the system ensure the readability of retained information? (After completion of clinical trials)
EMA Computerised Systems	4.5.b	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.
EMA Computerised Systems	6.2.1.e	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.
EMA Computerised Systems	6.4.b	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.
EMA eTMF Guideline	2	The TMF should provide for document identification, version history, search and retrieval; also, as stated in both Directive 2005/28/EC (Article 17) and the Regulation (Articles 57 and 58) it shall be archived in a way that ensures that it is readily available and directly accessible upon request, to the competent authorities of the Member States.
EMA eTMF Guideline	4.1.1	At all times the storage area for the TMF documents (such as paper or electronic media archives and server rooms) should be appropriate to maintain the documents in a manner that they remain complete and legible throughout the trial conduct and the required period of retention and can be made available to the competent authorities of the Member States, upon request.
EMA Q&A eTMF 1	a	The e-TMF should allow review in an efficient manner, analagous to that possible with paper TMFs. Such a review should not take longer to access than for a paper TMF. (Efficient, straightforward navigation and opening of documents permitting searching and browsing (analogous to leafing through a paper file).
MHLW ERES (Japan)	3.1.2	Readability of electromagnetic records The contents of electromagnetic records shall be output (output to display, output to paper and copy to electronic storage media) as human readable format.
MHLW ERES (Japan)	3.1.3.2	When maintained electromagnetic records will be migrated into other electronic storage media or method, migrated electromagnetic records shall be established its authenticity, readability and storability.
EU Annex 11	8.1	It should be possible to obtain clear printed copies of electronically stored data.
EU Clinical Trials Regulation 536 2014	58e	The media used to archive the content of the clinical trial master file shall be such that the content remains complete and legible throughout the period referred to in the first paragraph.
FDA Real World Data	III.E	Sponsors seeking to use registry data to support a drugs effectiveness and/or safety in a marketing application should ensure that patient-level data are provided to FDA in accordance with applicable legal and regulatory requirements. If the registry data are owned and controlled by third parties, sponsors should ensure that relevant patient-level data can be provided to FDA and that metadata and source records necessary to verify the RWD are made available for inspection, as applicable.

Copyright eClinical Forum

ICH GCP	1.63	A copy (irrespective of the type of media used) of the original record that has been verified (i.e., by a dated signature or by generation through a validated process) to have the same information, including data that describe the context, content, and structure, as the original.
JPMA EDC Guidance	4.1.1.3e	The electronic CRF copy which is maintained by investigators shall meet following requirements. - The electronic CRF copy is exported directly or converted automatically (which shall be qualified in advance) from the original data in the server. - The electronic CRF copy shall be comparable to the original. - The electronic CRF copy shall be identified. - Be able to identify the time point of copy from the original.
JPMA EDC Guidance	4.1.2	1) The ability to generate output for display and printouts of every input/modified data and audit trail (including electronic signature) for human readable format at anytime. 2) Readability means that not only human readable format but also legible and easy to read. Poor display functionality such as users are obliged to trace many tables according to some kind of key code is not met with readability requirements. All information shall be integrated when users display or print out.
JPMA EDC Guidance	4.2.2	Clinical data captured can be displayed on screen or printed on paper as forms or inventory for each clinical case.
JPMA EDC Supplement	1.5.2a	All the data entered into an ePRO system and audit trail should be able to output in a human-readable format (e.g. showing on a display device, printing on paper, copying to electromagnetic recording media). The output should be easy to read and handle.
NMPA Clinical Trial DM Guide	5.13.d	The following table illustrates the different types of clinical trial data and common archive format. - CSV: Comma delimited ASCII text file, you can use a text editor, word processor and Excel spreadsheet software to edit. - XML: In ASCII technology, different systems to facilitate the conversion of structured information. - SAS Version 5 transport files: SAS offers an open source format. Typically used to submit clinical trial data. - Adobe PDF: Widely used text output formats.
NMPA Clinical Trial DM Guide	5.13.e	For the use of electronic data test, clinical trial data management system vendor shall provide a copy of the clinical research center all the electronic case report form as a PDF file format to record.
Guidelines for RDC	3.7d	The trial host must also allow the competent authority to obtain and copy such records.
Taiwan Computerized Systems	4.5.b	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.
Taiwan Computerized Systems	6.2.1.e	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.
Taiwan Computerized Systems	6.4.b	The method of copying should be practical and should ensure that the resulting copy is complete and accurate, including relevant metadata.

Copyright eClinical Forum

Regulatory mapping for eCF Requirement ID C25

Copies of electronic records must be **certified copies** if they are being used for regulatory purposes

Regulation	Paragraph	Description
FDA 21 CFR Part 11 Q and A	Q3	...the copy maintained and retained should be a certified copy that includes the date and time when the copy was created. A certified copy is a copy (irrespective of the type of media used) of the original record that has been verified (i.e., by a dated signature or by generation through a validated process) to have the same information, including data that describe the context, content, and structure, as the original.
EMA Computerised Systems	4.5.b3	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.
EMA Computerised Systems	6.4.a	If essential documents or source documents are irreversibly replaced by a copy, the copy should be certified.
EMA Computerised Systems	6.4.b	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.
EMA Computerised Systems	6.5	...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.
EMA eTMF Guideline	5.1	A certified copy is a paper or electronic copy of the original document that has been verified (e.g. by a dated signature) or has been generated through a validated process to produce an exact copy having all the same information, including data that describe the context, content and structure, as the original. The ICH GCP guideline requires that copies (irrespective of the media used) in the eTMF that irreversibly replace originals should be certified copies of the original. Any transfer or conversion (e.g. digitisation or printing), which does not fulfil the criteria for a certified copy, is not suitable to replace an original file.
EMA Q&A eTMF 1	c	Documents held on an e-TMF should be evidently authentic, complete and legible copies of the original documents.
EMA RBM in CT	1.1	The key elements of the quality system include:... documentation system that preserves and allows for the retrieval of any information/documentation (quality records/essential documents) to show actions taken, decisions made and results
EMA RBM in CT	1.4	The key elements of the quality system include:... quality assurance including internal and external audits performed by independent auditors
FDA Real World Data	III.E	Sponsors seeking to use registry data to support a drugs effectiveness and/or safety in a marketing application should ensure that patient-level data are provided to FDA in accordance with applicable legal and regulatory requirements. If the registry data are owned and controlled by third parties, sponsors should ensure that relevant patient-level data can be provided to FDA and that metadata and source records necessary to verify the RWD are made available for inspection, as applicable.
ICH E6 GCP R3 Good Clinical Practice	C.2.9	When a copy is used to permanently replace the original essential record, the copy should fulfil the requirements for certified copies.
ICH GCP	1.63	A copy (irrespective of the type of media used) of the original record that has been verified (i.e., by a dated signature or by generation through a validated process) to have the same information, including data that describe the context, content, and structure, as the original.
ICH GCP	8.1	ADDENDUM The sponsor and investigator/institution should maintain a record of the location(s) of their respective essential documents including source documents. The storage system used during the trial and for archiving (irrespective of the type of media used) should provide for document identification, version history, search, and retrieval. Essential documents for the trial should be supplemented or may be reduced where justified (in advance of trial initiation) based on the importance and relevance of the specific documents to the trial. The sponsor should ensure that the investigator has control of and continuous access to the CRF data reported to the sponsor. The sponsor should not have exclusive control of those data. When a copy is used to replace an original document (e.g., source documents, CRF), the copy should fulfill the requirements for certified copies. The investigator/institution should have control of all essential documents and records generated by the investigator/institution before, during, and after the trial.
JPMA EDC	4.1.3.2.A1	In case of data (original) transfer, the data shall be exported directly or converted automatically (which shall be qualified in advance)

Copyright eClinicalForum

Guidance		and keeping their contents and meaning.
MHRA GXP Data Integrity Guidance	6.11.2	A copy (irrespective of the type of media used) of the original record that has been verified (i.e. by a dated signature or by generation through a validated process) to have the same information, including data that describe the context, content, and structure, as the original.
Taiwan Computerized Systems	4.5.b3	Data should be the original first generation/capture of the observation. Certified copies can replace original data. Information that is originally captured in a dynamic state should remain available in that state.
Taiwan Computerized Systems	6.4.a	If essential documents or source documents are irreversibly replaced by a copy, the copy should be certified.
Taiwan Computerized Systems	6.4.b	The method of copying should be practical and should ensure that the resulting copy is complete and accurate, including relevant metadata.
Taiwan Computerized Systems	6.5	...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.

Copyright eClinical Forum

Regulatory mapping for eCF Requirement ID C26

There are sufficient system and/or process controls for **backup and recovery** procedures. Documentation can be produced for **inspection** by a monitor, auditor or inspector.

Regulation	Paragraph	Description
FDA CSUCI	F4a	When electronic formats are the only ones used to create and preserve electronic records, sufficient backup and recovery procedures should be designed to protect against data loss.
FDA CSUCI	F4b	Records should regularly be backed up in a procedure that would prevent a catastrophic loss and ensure the quality and integrity of the data. Records should be stored at a secure location specified in the SOP. Storage should typically be offsite or in a building separate from the original records.
FDA CSUCI	F4c	We recommend that you maintain backup and recovery logs to facilitate an assessment of the nature and scope of data loss resulting from a system failure.
FDA CSUCI	S09	- Data backup, recovery, and contingency plans
PMDA EDC Management Sheet version 2	59 and 61	Procedures for data backup and recovery: Written procedure for management of data backup and recovery (During the conduct of clinical trials and after completion of clinical trials)
EMA Computerised Systems	6.8.a	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.
EMA Computerised Systems	6.8.b	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.
EMA eTMF Guideline	4.1.2c	The primary eTMF is a system for managing documents that should contain the controls listed below: regular backup;
EMA eTMF Guideline	4.1.2d	The primary eTMF is a system for managing documents that should contain the controls listed below: periodic test retrieval or restores to confirm the on-going availability and integrity of the data;
EMA IRT Reflection Paper	2.2.3d	Disaster recovery system - there should be back-up systems in place such that if there is a server break-down the IRT is still able to keep running. There will be occasions when the system is down and the provider should have prepared for these such that manual interventions can be made, documented and the system updated when it is fully operational again.
EMA RBM in CT	1.4	The key elements of the quality system include:... quality assurance including internal and external audits performed by independent auditors
MHLW ERES (Japan)	3.1.1.3	The procedure of backup of electromagnetic records is documented and practicing appropriately.
MHLW ERES (Japan)	3.1.3	Storability electromagnetic records Electromagnetic records shall be maintained with keeping its authenticity and readability.
EU Annex 11	7.2	Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically.
EU Clinical Trials Regulation 536 2014	58b	The content of the clinical trial master file shall be archived in a way that ensures that it is readily available and accessible, upon request, to the competent authorities.
EU GDPR	Article 32.1b	The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
EU GDPR	Article 32.1c	The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
EU GDPR	Article 32.1d	A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
EU GDPR	Article 32.2	In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
EU GDPR	Article 5.1e	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality).

Copyright eClinical Forum

USA HIPAA	164.308a7iiB	Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.
ICH E6 GCP R3 Good Clinical Practice	III.4.3.3c	The responsible party should maintain adequate backup of the data.
ICH E6 GCP R3 Good Clinical Practice	III.4.3.3d	Procedures should cover the following: system security measures, data backup and disaster recovery to ensure that unauthorised access and data loss are prevented. Such measures should be periodically tested, as appropriate.
ICH GCP	4.9.4	The investigator/institution should maintain the trial documents as specified in Essential Documents for the Conduct of a Clinical Trial (see 8.) and as required by the applicable regulatory requirement(s). The investigator/institution should take measures to prevent accidental or premature destruction of these documents.
ICH GCP	5.5.3b	When using electronic trial data handling and/or remote electronic trial data systems,the sponsor should: b) Maintains SOPs for using these systems. ADDENDUM The SOPs should cover system setup, installation, and use. The SOPs should describe system validation and functionality testing, data collection and handling, system maintenance, system security measures, change control, data backup, recovery, contingency planning, and decommissioning. The responsibilities of the sponsor, investigator, and other parties with respect to the use of these computerized systems should be clear, and the users should be provided with training in their use.
ICH GCP	5.5.3f	When using electronic trial data handling and/or remote electronic trial data systems,the sponsor should: f) Maintain adequate backup of the data.
JPMA EDC Guidance	4.1.1.5	Backup of CRF data and EDC system (including users list, access rights information, and so on) is performed appropriately. a) According to the documented procedures, latest electronic CRF data, audit trail and electronic signatures are backup periodically. In case of emergency, CRF data shall be recovered in accordance with predetermined procedures. In this case the original data set shall be uniquely identified. b) In terms of recognizing that the recovered data is original, recovering procedures shall be tested and qualified in advance. c) In case of H/W or S/W incidents, the environments shall be recovered in accordance with predetermined procedures.
JPMA EDC Supplement	1.4e	Maintain the adequate backup of the data;
JPMA EDC Supplement	1.5.1.4a	Based on a documented procedure, the latest data should be backed up on a regular schedule. In case of an unexpected situation, the data should be restored through a predetermined procedure.
MHLWCS	6.5.3	The Operation Manager should have the designated persons designated conduct the following activities in accordance with the Operations Management Code, etc.; (3) To document and retain records on backup and restore
MHRA GXP Data Integrity Guidance	6.17.2	Backup and recovery processes should be validated and periodically tested. Each back up should be verified to ensure that it has functioned correctly e.g. by confirming that the data size transferred matches that of the original record. The backup strategies for the data owners should be documented.
MHRA GXP Data Integrity Guidance	6.17a	Data retention may be for archiving (protected data for long-term storage) or backup (data for the purposes of disaster recovery).
NMPA Clinical Trial DM Guide	3.3.1.f	Clinical trial data management system validation include the following aspects: - Disaster Recovery Plan / Backup
NMPA Clinical Trial DM Guide	5.12.a	Data management throughout the study process, the database should be backed up. Usually in addition a separate computer for backup, and according to the progress of work weekly backup file synchronization update. Final data set will be backed up on CD-ROM form, when necessary, the dataset is not locked disc can also be backed up. When the database irreparable damage occurs, you should use the most recent backup to restore the database and adds the corresponding data entry.
NMPA PISS	10.3	Personal information controllers should establish appropriate data security capabilities and implement necessary management and technical measures to prevent leakage, damage, and loss of personal information in accordance with the requirements of relevant national standards.
NMPA PISS	10.5d	Unauthorized access, tampering or deletion of audit records should be prevented.
Taiwan Computerized Systems	6.8.a	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.
Taiwan Computerized Systems	6.8.b	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.

Copyright eClinical Forum

Regulatory mapping for eCF Requirement ID C28

Process and/or system controls ensure that regulated data used for clinical research, including source data and metadata are enduring, continue to be available, readable and understandable and are retained in an **archive** for the legal period.

Regulation	Paragraph	Description
FDA 21 CFR Part 11	10c	(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.
FDA 21 CFR Part 11	10e	(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.
FDA 21 CFR Part 11 Q and A	Q5a	Regulated entities must ensure that electronic records are maintained for the applicable retention period, and these records must be available for inspection in accordance with any applicable requirements.
FDA 21 CFR Part 312	62c	An investigator shall retain records required to be maintained under this part for a period of 2 years following the date a marketing application is approved for the drug for the indication for which it is being investigated; or, if no application is to be filed or if the application is not approved for such indication, until 2 years after the investigation is discontinued and FDA is notified
Japanese APPI	Article 22	A business operator handling personal information shall keep personal data accurate and up-to-date to the extent necessary to achieve the purpose of use, and when it is no longer necessary to use the personal data, the personal data shall be deleted without delay. Efforts must be made to eliminate.
FDA CSUCI	C2	Under 21 CFR 312.62, 511.1(b)(7)(ii) and 812.140, the clinical investigator must retain records required to be maintained under part 312, 511.1(b), and part 812, for a period of time specified in these regulations. This requirement applies to the retention of the original source document, or a copy of the source document.
PMDA EDC Management Sheet version 2	51	Written procedure for securing the authenticity of retained information: Written procedure for modifying information retained in the EDC System
PMDA EDC Management Sheet version 2	73	Ensuring the storability throughout the retention period: Written procedure for retaining electromagnetic records after the completion of clinical trials
EMA Computerised Systems	4.5.d	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.
EMA Computerised Systems	4.5.e	Data should be stored throughout the data life cycle and should be readily available for review when needed.
EMA Computerised Systems	6.11	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.
EMA Computerised Systems	6.12.a	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. ... Static formats of dynamic data will not be considered adequate.
EMA Computerised Systems	A5.3.2	Secure archiving should ensure availability and legibility for the required retention period.

Copyright eClinicalForum

EMA Computerised Systems	A5.3.7	The informed consent documents are essential documents that should be available at the trial site in the investigator TMF for the required retention period.
EMA Computerised Systems	A5.3.9	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.
EMA Computerised Systems	A6.10	Appropriate archiving should be in place to ensure long term readability, reliability, retrievability of electronic data (and metadata), in line with regulatory retention requirements.
EMA eTMF Guideline	2	The TMF should provide for document identification, version history, search and retrieval; also, as stated in both Directive 2005/28/EC (Article 17) and the Regulation (Articles 57 and 58) it shall be archived in a way that ensures that it is readily available and directly accessible upon request, to the competent authorities of the Member States.
EMA eTMF Guideline	3.2d	The clinical trial contract/agreement and other documents and procedures agreed between all parties should outline the arrangements for the TMF in some detail, such as: - retention times; - arrangements regarding the archiving of and access to data/documents held in centralised systems (such as central training documents and central e-mail repository).
EMA eTMF Guideline	3.2e	The clinical trial contract/agreement and other documents and procedures agreed between all parties should outline the arrangements for the TMF in some detail, such as: - procedures in case of an involved party closing down its business for any reason.
EMA eTMF Guideline	3.5.1	Documents demonstrating software validation may be retained by a CRO when the activity has been contracted by the sponsor, but the sponsor should ensure continued access to these documents in the contractual arrangements with the CRO for the required archiving period. Documents relating to the trial-specific software configuration are part of the TMF and it should be determined whether these are maintained/archived by the sponsor or CRO providing this service. Some documents from good manufacturing practice activities should also be defined as part of the TMF, for example, when these relate to the assembly and packaging of the investigational medicinal product (IMP) and confirm, as applicable, compliance with the randomisation schedule and blinding of the trial.
EMA eTMF Guideline	4.1.1	At all times the storage area for the TMF documents (such as paper or electronic media archives and server rooms) should be appropriate to maintain the documents in a manner that they remain complete and legible throughout the trial conduct and the required period of retention and can be made available to the competent authorities of the Member States, upon request.
EMA eTMF Guideline	4.1.2b	The primary eTMF is a system for managing documents that should contain the controls listed below: user accounts; a system in place locking/protecting individual documents or the entire eTMF (e.g. at time of archiving) to prevent changes to documents.
EMA eTMF Guideline	4.1.2g	The primary eTMF is a system for managing documents that should contain the controls listed below: user accounts; the suitability of the system for archiving purposes should be appropriate.
EMA eTMF Guideline	4.1.3g	All agreements should include provisions for the situation that any of the parties mentioned above are going out of business and how the integrity and accessibility of the complete investigator TMF will be maintained throughout the required archiving period.
EMA Q&A eTMF 1	d	The e-TMF system should have validated methods for preventing any changes being made to the TMF documents, this includes the process of transferring from original media to the electronic medium.
MHLW ERES (Japan)	3.1.1	Authenticity of electromagnetic records Electromagnetic records are complete, accurate and reliable, and also responsibilities of its creation, modification and deletion are definite.
MHLW ERES (Japan)	3.1.3	Storability electromagnetic records Electromagnetic records shall be maintained with keeping its authenticity and readability.
EU Annex 11	17	Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested.
EU Directive 2005 28	2.4.17	The sponsor and the investigator shall retain the essential documents relating to a clinical trial for at least five years after its completion.They shall retain the documents for a longer period, where so required by other applicable requirements or by an agreement between the sponsor and the investigator. Essential documents shall be archived in a way that ensures that they are readily available, upon request, to the competent authorities.The medical files of trial subjects shall be retained in accordance with national legislation and in accordance with the maximum period of time permitted by the hospital, institution or privatepractice.
EU Directive 2005 28	2.4.20	The media used to store essential documents shall be such that those documents remain complete and legible throughout the required period of retention and can be made available to the competent authorities upon request. Any alteration to records shall be traceable.
EU Clinical Trials Regulation 536 2014	57	The clinical trial master file shall at all times contain the essential documents relating to that clinical trial which allow verification of the conduct of a clinical trial and the quality of the data generated, taking into account all characteristics of the clinical trial, including in particular whether the clinical trial is a low-intervention clinical trial. It shall be readily available, and directly accessible upon request, to the Member States.
EU Clinical Trials Regulation	58a	Unless other Union law requires archiving for a longer period, the sponsor and the investigator shall archive the content of the clinical trial master file for at least 25 years after the end of the clinical trial. However, the medical files of subjects shall be archived

Copyright eClinical Forum

536 2014		in accordance with national law.
EU Clinical Trials Regulation 536 2014	58b	The content of the clinical trial master file shall be archived in a way that ensures that it is readily available and accessible, upon request, to the competent authorities.
EU Clinical Trials Regulation 536 2014	58e	The media used to archive the content of the clinical trial master file shall be such that the content remains complete and legible throughout the period referred to in the first paragraph.
FDA EHR Guidance	V.B.4	Records are available and retained for FDA inspection for as long as the records are required by applicable regulations.
FDA EHR Guidance	VI.2	Clinical investigators must retain all records.
FDA EHR Guidance	VI.3	Investigator or sponsor must maintain all records.
FDA Electronic Informed Consent Q&A	Q15	The eIC process should incorporate procedures to ensure that electronic documents can be archived appropriately and that all versions of the IRB-approved eIC can be retrieved easily.
FDA eSource Guidance	A2c	Transcription of Data From Paper or Electronic Sources to the eCRF Data elements can be transcribed into the eCRF from paper or electronic source documents. The authorized person transcribing the data from the source documents is regarded as the data originator. For these data elements, the electronic or paper documents from which the data elements are transcribed are the source. These data must be maintained by the clinical investigator(s) and available to an FDA inspector if requested (e.g., an original or certified copy of a laboratory report, instrument printout, progress notes of the physician, the study subjects hospital chart(s), nurses notes).
FDA and MHRA Data Integrity Discussions	P13	The sponsor has flexibility in where these essential documents should be retained but the location for long-term retention should be defined in the quality system and should be appropriate to the type of file (i.e., dynamic file or flat file). The retention times required by regulation necessitates the need for managed archival of electronic files.
FDA and MHRA Data Integrity Discussions	P14a	There should be quality assurance and quality control mechanisms at each stage of data handling.
FDA Real World Data	III.Db	Documentation of the process sponsors used to validate the transfer of data from an external data source to the registry should be available for FDA to review during sponsor inspections.
FDA Real World Data	III.Dc	Sponsors should also ensure that software updates to the registry database or additional data sources do not affect the integrity, interoperability, and security of data transmitted to the registry.
FDA Real World Data	III.E	Sponsors seeking to use registry data to support a drugs effectiveness and/or safety in a marketing application should ensure that patient-level data are provided to FDA in accordance with applicable legal and regulatory requirements. If the registry data are owned and controlled by third parties, sponsors should ensure that relevant patient-level data can be provided to FDA and that metadata and source records necessary to verify the RWD are made available for inspection, as applicable.
EU GDPR	Article 32.1b	The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
EU GDPR	Article 32.1c	The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
EU GDPR	Article 32.1d	A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
USA HIPAA	164.304a	Availability means the property that data or information is accessible and useable upon demand by an authorized person.
USA HIPAA	164.308a8	Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.
ICH E6 GCP R3 Good Clinical Practice	C.2.4	The storage system(s) used during the trial and for archiving (irrespective of the type of media used) should provide for appropriate identification, version history, search and retrieval of trial records.
ICH E6 GCP R3 Good Clinical Practice	C.3.1n	Contains the data as well as relevant metadata that would be needed to allow the appropriate evaluation of the conduct of the trial.
ICH E6 GCP		

Copyright eClinical Forum

R3 Good Clinical Practice	II.9.5a	Essential records should be retained securely by sponsors and investigators for the required period in accordance with applicable regulatory requirements.
ICH E6 GCP R3 Good Clinical Practice	III.2.12.12	The investigator/institution should retain the essential records for the required retention period in accordance with applicable regulatory requirements or until the sponsor informs the investigator/institution that these records are no longer needed, whichever is the longest. The investigator/institution should take measures to ensure availability, accessibility and readability and to prevent unauthorised access and accidental or premature destruction of these records.
ICH E6 GCP R3 Good Clinical Practice	III.3.16.1e	The sponsor should ensure that documented processes are implemented to ensure the data integrity for the full data life cycle.
ICH E6 GCP R3 Good Clinical Practice	III.3.16.1m	The sponsor should ensure that the investigator has access to the required data for retention purposes.
ICH E6 GCP R3 Good Clinical Practice	III.3.16.3a	The sponsor (or subsequent owners of the data) should retain the sponsor-specific essential records pertaining to the trial in accordance with the applicable regulatory requirement(s).
ICH E6 GCP R3 Good Clinical Practice	III.3.16.3b	The sponsor should inform the investigator(s)/institution(s) and service providers, when appropriate, in writing of the requirements for the retention of essential records and should notify the investigator(s)/institution(s) and service providers, when appropriate, in writing when the trial-related records are no longer needed in accordance with applicable regulatory requirements.
ICH E6 GCP R3 Good Clinical Practice	III.3.6.3c	The sponsor should obtain the investigator's/institution's and, where applicable, service provider's agreements: (c) To retain the essential records for the required retention period in accordance with applicable regulatory requirements or until the sponsor informs the investigator/institution or, where applicable, the service provider that these records are no longer needed, whichever is longest.
ICH E6 GCP R3 Good Clinical Practice	III.4.2.7	The trial data and relevant metadata should be archived in a way that allows for their retrieval and readability and should be protected from unauthorised access and alterations throughout the retention period.
ICH GCP	4.9.0	The investigator/institution should maintain adequate and accurate source documents and trial records that include all pertinent observations on each of the site's trial subjects. Source data should be attributable, legible, contemporaneous, original, accurate, and complete. Changes to source data should be traceable, should not obscure the original entry, and should be explained if necessary (e.g., via an audit trail).
ICH GCP	4.9.4	The investigator/institution should maintain the trial documents as specified in Essential Documents for the Conduct of a Clinical Trial (see 8.) and as required by the applicable regulatory requirement(s). The investigator/institution should take measures to prevent accidental or premature destruction of these documents.
ICH GCP	4.9.5	Essential documents should be retained until at least 2 years after the last approval of a marketing application in an ICH region and until there are no pending or contemplated marketing applications in an ICH region or at least 2 years have elapsed since the formal discontinuation of clinical development of the investigational product. These documents should be retained for a longer period however if required by the applicable regulatory requirements or by an agreement with the sponsor. It is the responsibility of the sponsor to inform the investigator/institution as to when these documents no longer need to be retained (see 5.5.12).
ICH GCP	5.18.4k	Verifying that source documents and other trial records are accurate, complete,kept up-to-date and maintained.
ICH GCP	8.1	ADDENDUM The sponsor and investigator/institution should maintain a record of the location(s) of their respective essential documents including source documents. The storage system used during the trial and for archiving (irrespective of the type of media used) should provide for document identification, version history, search, and retrieval. Essential documents for the trial should be supplemented or may be reduced where justified (in advance of trial initiation) based on the importance and relevance of the specific documents to the trial. The sponsor should ensure that the investigator has control of and continuous access to the CRF data reported to the sponsor. The sponsor should not have exclusive control of those data. When a copy is used to replace an original document (e.g., source documents, CRF), the copy should fulfill the requirements for certified copies. The investigator/institution should have control of all essential documents and records generated by the investigator/institution before, during, and after the trial.
JPMA EDC Guidance	4.1.1.3.5	In the institutes, authority and investigators are able to check the data of CRF at anytime within the retention period.
JPMA EDC Guidance	4.1.1.6.4	After new EDC system has gone live, if you discard previous EDC system, related records such as validation deliverables shall be maintained and ensure adequacy of all documents produced by previous EDC system.
JPMA EDC Guidance	4.1.2	1) The ability to generate output for display and printouts of every input/modified data and audit trail (including electronic signature) for human readable format at anytime. 2) Readability means that not only human readable format but also legible and easy to read. Poor display functionality such as users are obliged to trace many tables according to some kind of key code is not met with readability requirements. All information shall

Copyright eClinical Forum

		be integrated when users display or print out.
JPMA EDC Supplement	1.2a	...it is required to prepare necessary equipment (e.g. devices) and environment (e.g. internet line, telephone line) for data entry by subjects, make operational procedures for transmitting subject data to the operational database, operational procedures for providing the collected subject data to investigators. and sponsors, and also procedures for data retention after completion of the clinical trial and location of storage.
JPMA EDC Supplement	1.2d	After the completion of the trial, the source documents on the vendor server are transferred to a CD-R or other general media, such as a PDF file or other format that can adress the requirements of readability and retainability, through a process required for ensuring authenticity, and are stored at the site.
JPMA EDC Supplement	1.4h	It must also be noted that, the ePRO must be durable enough to be kept for their retention period specified in Article 26 of the GCP, The sponsor shall appropriately retain the records, since ePRO refers to data generated in conducting the clinical trial.
JPMA EDC Supplement	1.5.2c	During the transfer of data with the relevant audit trail to recording media for archiving after the completion of the trial, the readability should be maintained at the same level as in the ePRO system, so that such data is easily accessible throughout the specified period of record keeping.
JPMA EDC Supplement	1.5.3	Throughout the specified period of record keeping, the authenticity and readability of the electromagnetic records must be ensured.
MHRA GXP Data Integrity Guidance	6.17.1	Archived records may be the original record or a 'true copy' and should be protected so they cannot be altered or deleted without detection and protected against any accidental damage such as fire or pest. Archive arrangements must be designed to permit recovery and readability of the data and metadata throughout the required retention period. In the case of archiving of electronic data, this process should be validated, and in the case of legacy systems the ability to review data periodically verified (i.e. to confirm the continued support of legacy computerised systems). Where hybrid records are stored, references between physical and electronic records must be maintained such that full verification of events is possible throughout the retention period.
MHRA GXP Data Integrity Guidance	6.2	In the case of basic electronic equipment that does not store electronic data, or provides only a printed data output (e.g. balances or pH meters), then the printout constitutes the raw data. Where the basic electronic equipment does store electronic data permanently and only holds a certain volume before overwriting; this data should be periodically reviewed and where necessary reconciled against paper records and extracted as electronic data where this is supported by the equipment itself.
NMPA Clinical Trial DM Guide	5.13.a	Ensure data security is to prevent the data may be subject to physical damage or damaged. Conducting clinical trials in the process, all the collected raw data (such as CRF and electronic data) stored in a safe place, such as a controlled room to ensure that the appropriate temperature, humidity, fire safety measures have improved, fireproof lock document cabinet. The original document is traced to the original data audit part of the path should be like an electronic audit trail of any changes to the database or backup recording done the same strict protection. Recommended data kept for at least 10 years. Data were entered into the database content and time input data in the database and the history of the amendment requires all intact. Ensure data accessibility refers to the user when needed, such as login and retrieve data from, and the data in the database can be transmitted in a timely manner as needed.
NMPA Clinical Trial DM Guide	5.13.c	In clinical trials completed, the response during the test documents to be archived.
NMPA PISS	6.1a	The retention period of personal information should be the minimum time necessary to achieve the purpose.
Guidelines for RDC	3.7a	DHT to record and transmit data during clinical trials, the relevant data obtained by DHT, including all relevant interpretation data, should be securely transmitted and retained in a durable electronic data repository as part of the clinical trial record.
Guidelines for RDC	3.7b	DHT data output supporting the clinical trial indicator and associated interpretation data should typically be transferred to a durable electronic data repository.
Guidelines for RDC	3.7c	For data collected directly from trial participants through the DHT, data in durable electronic data repositories are generally considered raw data. Such data may have to be reviewed to reconstruct and evaluate the clinical trial and should be available for review.
Guidelines for RDC	3.8.1b	Ensure that data is downloaded from the DHT to a durable electronic data store.
Taiwan Computerized Systems	4.5.d	Data should be maintained appropriately such that they remain intact and durable through the entire data lifecycle.
Taiwan Computerized Systems	4.5.e	Data should be stored all the time and be readily available for review when needed.
Taiwan Computerized Systems	6.10	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 management system of clinical trials, such as trial master file (TMF) 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 remain accessible, throughout the retention period.
		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 that archived formats provide the possibility to restore the database(s). This includes the restoration of

Copyright eClinical Forum

Taiwan Computerized Systems	6.11.a	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 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. ...Static formats of dynamic data will not be considered adequate.
Taiwan Computerized Systems	8.2.3.2.c	Secure archiving should ensure availability and legibility for the required retention period.
Taiwan Computerized Systems	8.2.3.7	The informed consent documents are essential documents that should be available at the trial site in the investigator TMF for the required retention period.
Taiwan Computerized Systems	8.2.3.9	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.
Taiwan Computerized Systems	8.3.10	Appropriate archiving should be in place to ensure long term readability, reliability, retrievability of electronic data (and metadata), in line with regulatory retention requirements.

Copyright eClinical Forum

Regulatory mapping for eCF Requirement ID C29

There are sufficient process controls for the system covering **Business Continuity** to manage disruptive incidents.

Regulation	Paragraph	Description
Japanese APPI	Article 23	A business operator handling personal information must take necessary and appropriate measures to prevent leakage, loss or damage of the personal data it handles and to otherwise manage the security of personal data.
FDA CSUCI	S09	- Data backup, recovery, and contingency plans
FDA CSUCI	S10	- Alternative recording methods (in the case of system unavailability)
EMA Computerised Systems	6.9	Agreements and procedures should be in place to allow trial continuation and prevent loss of data critical to participant safety and trial results.
EMADCT	1	A contingency plan should be in place to minimise the impact of any risk, for example malfunction of a digital tool or disruption of a planned decentralised visit, for identified critical- to-quality decentralised elements.
EMA eTMF Guideline	4.1.3g	All agreements should include provisions for the situation that any of the parties mentioned above are going out of business and how the integrity and accessibility of the complete investigator TMF will be maintained throughout the required archiving period.
EMA IRT Reflection Paper	2.2.3d	Disaster recovery system - there should be back-up systems in place such that if there is a server break-down the IRT is still able to keep running. There will be occasions when the system is down and the provider should have prepared for these such that manual interventions can be made, documented and the system updated when it is fully operational again.
EU Annex 11	16	For the availability of computerised systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system). The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.
EU Annex 11	7.1	Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period.
EU GDPR	Article 32.1b	The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
EU GDPR	Article 32.1c	The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
EU GDPR	Article 32.1d	A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
EU GDPR	Article 32.2	In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
EU GDPR	Article 5.1e	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality).
USA HIPAA	164.308a8	Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.
ICH E6 GCP R3 Good Clinical Practice	III.4.3.6	Contingency procedures should be in place to prevent loss or lack of accessibility to data essential to participant safety, trial decisions or trial outcomes.
ICH GCP	5.5.3b	When using electronic trial data handling and/or remote electronic trial data systems,the sponsor should: b) Maintains SOPs for using these systems. ADDENDUM The SOPs should cover system setup, installation, and use. The SOPs should describe system validation and functionality testing, data collection and handling, system maintenance, system security measures, change control, data backup, recovery, contingency planning, and decommissioning. The responsibilities of the sponsor, investigator, and other parties with respect to the use of these computerized systems should be clear, and the users should be provided with training in their use.
JPMA EDC Supplement	1.5.1.4b	In case of hardware or software failure, the operating environment should be restored through a predetermined procedure.
		Personal information controllers should establish appropriate data security capabilities and implement necessary management and

Copyright eClinicalForum

NMPA PISS	10.3	technical measures to prevent leakage, damage, and loss of personal information in accordance with the requirements of relevant national standards.

Copyright eClinical Forum

Regulatory mapping for eCF Requirement ID C30

There are sufficient process controls based on industry standards, covering **Disaster Recovery** Procedures.

Regulation	Paragraph	Description
Japanese APPI	Article 23	A business operator handling personal information must take necessary and appropriate measures to prevent leakage, loss or damage of the personal data it handles and to otherwise manage the security of personal data.
EMA Computerised Systems	6.8.c	Disaster mitigation and recovery plans should be in place to deal with events that endanger data security. Such plans should be regularly reviewed.
EMA Computerised Systems	A4.2	A disaster recovery plan should be in place and tested.
EMA IRT Reflection Paper	2.2.3d	Disaster recovery system - there should be back-up systems in place such that if there is a server break-down the IRT is still able to keep running. There will be occasions when the system is down and the provider should have prepared for these such that manual interventions can be made, documented and the system updated when it is fully operational again.
EU GDPR	Article 32.1b	The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
EU GDPR	Article 32.1c	The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
EU GDPR	Article 32.1d	A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
EU GDPR	Article 32.2	In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
EU GDPR	Article 5.1e	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality).
USA HIPAA	164.308a7iiB	Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.
ICH E6 GCP R3 Good Clinical Practice	III.4.3.3d	Procedures should cover the following: system security measures, data backup and disaster recovery to ensure that unauthorised access and data loss are prevented. Such measures should be periodically tested, as appropriate.
ICH E6 GCP R3 Good Clinical Practice	III.4.3.6	Contingency procedures should be in place to prevent loss or lack of accessibility to data essential to participant safety, trial decisions or trial outcomes.
ICH GCP	4.9.4	The investigator/institution should maintain the trial documents as specified in Essential Documents for the Conduct of a Clinical Trial (see 8.) and as required by the applicable regulatory requirement(s). The investigator/institution should take measures to prevent accidental or premature destruction of these documents.
ICH GCP	5.5.3b	When using electronic trial data handling and/or remote electronic trial data systems,the sponsor should: b) Maintains SOPs for using these systems. ADDENDUM The SOPs should cover system setup, installation, and use. The SOPs should describe system validation and functionality testing, data collection and handling, system maintenance, system security measures, change control, data backup, recovery, contingency planning, and decommissioning. The responsibilities of the sponsor, investigator, and other parties with respect to the use of these computerized systems should be clear, and the users should be provided with training in their use.
JPMA EDC Supplement	1.5.1.4b	In case of hardware or software failure, the operating environment should be restored through a predetermined procedure.
MHRA GXP Data Integrity Guidance	6.17b	Data and document retention arrangements should ensure the protection of records from deliberate or inadvertent alteration or loss. Secure controls must be in place to ensure the data integrity of the record throughout the retention period and should be validated where appropriate (see also data transfer/migration).
NMPA Clinical Trial DM Guide	3.3.1.f	Clinical trial data management system validation include the following aspects: - Disaster Recovery Plan / Backup
		Personal information controllers should establish appropriate data security capabilities and implement necessary management and

Copyright eClinicalForum

NMPA PISS	10.3	technical measures to prevent leakage, damage, and loss of personal information in accordance with the requirements of relevant national standards.
Taiwan Computerized Systems	6.8.c	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.

Copyright eClinical Forum

Regulatory mapping for eCF Requirement ID C31

There is a process to demonstrate that individuals who develop, maintain, or use the system should be qualified by having appropriate **education, training**, and experience necessary to perform their assigned task.

Regulation	Paragraph	Description
FDA 21 CFR Part 11	10i	(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.
FDA 21 CFR Part 11 Q and A	Q15	Anyone who develops, maintains, or uses electronic systems subject to part 11 must have the education, training, and experience necessary to perform their assigned tasks.
FDA CSUCI	E2	Staff should be kept thoroughly aware of system security measures and the importance of limiting access to authorized personnel.
FDA CSUCI	G1	Those who use computerized systems must determine that individuals (e.g., employees, contractors) who develop, maintain, or use computerized systems have the education, training and experience necessary to perform their assigned tasks (21 CFR 11.10(i)).
FDA CSUCI	G2	Training should be provided to individuals in the specific operations with regard to computerized systems that they are to perform
FDA CSUCI	G3	Training should be conducted by qualified individuals on a continuing basis, as needed, to ensure familiarity with the computerized system and with any changes to the system during the course of the study.
FDA CSUCI	G4	We recommend that computer education, training, and experience be documented.
FDA CSUCI	S11	- Computer user training
PMDA EDC Management Sheet version 2	95 and 101	Management Method Training Describe the training for the person who manages/maintains electromagnetic records. Training for end users should be described in the above section of "security training for users" (During the conduct of clinical trials and after completion of clinical trials)
EMA Computerised Systems	4.1.c	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.
EMA Computerised Systems	5.3	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.
EMA Computerised Systems	6.2.2	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.
EMA Computerised Systems	A3.1.b	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).
EMA Computerised Systems	A5.1.1.8	Training should be customised to meet the specific needs of the end users.
EMA Computerised Systems	A6.3	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.
EMADCT	2.3	Trial participants, investigators and service providers involved in the trial should receive training on how to use the digital tools employed in the trial, to ensure proper data collection, review, and transmission.
EMADCT	5.3	In the event of trial participants performing trial related tasks it should be ensured that appropriate training is provided to them, and any additional trial participant burden duly considered, including tasks related to digital data collection.
EMADCT	5.4	The sponsor and/or investigator should ensure that appropriate guidance and training is provided to the delegated person(s) to conduct the tasks at home correctly.
EMA eTMF Guideline	3.2g	When a CRO is used for the management of the eTMF and/or for the digitisation/transfer of TMF documents, appropriate pre-qualification checks should be undertaken prior to contracting the CRO. It should be verified during the clinical trial that the CROs quality management measures are complied with.
EMA eTMF	4.1.2i	All staff members involved in the conduct of the trial and using the system should receive appropriate training.

Copyright eClinical Forum

Guideline		
EMA eTMF Guideline	6.1b	The appointment and appropriate training of these individuals should be documented. These individuals should be employed within the organisation of the sponsor or the organisation contracted by the sponsor.
EMA IRT Reflection Paper	2.2.2c	The quality system encompassing the IRT system should include: - Training records for all those involved in the development and day to day running of the system. This should include help desk personnel.
EMA RBM in CT	1.2	The key elements of the quality system include:... appropriate training of sponsor personnel as well as of the personnel in affiliates, at the Contract Research Organisations (CROs), vendors or other service providers and at trial sites
MHLW ERES (Japan)	5	Persons who uses electromagnetic records and electronic signatures for materials and raw-materials of applications for approval or licensing of drugs, and for registration of conformity certification bodies shall prepare documents described persons in charge, managers, organizations, equipments and training for using electromagnetic records and electronic signatures.
EU Annex 11	2	There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.
FDA DHT for RDA in CI	IV.H.3	Trial participants and trial personnel should be trained on the appropriate use of DHTs. In some situations, it may also be appropriate to provide training to participants caregivers.
FDA Electronic Informed Consent Q&A	Q2	If the investigator delegates this responsibility, the responsibility should be delegated to an individual qualified by education, training, and experience to perform this activity.
FDA eSource Guidance	D	Data Access Sponsors, CROs, data safety monitoring boards, and other authorized personnel can view the data elements in the eCRF before and after the clinical investigator(s) has electronically signed the completed eCRF. We encourage viewing the data to allow early detection of study-related problems (e.g., safety concerns, protocol deviations) and problems with conducting the study (e.g., missing data, data discrepancies). The sponsor should have a list (e.g., in a data management plan) of the individuals with authorized access to the eCRF. Only those individuals who have documented training and authorization should have access to the eCRF data. Individuals with authorized access should be assigned their own identification (log-on) codes and passwords. Log-on access should be disabled if the individual discontinues involvement during the study.
FDA Real World Data	III.Ca	When considering using data from an existing registry or establishing a registry de novo, sponsors should ensure that there are processes and procedures to govern registry operation, education and training of registry staff, resource planning, and practices that help ensure the quality of the registry data.
EU GDPR	Article 41.2b	Established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation.
USA HIPAA	164.308a5i	Implement a security awareness and training program for all members of its workforce (including management).
ICH E6 GCP R3 Good Clinical Practice	II.5.1	Individuals involved in a trial should be qualified by education, training and experience to perform their respective task(s).
ICH E6 GCP R3 Good Clinical Practice	III.2.1.1	The investigator(s) should be qualified by education, training and experience to assume responsibility for the proper conduct of the trial and should provide evidence of such qualifications.
ICH E6 GCP R3 Good Clinical Practice	III.2.12.10d	Where equipment for data acquisition is provided to trial participants by the investigator, ensure that traceability is maintained and that participants are provided with appropriate training.
ICH E6 GCP R3 Good Clinical Practice	III.3.16.1n	The sponsor should ensure that the investigator receives instructions on how to navigate systems, data and relevant metadata for the trial participants under their responsibility.
ICH E6 GCP R3 Good Clinical Practice	III.3.16.1xii	Ensure that ... adequate training are in place to ensure the correct development, maintenance and use of computerised systems in clinical trials.
ICH E6 GCP R3 Good Clinical Practice	III.3.4	The sponsor should utilise appropriately qualified individuals for the activities to which they are assigned (e.g., biostatisticians, clinical pharmacologists, physicians, data scientists/data managers, auditors and monitors) throughout the trial process.
ICH E6 GCP R3 Good		

Copyright eClinical Forum

Clinical Practice	III.4.3.2	The responsible party should ensure that those using computerised systems are appropriately trained in their use.
ICH E6 GCP R3 Good Clinical Practice	III.4.b	Processes for managing computerised systems to ensure that they are fit for purpose and used appropriately.
ICH GCP	5.5.3b	When using electronic trial data handling and/or remote electronic trial data systems,the sponsor should: b) Maintains SOPs for using these systems. ADDENDUM The SOPs should cover system setup, installation, and use. The SOPs should describe system validation and functionality testing, data collection and handling, system maintenance, system security measures, change control, data backup, recovery, contingency planning, and decommissioning. The responsibilities of the sponsor, investigator, and other parties with respect to the use of these computerized systems should be clear, and the users should be provided with training in their use.
JPMA EDC Guidance	4.1.1.1c	Operation shall be adequate and compliance shall be ensured by training. (i.e. Prevent from spoofing, stealing password and so on.)
JPMA EDC Guidance	4.1.1.4b	Training record of every related people shall be maintained.
JPMA EDC Supplement	1.5.1.1b	Appropriate training must be provided to ensure appropriate usage and compliance. Since the users of an ePRO system are subjects, it is essential to provide them with understandable manuals and pre-trial trainings using equipment related to the ePRO system in order to collect intended data and improve quality of the trial data. It must be noted that, basic handling procedures of equipment and management of passwords and IDs must be included in the training program. It is also desirable to establish a help desk in advance to minimize loss of data reliability due to missing data that may be caused by device failure, forgotten access codes etc., and subsequent transcription from paper media.
JPMA EDC Supplement	3.2.1d	To establish rules for users to be granted with the authority of electronic signatures, and the timing of authorization and other relevant rules (e.g. after education, training) must be established in advance.
JPMA EDC Supplement	3.2.5	Relevant education and/or training should be provided to all related persons, and recorded.
MHLWCS	6.1.8	The Marketing Authorization holders, etc. should establish a document concerning the operations management of computerized systems. (8) Education and training for persons in charge
MHLWCS	6.8.1	The Operation Manager should have the designated persons create an education and training plan for persons engaged in the activities using the computerized system.
MHLWCS	6.8.3	The Operation Manager should retain the education and training records.
MHRA GXP Data Integrity Guidance	5.1h	Sufficient training in data integrity principles provided to all appropriate staff (including senior management).
NMPA Clinical Trial DM Guide	2.2	Responsible for the management of clinical trial data must go through GCP, relevant laws and regulations, the relevant standard operating procedures (SOP, Standard Operating Procedure), and data management professional training, job requirements to ensure that it has appropriate qualifications.
NMPA Clinical Trial DM Guide	3.3.1.h	Clinical trial data management system validation include the following aspects: - User Training
NMPA Clinical Trial DM Guide	3.3.1.j	Clinical trial data management software end users, the need for local installation and commissioning, testing and training of personnel records.
NMPA Clinical Trial DM Guide	6.1.1.1	All clinical researchers should have qualified and trained. Develop quality control procedures, such as: - Security: clinical researchers have been trained, and in accordance with rights management procedures. - Equipment: clinical researchers follow procedures to ensure safe and proper equipment and data storage. - Data privacy: Ensuring compliance with procedures to protect the privacy of the subjects. - Quality Audit: clinical researchers conducted an internal audit of the data. - Storage and archiving: Ensuring data and files stored in the archive.
NMPA PISS	10.4e	Personal information security professional training and assessment should be carried out on relevant personnel in personal information processing positions on a regular basis (at least once a year) or in the event of major changes in the privacy policy to ensure that relevant personnel are proficient in privacy policies and related procedures.
PMDA Points to Note in CR and PMS	4.C.6.A	A person who has prepared an information and communication device, etc., shall establish a procedure manual and an education and training environment for explaining to those who use the information and communication equipment, etc., to whom information and communication equipment is used to collect information on its effectiveness and safety.
PMDA Points to Note in CR and PMS	4.C.6.A.1	Those who have prepared information and communication equipment, etc., shall prepare to respond appropriately, such as preparing materials for education and training on how to use information and communication equipment, etc., and security risks such as information leakage and unauthorized access to those who use information and communication equipment.
		The person who has prepared the information and communication equipment, etc., shall prepare explanatory materials for the

Copyright eClinical Forum

PMDA Points to Note in CR and PMS	4.C.6.A.2	subjects, etc., that clarify how to use the information and communication equipment, etc. The Investigator shall explain to the Subjects in advance how to use the information and communication devices and the risks associated with the evaluation using the information and communication devices.
PMDA Points to Note in CR and PMS	4.C.6.A.3	In the event that a person who has prepared information and communication equipment, etc. prepares educational and training materials through a company that develops information and communication equipment, etc., the person who prepared the information and communication equipment, etc. is responsible for the education and training materials.
PMDA Points to Note in CR and PMS	4.C.6.A.4	In explaining how to use information and communication devices, etc., to investigators, etc., clinical trial collaborators, and other clinical trial personnel at the conducting medical institution, it is acceptable for the company that developed the information and communication equipment, etc., to intervene as necessary. However, the development company, etc. may not provide explanations to the subjects, etc.
Guidelines for RDC	3.8.1a	Ensure that DHT and Common Computing Platform use training is performed for trial subjects and trial participants based on the Protocol, such as wearing DHT for a specified period of time.
Guidelines for RDC	3.8.3a	Training on proper use of DHT and common computing platforms for trial subjects and trial participants, including training on data collection responsibilities in clinical trials, is critical to proper use of DHT and maintaining data integrity and data quality throughout the duration of the trial. Training records should be retained. Training materials available to participants are replaced by instructions in the official language and will be available to participants upon approval.
Guidelines for RDC	3.8.3b	Training should be provided as appropriate during the trial period for test personnel and test subjects who have difficulty using DHT or general computing platforms.
Guidelines for RDC	3.8.3c	The test commissioner should consider the following as part of the training of test subjects and test personnel: - Set up, activate, and operate DHT and applicable general computing platforms. - Collect data at the correct intervals. - Upload or sync data. - Ensure the security and privacy of data collected by DHT. - Correct wearing of DHT, such as wearing position and wearing period. - DHT properly before and after use. - Share the same DHT and common computing platform with others. - Connect to a wireless network. - Manage known adverse events associated with DHT, such as rash caused by the actigraph wristband. - Handles DHT- related signals, notifications, and errors, including troubleshooting and evaluating unresolved issues. - Ensure that DHT is used correctly, and data is collected, uploaded, or synchronized as planned.
Taiwan Computerized Systems	4.1.c	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.
Taiwan Computerized Systems	5.3	Each individual involved in using a computerized system should be qualified by education, training, and experience to perform their respective task(s). Systems and training should be designed to meet the specific needs of the system users (e.g. sponsor, CRO personnel and investigator). 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 regulation and guidelines for those involved in developing, coding, building, and managing computerized systems, including those employed at a service provider supplying eCRF, IRT, ePRO, trial specific configuration, customization, and management of the system. All training should be documented, and the records retained and available for monitoring, auditing, and inspections.
Taiwan Computerized Systems	6.2.2.b	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.
Taiwan Computerized Systems	8.2.1.1.8	Training should be customized to meet the specific needs of the end users.
Taiwan Computerized Systems	8.3.3	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.

Copyright Clinical Forum

Regulatory mapping for eCF Requirement ID C32

The development, hosting, deployment and change control of a computerised system has objective evidence that system components are traceable to requirements and have been **validated** based on risk, using good **software lifecycle** practices.

Regulation	Paragraph	Description
FDA 21 CFR Part 11	10a	(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.
FDA 21 CFR Part 11	10f	(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.
FDA 21 CFR Part 11	10h	(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.
FDA 21 CFR Part 11	10k	(k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.
FDA 21 CFR Part 11 Q and A	Q6	Regulated entities should ensure that these systems are fit for purpose and implemented in a way that is proportionate to the risks to participant safety and the reliability of trial results.
FDA 21 CFR Part 11 Q and A	Q7a	Validation, including user acceptance testing, is a process to establish and document that the specified requirements of a computerized system can be consistently fulfilled from design until decommissioning of the system or transitioning to a new system. ... Validation should be applied to system functionality, configurations specific to the clinical trial protocol, customizations, data transfers, and interfaces between systems (e.g., interoperability and communication).
FDA CSUCI	A3	The computerized systems should be designed: (1) to satisfy the processes assigned to these systems for use in the specific study protocol (e.g., record data in metric units, blind the study), and (2) to prevent errors in data creation, modification, maintenance, archiving, retrieval, or transmission (e.g., inadvertently unblinding a study).
FDA CSUCI	F5a	The integrity of the data and the integrity of the protocols should be maintained when making changes to the computerized system, such as software upgrades, including security and performance patches, equipment, or component replacement, or new instrumentation.
FDA CSUCI	F5b	The effects of any changes to the system should be evaluated and some should be validated depending on risk. Changes that exceed previously established operational limits or design specifications should be validated. Finally, all changes to the system should be documented.
FDA CSUCI	S03	- System operating manual
FDA CSUCI	S04	- Validation and functionality testing
FDA CSUCI	S06	- System maintenance (including system decommissioning)
FDA CSUCI	S08	- Change control
PMDA EDC Management Sheet version 2	36	Procedure of validating trial-specific setup: Written procedure of validating trial-specific setup
EMA Computerised Systems	4.10	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.
EMA Computerised Systems	4.8.b	The electronic signature functionality in these systems should be proven during system validation to meet the expectations mentioned above.
EMA Computerised Systems	A2.1.a	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.
EMA Computerised	A2.10	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

Copyright eClinical Forum

Systems		details of the protocol amendment if applicable.
EMA Computerised Systems	A2.3	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.
EMA Computerised Systems	A5.2.1.1	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.
EMA Computerised Systems	A5.2.2	The process for emergency unblinding should be tested.
EMA Computerised Systems	A6.1	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. ... As many systems are designed with different configuration options, it should be ensured that the systems are configured in a GCP compliant manner.
EMADCT	6.1	Utilising multiple systems and parties adds complexity and requires an adequate oversight and implementation of adequate measures by the sponsor. To this end, the sponsor should: Ensure that the used data acquisition tools are configured and validated in accordance with their intended use.
EMA eTMF Guideline	3.5.1	Documents demonstrating software validation may be retained by a CRO when the activity has been contracted by the sponsor, but the sponsor should ensure continued access to these documents in the contractual arrangements with the CRO for the required archiving period. Documents relating to the trial-specific software configuration are part of the TMF and it should be determined whether these are maintained/archived by the sponsor or CRO providing this service. Some documents from good manufacturing practice activities should also be defined as part of the TMF, for example, when these relate to the assembly and packaging of the investigational medicinal product (IMP) and confirm, as applicable, compliance with the randomisation schedule and blinding of the trial.
EMA eTMF Guideline	4.1.2h	The eTMF systems should be validated to demonstrate that the functionality is fit for purpose, with formal procedures in place to manage this process.
EMA IRT Reflection Paper	2.2.1	The validation of the IRT system should be in line with the expectations of Annex 11, Volume 4 of Good Manufacturing Practice, and Medicinal Products for Human and Veterinary Use, hereafter called Annex 11. The principles of Good Automated Manufacturing Practice (GAMP) should be considered.
EMA IRT Reflection Paper	2.2.1a	With regards to the validation, as a minimum, the following should be in place: - Regardless of what clinical research activities are undertaken by the IRT, the sponsors should assure themselves that the IRT provider has adequately validated the system. This system should be subject to a robust change control procedure. The expectations would be the same for any in-house system. - A user requirements specification (URS) or equivalent should be produced and approved by the sponsor. Any subsequent validation documents produced by the provider should be mapped back to the URS. This should be down to the level of mapping individual test scripts back to the requirement tested. - Client user acceptance testing (UAT) should always be offered to sponsors. This is an opportunity for the sponsor to test the system and this should be undertaken, preferably with test scripts written by the sponsor. - All incidents affecting functionality should be fixed prior to release and this should be documented appropriately. It is acceptable for some bug fixes to be remedied at a later stage if they do not affect the initial calls into the system, for example an end of study visit (with the exception of early withdrawals); however, it is expected that a plan for fixing such incidents should be in place prior to the system going live. There should be clear traceability of the testing of these fixes right back to the URS. - It is recommended that key steps should be subject to review and sign off by an independent department (QA), which could be at the IRT provider or outsourced. - There should be a formal sign off of the system prior to use.
EMA QA GCP Matters 8	4	- That GCP inspections can take place at the vendor in case the vendor is performing services for the sponsor, when the sponsor has relied fully or partly on the vendor to perform the qualification activities and when it was established during the inspection of the sponsor that part of the documentation can only be verified by inspection of the vendor. - That any qualification documentation prepared by the vendor in relation to the system should be available for inspection.
EMA QA GCP Matters 9	2	Sponsors and vendors should be aware that if the electronic systems are used for generating/handling relevant clinical trial data or to maintain control and oversight of clinical trial processes, documentation regarding the qualification process and any other relevant documentation on the electronic system maintained at the sponsor level, as well as on the vendor level, and it is the sponsor's responsibility to ensure that these documents are available for inspections by Member States GCP inspectors.
EMA RBM in CT	1.3	The key elements of the quality system include:... validation of computerised systems
EMA RBM in CT	1.4	The key elements of the quality system include:... quality assurance including internal and external audits performed by independent auditors
Use of AI in Product	2.3.3.1	Of note, if the use could be of high regulatory impact or high patient risk in a clinical trial, and the method has not been previously qualified by the EMA for the specific context of use, the full model architecture, logs from model development, validation and testing, training data and description of the data processing pipeline would likely be considered parts of the clinical trial data or trial

Copyright ECRF Clinical Forum

Lifecycle		protocol dossier and thus may be requested for comprehensive assessment at the time of market authorisation, clinical trial application or GCP inspection.
Use of AI in Product Lifecycle	2.3.7	...it remains the responsibility of the MAH to validate, monitor and document model performance and include AI/ML operations in the pharmacovigilance system, to mitigate risks related to all algorithms and models used.
Use of AI in Product Lifecycle	2.5.2	For AI/ML, validation refers to the data used to inform on the selection of model architecture and hyperparameter tuning and is hence part of the data driven process. The validation subset can be static or iteratively sampled from the training data using cross-validation. Once this process is completed, the final performance of the model is evaluated once using the hold-out test data set. If test performance is unsatisfactory and further model development is needed, the current test data set cannot be re-used for this purpose and a completely new and independent test dataset is required to repeat the test procedure for an updated model.
Use of AI in Product Lifecycle	2.5.3	It is the responsibility of the sponsor, applicant or MAH to ... keep traceable documentation and development logs to allow secondary assessment of development practices. If a third-party AI model or service is to be used within the medicinal product lifecycle with high regulatory impact or high patient risk, it is expected that the manufacturer of the system has provided such details through a methodology qualification process (see Regulatory interactions) covering the specific context of use.
MHLW ERES (Japan)	3.1	Following items shall be established by electromagnetic records system and its operating procedures. In this case, ensuring the system reliability by computerized system validation of the electromagnetic records system is premised.
EU Annex 11	10	Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure.
EU Annex 11	4.1	The validation documentation and reports should cover the relevant steps of the life cycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment.
EU Annex 11	4.2	Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.
EU Annex 11	4.3	An up to date listing of all relevant systems and their GMP functionality (inventory) should be available. For critical systems an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available.
EU Annex 11	4.4	User Requirements Specifications should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the life-cycle.
EU Annex 11	4.5	The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately.
EU Annex 11	4.6	For the validation of bespoke or customised computerised systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the life-cycle stages of the system.
EU Annex 11	4.7	Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered. Automated testing tools and test environments should have documented assessments for their adequacy.
EU Annex 11	6	For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management.
FDA DHT for RDA in CI	IV.A.2	To select the appropriate DHT for a clinical investigation, the sponsor should identify the minimum technical and performance specifications of the DHT. If applicable, the sponsor should identify a specific product or products (e.g., model and/or version) that meet the minimum technical and performance specifications for a DHT to remain fit-for-purpose.
FDA DHT for RDA in CI	IV.C	Verification and validation activities should consider all relevant functions of the DHT in the context of use in the clinical investigation.
FDA and MHRA Data Integrity Discussions	P11a	The sponsor may choose what validation model to follow; however, all validation documentation (for both the core software and the study-specific configuration) demonstrating that the eSystem is validated should be retained and available for inspection.
FDA and MHRA Data Integrity Discussions	P14b	SOPs should cover the setup, installation, and use of eSystems. The SOPs should also describe eSystem validation and functionality testing, data collection and handling, system maintenance, system security measures, change control, data backup, recovery, contingency planning, and decommissioning.
FDA Mobile Medical Applications	F2	FDA believes all manufacturers of medical device software should have in place an adequate quality management system that helps ensure that their products consistently meet applicable requirements and specifications and can support the software throughout its total life cycle. Adequate quality management systems incorporate appropriate risk management strategies, good design practices, adequate verification and validation, and appropriate methods to correct and prevent risks to patients and adverse events that may arise from the use of the product.
FDA Real World Data	III.Cb	Validation of the electronic systems used to collect registry data
FDA Real World Data	III.Dc	Sponsors should also ensure that software updates to the registry database or additional data sources do not affect the integrity, interoperability, and security of data transmitted to the registry.

Copyright ECFUR Forum

EU GDPR	Article 32.2	In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
EU GDPR	Article 5.1e	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality).
ICH E6 GCP R3 Good Clinical Practice	II.9.2	Systems and processes that aid in data capture, management and analyses, as well as those that help ensure the quality of the information generated from the trial, should be fit for purpose.
ICH E6 GCP R3 Good Clinical Practice	II.9.3	Computerised systems used in clinical trials should be fit for purpose (e.g., through risk-based validation).
ICH E6 GCP R3 Good Clinical Practice	III.3.10.1.1	The sponsor should identify risks that may have a meaningful impact on critical to quality factors prior to trial initiation and throughout trial conduct. Risks should be considered across the processes and systems, including computerised systems, used in the clinical trial (e.g., trial design, participant selection, informed consent process, randomisation, blinding, investigational product administration, data handling and service provider activities).
ICH E6 GCP R3 Good Clinical Practice	III.3.16.1d	The sponsor should ensure that data acquisition tools are fit for purpose and designed to capture the information required by the protocol. They should be validated and ready for use prior to their required use in the trial.
ICH E6 GCP R3 Good Clinical Practice	III.3.16.1xi	Have a record of the important computerised systems used in a clinical trial. This should include the use, functionality, interfaces and validation status of each computerised system, and who is responsible for its management should be described. The record should also include a description of implemented access controls and internal and external security measures.
ICH E6 GCP R3 Good Clinical Practice	III.3.16.1xvi	Assess whether such systems, if identified as containing source records in the trial, (e.g., electronic health records, other record keeping systems for source data collection and investigator site files) are fit for purpose or whether the risks from a known issue(s) can be appropriately mitigated. This assessment should occur during the process of selecting clinical trial sites and should be documented.
ICH E6 GCP R3 Good Clinical Practice	III.3.16.1xvii	In situations where clinical practice computerised systems are being considered for use in clinical trials (e.g., electronic health records or imaging systems used or deployed by the investigator/institution), these systems should be assessed for their fitness for purpose in the context of the trial.
ICH E6 GCP R3 Good Clinical Practice	III.3.16.2f	The sponsor should retain the statistical programming records that relate to the output contained or used in reports of the trial results, including quality control/validation activities performed.
ICH E6 GCP R3 Good Clinical Practice	III.4.3.4a	The responsible party is responsible for the validation status of the system throughout its life cycle.
ICH E6 GCP R3 Good Clinical Practice	III.4.3.4b	Validation should demonstrate that the system conforms to the established requirements for completeness, accuracy and reliability and that its performance is consistent with its intended purpose.
ICH E6 GCP R3 Good Clinical Practice	III.4.3.4c	Systems should be appropriately validated prior to use. Subsequent changes to the system should be validated based on risk and should consider both previously collected and new data in line with change control procedures.
ICH E6 GCP R3 Good Clinical Practice	III.4.3.4e	Both standard system functionality and protocol-specific configurations and customisations, including automated data entry checks and calculations, should be validated. Interfaces between systems should also be defined and validated.
ICH E6 GCP R3 Good Clinical Practice	III.4.3.4f	Where relevant, validation procedures (until decommissioning) should cover the following: system design, system requirement, functionality testing, configuration, release, setup, installation and change control.
ICH E6 GCP R3 Good Clinical Practice	III.4.3.4g	The responsible party should ensure that the computerised systems are validated as fit for purpose for use in the trial, including those developed by other parties. They should ensure that validation documentation is maintained and retained.

Copyright eClinical Forum

ICH E6 GCP R3 Good Clinical Practice	III.4.3.4h	Validation should generally include defining the requirements and specifications for the system and their testing, along with the associated documentation, to ensure the system is fit for purpose for use in the trial.
ICH E6 GCP R3 Good Clinical Practice	III.4.b	Processes for managing computerised systems to ensure that they are fit for purpose and used appropriately.
ICH GCP	1.65	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 trial results.
ICH GCP	5.5.3a	When using electronic trial data handling and/or remote electronic trial data systems,the sponsor should: a) Ensure and document that the electronic data processing system(s) conforms to the sponsors established requirements for completeness, accuracy, reliability, and consistent intended performance (i.e. validation). ADDENDUM The sponsor should base their approach to validation of such systems 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 trial results.
ICH GCP	5.5.3b	When using electronic trial data handling and/or remote electronic trial data systems,the sponsor should: b) Maintains SOPs for using these systems. ADDENDUM The SOPs should cover system setup, installation, and use. The SOPs should describe system validation and functionality testing, data collection and handling, system maintenance, system security measures, change control, data backup, recovery, contingency planning, and decommissioning. The responsibilities of the sponsor, investigator, and other parties with respect to the use of these computerized systems should be clear, and the users should be provided with training in their use.
ICH GCP	5.5.3h	ADDENDUM (h) Ensure the integrity of the data including any data that describe the context, content, and structure. This is particularly important when making changes to the computerized systems, such as software upgrades or migration of data.
JPMA EDC Guidance	4.1.1.6.1	The revised system shall be ensured its quality by CSV in accordance with CSV policy. The revising means followings, - EDC systems version up. (Program change such as functionality addition, modification and elimination to the system, and environment change.) - Revising input form of electronic CRF. (In case of protocol amendments or bug fix.) - Program addition, modification and elimination due to automatically query output.
JPMA EDC Guidance	4.1.1.6.2	In case of data migration due to revising of EDC system, the original data shall be exported directly or converted automatically (which shall be qualified in advance) and keeping their contents and meaning. And also readability of data (including audit trail) is ensured. - Validation deliverables shall be maintained that ensure the data is converted or exported according to the qualified procedures and the data is in consistency with original data.
JPMA EDC Guidance	4.1.1.6.3	In case of revising of related records such as validation deliverables, change control procedures shall be predetermined, and creation or change history of validation deliverables shall be maintained and traceable in chronological order.
JPMA EDC Guidance	4.1.1.6.4	After new EDC system has gone live, if you discard previous EDC system, related records such as validation deliverables shall be maintained and ensure adequacy of all documents produced by previous EDC system.
JPMA EDC Guidance	4.1.3.2.B1	In case of not maintain EDC system after data transfer, necessary records should be maintained. - In case of not maintain EDC system after data transferred to permanent electronic CRF, validation deliverables such as system requirements specification deliverables, design specification deliverables and qualification deliverables are to be maintained for inspection.
JPMA EDC Guidance	4.1.3.2.B2	Readability shall be ensured if the EDC software is migrated for new computer system. - After data transfer, if you intend to preserve EDC software and re-install it in any occasion, readability shall be ensured on the new computer environment.
JPMA EDC Supplement	1.4a	Ensure and document that the electronic data processing systems fulfill the sponsors established requirements for completeness, accuracy, reliability and consistent intended performance (i.e. validation);
JPMA EDC Supplement	1.5.1.5a	Revision of an ePRO system includes upgrading of the system version, modification of the data entry screen, and addition, correction, deletion of programmed automatic queries, etc. In any case, reliability of the system must be ensured through CSV.
JPMA EDC Supplement	1.5.1.5c	Procedures for the revision and change control of validation documents and other documents must also be established in advance, thus enabling a chronological and traceable history of the creation and revision of validation documents and other documents to be retained.
MHLWCS	4.1	The Marketing Authorization Holders, etc. should document a plan for development.
MHLWCS	4.2	The Development Project Manager should document requirements for the computerized system.
MHLWCS	4.4	The Development Project Manager should approve the document created by the supplier on functional specification which describes specific functions and performances ... of the computerized system corresponding to the requirements in the User Requirement Specification.
		The Development Project Manager should approve the document created by the supplier on design specification which describes

Copyright eClinical Forum

MHLWCS	4.5	detailed functions ... of the computerized system based on the Functional Specification.
MHLWCS	4.6	The Development Product Manager should have suppliers produce and test the programs as necessary.
MHLWCS	4.6.1	The supplier should document program specifications ... based on the Design Specification.
MHLWCS	4.6.2	(1) The supplier should document their program testing plan which specifies program testing methods, judging methods and acceptance criteria for program testing results (hereinafter referred to as 'Program Testing Plan'). (2) Based on the Program Testing Plan, the supplier should test programs and keep records.
MHLWCS	4.7	The supplier should perform system test upon the request from the Development Project Manager if necessary.
MHLWCS	4.7.1	Prior to the system test, the supplier should document a system testing plan.
MHLWCS	4.7.2	The supplier should execute the system tests and document its results (including issues arisen during the tests and corrective actions).
MHLWCS	4.8	In order to confirm that all or parts of function and performance of the system meet the User Requirement Specification, the Development Project Manager should have suppliers perform acceptance tests.
MHLWCS	5.1	...the Validation Project Manager should document plans throughout the validation activities.
MHLWCS	5.2	The Validation Project Manager should conduct the Design Qualification to verify that requirements specified in the User Requirement Specification are correctly reflected in the Functional Specification and the Design Specification.
MHLWCS	5.2.3	The Validation Project Manager should document a report of the Design Qualification.
MHLWCS	5.3.1	The Validation Project Manager should document a plan for hardware and software installation qualification.
MHLWCS	5.3.3	The Validation Project Manager should document a report for hardware and software installation qualification.
MHLWCS	5.4.1	The Validation Project Manager should document a plan for the Operational Qualification.
MHLWCS	5.4.3	The Validation Project Manager should document a report for the Operational Qualification.
MHLWCS	5.7	The Validation Project Manager should document an overall reporting throughout the validation stage summarizing results of each qualifications and an overall judgment.
MHRA GXP Data Integrity Guidance	6.19	Computerised systems should comply with regulatory requirements and associated guidance. These should be validated for their intended purpose which requires an understanding of the computerised system's function within a process. For this reason, the acceptance of vendor- supplied validation data in isolation of system configuration and users intended use is not acceptable. In isolation from the intended process or end-user IT infrastructure, vendor testing is likely to be limited to functional verification only and may not fulfil the requirements for performance qualification.
NMPA Clinical Trial DM Guide	3.3.1.a	Reliability refers to a system under specified conditions, within the specified time, the ability to achieve the required functionality. Clinical trial data management system must be based on risk considerations validation to ensure data integrity, security and credibility, and to reduce the problems due to system or process arising from the possibility of error.
NMPA Clinical Trial DM Guide	3.3.1.b	Clinical trial data management system validation include the following aspects: - Proof system to meet the specific purpose of use
NMPA Clinical Trial DM Guide	3.3.1.g	Clinical trial data management system validation include the following aspects: - System maintenance and change control
NMPA Clinical Trial DM Guide	3.3.1.i	Data management software development software manufacturers have their rigorous design, serious verification, and rigorous testing.
NMPA Clinical Trial DM Guide	6.1.1.3	Computer system life cycle process and quality control If using a computer system, must meet the test and let staff needs. In every step of the life cycle of the system are required to perform quality control to ensure that all requirements are documented, tested and met. For example: - Requirements: To ensure system operation and maintenance covers all users as well as technical, commercial and regulatory requirements. - System verification process: ensure compliance with the procedures defined verification and record complete and accurate. - Change control: system life cycle process all changes are subject to evaluation and testing.
NMPA Clinical Trial DM Guide	6.1.1.4	Quality Control of the design, such as CRF design, database design and the establishment of the logical test, are generally multi-process quality control method for use. Process provides product quality control in the production process quality status at every stage to ensure the quality of each stage are reliable.
PMDA Points to Note in CR and PMS	4.2.C.4	Sponsors should ensure that accurate data can be obtained by implementing appropriate quality assurance and quality control. and, if necessary, to be able to present these records at the time of the conformity study.
PMDA Points to Note in CR and PMS	4.C.2	It should be noted that risk assessment is required not only for information and communication equipment used to collect information on efficacy and safety, but also for communication between information and communication equipment, etc., servers that store data, terminals that receive information from servers, and data acquisition processes.
PMDA Points to Note in CR and PMS	4.C.4	Regarding validation and verification of information and communication equipment, etc. the person who prepared the information and communication equipment, etc. may use the results conducted by the company that developed the information and communication equipment, or a third party organization, after confirming its validity.

Copyright eCTIntal Forum

Guidelines for RDC	3.0	The test commissioner should confirm that DHT meets the test purpose, that is, the level of validation of DHT.
Guidelines for RDC	3.1.2	DHT hardware, software, and general computing platforms should be considered to determine whether the DHT is fit for purpose.
Guidelines for RDC	3.1.3	The trial sponsor should ensure that the specific DHT or general computing platform (specify brand, model and / or version) meets the minimum technical and performance specifications. If so, the subject may be allowed to use the self-provided DHT during the clinical trial.
Guidelines for RDC	3.3.5	Usability studies are a critical part of determining the suitability of DHT and / or general computing platforms for a clinical trial plan. Such studies are considered part of the validation process and should include populations similar to the target subjects. Usability studies should test the ability of subjects to use DHT in the future as directed in the trial plan.
Guidelines for RDC	3.8.4	For each DHT and general computing platform used to collect remote data during clinical trials, the trial client should keep records of the time and nature of any updates. Trial sponsors should evaluate all updates to the DHT to ensure that validation and verification studies remain appropriate and do not significantly affect the clinical events or characteristics measured using the DHT. ... Whenever feasible, updates to the planned software or operating system that may modify the way DHT signals are processed / interpreted should be delayed until after the clinical trial is completed, unless there are safety issues.
Taiwan Computerized Systems	4.10	Computerized system used in a clinical trial should be subject to application regulation and is fit for its purpose. System validation should ensure accuracy, reliability and consistent intended performance from the design until the decommissioning of the system or transition to a new system.
Taiwan Computerized Systems	4.6.b	Risks in relation to the use of computerized 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, analyzed, and mitigated or accepted, where justified, throughout the life cycle of the system.
Taiwan Computerized Systems	4.6.e	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.
Taiwan Computerized Systems	6.1.4	Computerized 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.
Taiwan Computerized Systems	8.1.1.a	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 risk assessment.
Taiwan Computerized Systems	8.1.10	There should be a formal change control process. Requests for change should be documented and authorized 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 customizations, the change request should include the details of the protocol amendment if applicable.
Taiwan Computerized Systems	8.2.2.1.1	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.
Taiwan Computerized Systems	8.2.2.2	The process for emergency unblinding should be tested.
Taiwan Computerized Systems	8.3.1	The investigator/institution should have adequate facilities for a clinical trial. This also applies to the computerized 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. ... As many systems are designed with different configuration options, it should be ensured that the systems are configured in a GCP compliant manner.

Copyright BCIRA Forum

Regulatory mapping for eCF Requirement ID C36

There are sufficient system and/or process controls over **data transfers and migrations** from/to systems to ensure the integrity of data, and continued availability of the audit trail.

Regulation	Paragraph	Description
FDA 21 CFR Part 11	30	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.
Japanese APPI	Article 27.2	Regarding personal data to be provided to a third party, if an entity handling personal information decides to stop providing to a third party personal data that can identify the person in question at the request of the person, in accordance with the rules of the Personal Information Protection Commission, the following matters shall be notified to the person in advance or placed in a state where the person can easily know, and when notified to the Personal Information Protection Commission: Notwithstanding the provisions, such personal data may be provided to third parties.
Japanese APPI	Article 28	A business operator handling personal information shall be a foreign country (meaning a country or region outside Japan… Excluding those specified by the rules of the Personal Information Protection Commission as foreign countries that have a system regarding the protection of personal information that is recognized to be at the same level as Japan in terms of protection...) ...a business operator handling personal information is required to take pursuant to the provisions of this Section regarding the handling of personal data... the consent of the person to the effect that the provision to a third party in a foreign country is permitted must be obtained in advance.
Japanese APPI	Article 29	A business operator handling personal information shall transfer personal data to a third party, the date on which the personal data was provided, the name or name of the third party, and other information pursuant to the rules of the Personal Information Protection Commission. A record must be made concerning the matters specified by the rules of the Personal Information Protection Commission.
Japanese APPI	Article 30	When receiving personal data from a third party, a business operator handling personal information must confirm the following matters pursuant to the rules of the Personal Information Protection Commission. (i) the name and address of the third party and, in the case of a corporation, the name of its representative; (ii) Background of acquisition of the personal data by the third party
PMDA EDC Management Sheet version 2	40	Measures for maintaining security: Encryption of the communication between the terminal and server - SSL (Secure Socket Layer) - VPN (Virtual Private Network) - Other ( )
EMA Computerised Systems	4.5.c	The process of data transfer between systems should be validated to ensure the data remain accurate.
EMA Computerised Systems	4.7.a	The sponsor should ensure the traceability of data transformations and derivations during data processing and analysis.
EMA Computerised Systems	6.1.2	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).
EMA Computerised Systems	6.10	Migration as opposed to the transfer of data is the process of permanently moving existing data (including metadata) from one system into another system. It should be ensured that the migration does not adversely affect existing data and metadata.
EMA Computerised Systems	A2.1.c	Interfaces between systems should be clearly defined and validated e.g. transfer of data from one system to another.
EMA Computerised	A5.1.1.2.a	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.

Copyright eClinical Forum

Systems		
EMA Computerised Systems	A5.1.1.2.e	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.
EMA Computerised Systems	A5.1.1.2.f	Important actions should be time-stamped in an unambiguous way.
EMADCT	6.2	Utilising multiple systems and parties adds complexity and requires an adequate oversight and implementation of adequate measures by the sponsor. To this end, the sponsor should: Ensure that when source data captured by a data acquisition tool is transferred to another location and subsequently irreversibly deleted from the data acquisition tool, both the data and the metadata are transferred.
EMADCT	6.3	Utilising multiple systems and parties adds complexity and requires an adequate oversight and implementation of adequate measures by the sponsor. To this end, the sponsor should: Implement measures such as encryption to minimise the risk of unauthorised access, when transferring the data from a data acquisition tool to a server.
EMA eTMF Guideline	4.1.2j	When different TMF systems are linked to facilitate the trial conduct, e.g. when the CRO eTMF system uploads documents into the sponsor eTMF system (possibly by an intermediate system), the process for transferring documents should be robust and should be validated to prevent any loss.
EMA eTMF Guideline	5.4	The use of eTMFs and electronic archiving may require the digitisation of paper documents or the transfer of electronic documents to generate electronic copies of the documents. The process of digitisation or transfer should be validated to ensure that no information is lost or altered.
EMA Q&A eTMF 1	d	The e-TMF system should have validated methods for preventing any changes being made to the TMF documents, this includes the process of transferring from original media to the electronic medium.
EMA Q&A eTMF 1	e	The process for transferring original TMF documents to e-TMF (or other media) should be robust and have been validated to prevent failure of transfer the entire content of the original TMF without loss (i.e. there should be a demonstrable 1:1 mapping between the content of the original TMF and the e-TMF).
MHLW ERES (Japan)	3.1.3.2	When maintained electromagnetic records will be migrated into other electronic storage media or method, migrated electromagnetic records shall be established its authenticity, readability and storability.
MHLW ERES (Japan)	3.3	Using open system Persons who use open systems to create, modify, maintain, retrieve or transmit electromagnetic records shall meet requirements identified in 3.1, additionally shall employ appropriate controls to ensure integrity and confidentiality of electromagnetic records from the point of their creation to the point of their receipt. Such controls shall include such as document encryption and use of appropriate digital signature. Also, persons who use electronic signature shall meet requirements identified in 4.
EU Annex 11	4.8	If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process.
FDA DHT for RDA in CI	IV.A.3	Safeguards should be in place to manage cybersecurity risks, prevent unauthorized access to the DHT and the data it collects, and ensure privacy and security.
FDA DHT for RDA in CI	IV.Ba	The sponsor should also describe the flow of data from the DHT to the first durable electronic data repository.
FDA DHT for RDA in CI	IV.G	When using DHTs to record and transmit data during a clinical investigation, the relevant data captured from the DHT, including all relevant associated metadata, should be securely transferred to and retained in a durable electronic data repository as part of the record of the clinical investigation. FDA regulations include record retention requirements for clinical investigators and sponsors and provide for FDA inspection of certain records relating to a clinical investigation.
FDA DHT for RDA in CI	IV.H.1	The sponsor should: Ensure that data have been transferred from the DHT into a durable electronic data repository.
FDA and MHRA Data Integrity Discussions	P11b	When integrating data in the study database, electronic transfer methods should be used rather than any manual entry via CRFs. Electronic data transfer requires careful controls to ensure no data loss or alteration, the correct data are allocated to correct fields in the new environment, and the fields are compatible (e.g., data type, length, and formats).
FDA Real World Data	III.Cf	Implement and maintain version control by documenting the date, time, and originator of data entered in the registry; performing preventative and/or corrective actions to address changes to the data (including flagging erroneous data without deleting the erroneous data, while inserting the corrected data for subsequent use); and describing reasons for any changes to data without obscuring previous entries
FDA Real World Data	III.Cg	Ensure that data transferred from another data format or system are not altered in the migration process
FDA Real World Data	III.Da	Sponsors should ensure that (1) sufficient testing is conducted to demonstrate interoperability of the linked data systems, (2) the automated electronic transmission of data elements to the registry functions in a consistent and repeatable fashion, and (3) the data are accurately, consistently, and completely transmitted.

Copyright eClinical Forum

FDA Real World Data	III.Db	Documentation of the process sponsors used to validate the transfer of data from an external data source to the registry should be available for FDA to review during sponsor inspections.
EU GDPR	Article 34.3a	Data affected by the personal data breach, in particular those that render data unintelligible such as encryption.
EU GDPR	Article 5.1e	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality).
USA HIPAA	164.502e1i	A covered entity may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.
ICH E6 GCP R3 Good Clinical Practice	III.4.2.5	Validated processes and/or other appropriate processes such as reconciliation should be in place to ensure that electronic data, including relevant metadata, transferred between computerised systems retains its integrity and preserves its confidentiality.
ICH GCP	5.5.3h	ADDENDUM (h) Ensure the integrity of the data including any data that describe the context, content, and structure. This is particularly important when making changes to the computerized systems, such as software upgrades or migration of data.
JPMA EDC Guidance	4.1.1.1h	If sponsor would like to capture certain electronic data in institute via electronic media, sponsor shall make clear the scope of responsibilities of quality assurance provision of transferring electronic data in a contract, and shall ensure its quality by checking of data.
JPMA EDC Guidance	4.1.1.1i	Sponsor shall check compliance of quality management agreement at institutes. - Sponsor shall check quality of provided data.
JPMA EDC Guidance	4.1.1.6.2	In case of data migration due to revising of EDC system, the original data shall be exported directly or converted automatically (which shall be qualified in advance) and keeping their contents and meaning. And also readability of data (including audit trail) is ensured. - Validation deliverables shall be maintained that ensure the data is converted or exported according to the qualified procedures and the data is in consistency with original data.
JPMA EDC Guidance	4.1.3.2.A23	2) Appropriate document format for permanent electronic CRF - Document format can be using throughout the records retention period. (i.e. open format such as PDF, XML, SGML are preferable) - Officially admit document format for long term retention. (i.e. ISO) - Searchable format. 3) Appropriate electronic media for permanent electronic CRF - Enough warranty periods for not data missing throughout the records retention period. - Method for checking quality of data on the electronic media periodically. - Not be able to amend and delete. (i.e. optical disk)
JPMA EDC Guidance	4.1.3.2.B2	Readability shall be ensured if the EDC software is migrated for new computer system. - After data transfer, if you intend to preserve EDC software and re-install it in any occasion, readability shall be ensured on the new computer environment.
JPMA EDC Guidance	4.2	If sponsors get clinical data directly from central laboratories not via institutes, and import them into sponsors server or EDC server, sponsors should have primary responsibility to assure identity of the data and data reported from central laboratories to institutes. In consequence, sponsors need to make measures to assure identity of data reported to institutes and data which sponsor imported directly from central laboratories by contracts with central laboratories. There are some cases that analysis results are included in electronic case report form or not, but in both case authenticity , readability and storability are should be guaranteed...
JPMA EDC Guidance	4.2.1.1.a	Make articles that central laboratories should comply with by contract documents to ensure scope of responsibilities for quality of transferred electronic data and reliability of data. 1. Central laboratories shall assure accuracy of analysis results and ensure that laboratory reports to institutes correspond with electronic data sent to sponsors. 2. Arrange procedures of handling electronic data and scope of responsibilities in central laboratories.
JPMA EDC Guidance	4.2.1.1.c	Create operation in advance procedures for data acceptance/acceptance confirmation, and data import/import confirmation at sponsors side.
JPMA EDC Guidance	4.2.1.1.d	Reliability, repeatability and security should be assured in methods of data import.
JPMA EDC Guidance	4.2.1.1.e	Records should be maintained to make sure that operations of both sponsors and central laboratories are done as procedures
JPMA EDC Guidance	4.2.1.2	Confirm laboratory reports regarding as source documents stored in institutes are correspond with electronic data transferred to sponsors.
JPMA EDC Supplement	1.2a	...it is required to prepare necessary equipment (e.g. devices) and environment (e.g. internet line, telephone line) for data entry by subjects, make operational procedures for transmitting subject data to the operational database, operational procedures for providing the collected subject data to investigators. and sponsors, and also procedures for data retention after completion of the clinical trial and location of storage.
JPMA EDC	1.2g	Encryption or other security methods must be implemented in data transmission to the server via an open system. Since the data stored in the device lacks durability, it is necessary to transfer the data to a durable ePRO server at an early stage, by a verified

Copyright eClinical Forum

Supplement		procedure.
JPMA EDC Supplement	1.5.1.5b	If data migration is needed after the revision of an ePRO system, validation documents must prove that the data conversion or export has been performed through a verified procedure, and the updated data are identical to the source data before the conversion or export.
JPMA EDC Supplement	1.5.4	When an open system is used for the creation, change, maintenance, storage, retrieval and/or transmission of electromagnetic records in an ePRO system, appropriate measures must be taken and added in addition to the requirements indicated from 1.5.1 through 1.5.3, in order to ensure the authenticity and confidentiality of electromagnetic records from their creation to receipt.
JPMA EDC Supplement	2.2	The sponsor must test its transfer and conversion processes of electronic data, and ensure that there are no problems with the operating procedures and data identicalness before and after the transfer or conversion of data.
MHLWCS	6.5.1	The Operation Manager should have the designated persons designated conduct the following activities in accordance with the Operations Management Code, etc.; (1) To backup the software and the data
MHRA GXP Data Integrity Guidance	6.8	Data migration is the process of moving stored data from one durable storage location to another.
NMPA PISS	8.2a	Conduct personal information security impact assessment in advance and take effective measures to protect the subject of personal information based on the assessment results.
NMPA PISS	8.2d	Accurately record and preserve the sharing and transfer of personal information, including the date, size, purpose of sharing, transfer, and basic information of the recipient of the data.
NMPA PISS	8.7	Where personal information collected and generated during the operation of the People's Republic of China is provided overseas, the personal information controller shall conduct safety assessment in accordance with the methods and relevant standards formulated by the State Administration of Credit and the relevant departments of the State Council, and meet the requirements.
PMDA Points to Note in CR and PMS	4.C.3	When collecting data directly from information and communication devices, the sponsor shall ensure reliability by including an audit trail . The audit trail should be available for presentation at the time of the conformity study, if necessary.
Guidelines for RDC	3.6.1	Trial clients should consider network security, which may affect DHT functionality and / or infringe on subject privacy. Therefore, trial clients should ensure that DHT can store and transmit data securely.
Guidelines for RDC	3.7a	DHT to record and transmit data during clinical trials, the relevant data obtained by DHT, including all relevant interpretation data, should be securely transmitted and retained in a durable electronic data repository as part of the clinical trial record.
Taiwan Computerized Systems	4.5.c	The process of data transfer between systems should be validated to ensure the data remain accurate.
Taiwan Computerized Systems	4.7.b	The sponsor should ensure the traceability of data transformations and derivations during data processing and analysis.
Taiwan Computerized Systems	6.1.2	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) by the sponsor.
Taiwan Computerized Systems	6.9	Migration as different from the transfer of data, 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.
Taiwan Computerized Systems	8.1.1.d	Interfaces between systems should be clearly defined and validated e.g. transfer of data from one system to another.
Taiwan Computerized Systems	8.2.1.1.2.a	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.
Taiwan Computerized Systems	8.2.1.1.2.e	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.
Taiwan Computerized Systems	8.2.1.1.2.f	Important actions should be time-stamped in an unambiguous way, e.g. data entries, transfer times and volume (bytes).

Copyright eClinical Forum

Regulatory mapping for eCF Requirement ID C37

When **service providers** are used to provide GxP-related services, **formal agreements** must exist and include clear statements of the roles and responsibilities, management and oversight of the service provider (and their GxP-related providers).

Regulation	Paragraph	Description
FDA 21 CFR Part 11 Q and A	C	When determining the suitability of the IT service and IT service provider, regulated entities should consider the following regarding the IT service provider's ability to ensure the authenticity, integrity, and confidentiality of clinical investigation records and data: - Policies the IT service provider has in place to allow the regulated entity to perform oversight of the clinical investigation activities provided by the IT service provider - Processes and procedures the IT service provider has in place for validation of specific IT services to be used in the clinical investigation - Ability of the IT service provider to generate accurate and complete copies of records and to provide access to data for as long as the records are required to be retained by applicable regulations - Processes and procedures the IT service provider has for data migration, data backup, recovery, contingency plans, and retaining records and making them available for FDA inspection for as long as the records are required to be retained by applicable regulations - Access controls used by the IT service provider for specific IT services used in the clinical investigation, including SOPs for granting and revoking access - Ability to provide secure, computer-generated, time-stamped audit trails of users actions and changes to data - Ability to secure and protect the confidentiality of data at rest and in transit (as appropriate for the content and nature of the record) - Processes and procedures the IT service provider has in place related to electronic signature controls - Relevant experience of the IT service provider
FDA 21 CFR Part 11 Q and A	Q17	The agreements should address services that provide data integrity and data security safeguards, such as participant confidentiality, data reliability, and adherence to applicable regulatory requirements. This should include, but not be limited to, the following: - The scope of the work and IT service being provided. - The roles and responsibilities of the regulated entity and the IT service provider, including those related to quality management. Sponsors are responsible for any regulatory obligations related to the clinical investigation not specifically and lawfully transferred to and assumed by an IT service provider. - A plan that ensures the sponsor will have access to data throughout the regulatory retention period.
FDA 21 CFR Part 11 Q and A	Q17a	FDA recommends that regulated entities have a written agreement (e.g., a master service agreement with an associated service level agreement or quality agreement) with IT service providers that describes how the IT services will meet the regulated entities' requirements.
Japanese APPI	Article 29	A business operator handling personal information shall transfer personal data to a third party, the date on which the personal data was provided, the name or name of the third party, and other information pursuant to the rules of the Personal Information Protection Commission. A record must be made concerning the matters specified by the rules of the Personal Information Protection Commission.
PMDA EDC Management Sheet version 2	25 to 27	Outsourcing contract (Construction/operation of the EDC System, operation of Help Desk, etc.: - Name of vendor/contracted resource - Scope of outsourced services - Date/period of Contract, etc.
EMA Computerised Systems	6.12.b	Where a service provider is involved, this should be addressed in the contractual arrangements.
EMA Computerised Systems	6.8.c	Disaster mitigation and recovery plans should be in place to deal with events that endanger data security. Such plans should be regularly reviewed.
EMA Computerised Systems	A1.a	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 partys oversight of sub-contracted activities should be specified.
EMA Computerised Systems	A2.1.b	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.
EMADCT	2.1	When the sponsor selects a service provider and the investigator is not involved in the contractual arrangement with this service provider, the contract between the sponsor and the investigator should clearly document the contractual arrangements with the service provider if it concerns tasks under investigators responsibility.
EMADCT	2.2	The sponsor should ensure that the contracted service provider is qualified and experienced in the tasks they conduct for the trial.
		The sponsor may choose to outsource duties and functions of the sponsor to a CRO. The sponsor remains responsible for the trial

Copyright eClinical Forum

EMA eTMF Guideline	3.2a	and will need to maintain oversight. Therefore, access to the CRO- maintained part of the sponsor TMF (e.g. by remote access to an eTMF) or at least regular access to relevant documents from it will be necessary to fulfil these responsibilities effectively. In conducting contracted duties and functions, the CRO will be generating documentation that should reside in the TMF. The clinical trial contract/agreement and other documents and procedures agreed between all parties should outline the arrangements for the TMF in some detail.
EMA eTMF Guideline	3.2f	If multiple CROs are involved, the sponsor should clearly define expectations regarding the creation, management, exchange or remote access and retention of documentation amongst CROs. Specific requirements may be put in place when CRO interaction is required. The sponsor should provide CROs access to sponsor essential documents of the TMF that are required by the CRO to execute their delegated duties and functions.
EMA eTMF Guideline	3.3	The investigator/institution may choose to delegate duties and functions related to the conduct of the trial to a third party (e.g. site management organisation or external archive).
EMA eTMF Guideline	3.5.1	Documents demonstrating software validation may be retained by a CRO when the activity has been contracted by the sponsor, but the sponsor should ensure continued access to these documents in the contractual arrangements with the CRO for the required archiving period. Documents relating to the trial-specific software configuration are part of the TMF and it should be determined whether these are maintained/archived by the sponsor or CRO providing this service. Some documents from good manufacturing practice activities should also be defined as part of the TMF, for example, when these relate to the assembly and packaging of the investigational medicinal product (IMP) and confirm, as applicable, compliance with the randomisation schedule and blinding of the trial.
EMA QA GCP Matters 17	1	Any sponsor may delegate, in a written contract, any or all of its tasks to an individual, a company, an institution or an organisation. Such delegation shall be without prejudice to the responsibility of the sponsor, in particular regarding the safety of subjects and the reliability and robustness of the data generated in the clinical trial.
EMA QA GCP Matters 17	2	A sponsor may delegate any or all of his trial-related functions to an individual, a company, an institution or an organisation. However, in such cases, the sponsor shall remain responsible for ensuring that the conduct of the trials and the final data generated by those trials comply with Directive 2001/20/EC as well as this Directive.
EMA QA GCP Matters 17	3	The following points are a non-exhaustive list of measures to consider: - detailed contracts/master-service agreements and work orders
EMA QA GCP Matters 17	4	The sponsor should be able to demonstrate oversight through adequate documentation, including: - ensuring that (direct) access to essential documents that are retained at the contracted service provider can be made available, for example validation/qualification documentation, training documentation, standard operating procedures (SOPs), etc.
EMA QA GCP Matters 17	5	Regardless of delegation of duties and functions (tasks), the complete trial conduct should remain traceable and verifiable. Therefore, the sponsor should ensure that (direct) access to all trial relevant documents can be provided.
EMA QA GCP Matters 8	1	Any trial-related tasks and functions that are delegated to a third party should be specified in a written contract and made clear between the sponsor, third party and when relevant, with the investigator.
EMA QA GCP Matters 8	2	Due diligence should be exercised from the sponsor to ensure that the distribution of tasks is clearly documented and agreed by the vendor, and that each party has the control and access to the data and information that their legal responsibilities require.
EMA QA GCP Matters 8	3	It is sometimes not stated that the sponsor should have access to conduct audits at the vendor site and that the vendor site could be subject to inspections (by national and international authorities) and shall accept these. In addition, it needs to be specified that vendors shall provide necessary documentation (e.g. qualification documentation prepared by the vendor in relation to the system) when requested during a GCP audit or inspection process.
EMA QA GCP Matters 9	3	A sponsor should amend any contract with vendors to ensure availability of qualification documentation.
EU Annex 11	3.1	When third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerised system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT-departments should be considered analogous.
FDA and MHRA Data Integrity Discussions	P12	The contracts should include details on maintaining sponsor access to and management of essential documents and central records (e.g., software validation records) and retaining the data to ensure full dynamic data are available.
EU GDPR	Article 28	Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.
EU GDPR	Article 30	Each controller and, where applicable, the controller representative, shall maintain a record of processing activities under its responsibility.
USA HIPAA	164.504e2iiD	...ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information;

Copyright eCFR Forum

ICH E6 GCP R3 Good Clinical Practice	C.3.1p	Documents that service providers are suitably qualified for conducting their delegated or transferred activities.
ICH E6 GCP R3 Good Clinical Practice	II.10.2	Agreements should clearly define the roles, activities and responsibilities for the clinical trial and be documented appropriately. Where activities have been transferred or delegated to service providers, the responsibility for the conduct of the trial, including quality and integrity of the trial data, resides with the sponsor or investigator, respectively.
ICH E6 GCP R3 Good Clinical Practice	II.10.3	The sponsor or investigator should maintain appropriate oversight of the aforementioned activities.
ICH E6 GCP R3 Good Clinical Practice	III.2.10.2	When the investigator/institution delegates some or all of their activities for investigational product(s) management to a pharmacist or another individual in accordance with local regulatory requirements, the delegated individual should be under the oversight of the investigator/institution.
ICH E6 GCP R3 Good Clinical Practice	III.3.16.1xv	Ensure that there is a process in place for service providers and investigators to inform the sponsor of system defects identified.
ICH E6 GCP R3 Good Clinical Practice	III.3.6.1	Agreements made by the sponsor with the investigator/institution, service providers and any other parties (e.g., independent data monitoring committee (IDMC), adjudication committee) involved with the clinical trial should be documented prior to initiating the activities.
ICH E6 GCP R3 Good Clinical Practice	III.3.6.2	Agreements should be updated when necessary to reflect significant changes in the activities transferred.
ICH E6 GCP R3 Good Clinical Practice	III.3.6.4	Any of the sponsor's trial-related activities that are transferred to and assumed by a service provider should be documented in an agreement.
ICH E6 GCP R3 Good Clinical Practice	III.3.6.9	The sponsor should ensure appropriate oversight of important trial-related activities that are transferred to service providers, including activities further subcontracted by the service provider.
ICH E6 GCP R3 Good Clinical Practice	III.3.9.5	The selection and oversight of investigators and service providers are fundamental features of the oversight process. Oversight by the sponsor includes quality assurance and quality control processes relating to the trial-related activities of investigators and service providers.
ICH GCP	4.2.5	The investigator is responsible for supervising any individual or party to whom the investigator delegates trial-related duties and functions conducted at the trial site.
ICH GCP	4.2.6	If the investigator/institution retains the services of any individual or party to perform trial-related duties and functions, the investigator/institution should ensure this individual or party is qualified to perform those trial-related duties and functions and should implement procedures to ensure the integrity of the trial-related duties and functions performed and any data generated.
ICH GCP	5.2.2	Any trial-related duty and function that is transferred to and assumed by a CRO should be specified in writing. ADDENDUM The sponsor should ensure oversight of any trial-related duties and functions carried out on its behalf, including trial-related duties and functions that are subcontracted to another party by the sponsors contracted CRO(s).
ICH GCP	5.5.3b	When using electronic trial data handling and/or remote electronic trial data systems,the sponsor should: b) Maintains SOPs for using these systems. ADDENDUM The SOPs should cover system setup, installation, and use. The SOPs should describe system validation and functionality testing, data collection and handling, system maintenance, system security measures, change control, data backup, recovery, contingency planning, and decommissioning. The responsibilities of the sponsor, investigator, and other parties with respect to the use of these computerized systems should be clear, and the users should be provided with training in their use.
JPMA EDC Guidance	4.1	Sponsor has the responsibility of ensuring the quality of entrusted business for vendors and CROs.
JPMA EDC Guidance	4.1.1.1h	If sponsor would like to capture certain electronic data in institute via electronic media, sponsor shall make clear the scope of responsibilities of quality assurance provision of transferring electronic data in a contract, and shall ensure its quality by checking of data.
		Make articles that central laboratories should comply with by contract documents to ensure scope of responsibilities for quality of transferred electronic data and reliability of data.

Copyright eClinical Forum

JPMA EDC Guidance	4.2.1.1.a	1. Central laboratories shall assure accuracy of analysis results and ensure that laboratory reports to institutes correspond with electronic data sent to sponsors. 2. Arrange procedures of handling electronic data and scope of responsibilities in central laboratories.
MHRA GXP Data Integrity Guidance	6.20	The responsibilities of the contract giver and acceptor should be defined in a technical agreement or contract. This should ensure timely access to data (including metadata and audit trails) to the data owner and national competent authorities upon request. Contracts with providers should define responsibilities for archiving and continued readability of the data throughout the retention period (see archive).
NMPA Clinical Trial DM Guide	2.1.5	Upon election, the sponsor will be entered into a valid contract with the CRO, required in the contract specifying the responsibilities, rights and interests. Trial sponsors when necessary, conduct relevant training for CRO to ensure that the services provided meet its sponsor quality standards. In clinical trials, data management process, trial sponsors are required to carry out the activities for the CRO immediate and effective management, communication and verification, to ensure compliance with mutually agreed process requirements. The quality management plan sponsor must include CRO quality management information, and must be clear processes and desired outcomes.
NMPA PISS	8.2e	When personal information controllers need to share and transfer, they should pay full attention to risks. Sharing or transferring personal information, other than due to acquisition, merger, or restructuring, shall comply with the following requirements: ... e) bear the corresponding responsibility for damage caused by sharing or transferring personal information to the legitimate rights and interests of the individual's information subject
PMDA Points to Note in CR and PMS	4.C.5.B	As a general rule, in the contract between the person who prepared the information and communication equipment, etc., and the company that developed the information and communication equipment, etc., the secondary use of the data obtained from the clinical trial should be prohibited. If it is not possible to prohibit it, appropriately explain to the Subject, etc., that the data under clinical trial may be used for secondary use for the improvement of information and communication equipment, etc., and obtain consent for the purpose and scope of provision of the secondary use. In addition, the same should be done when the application is installed and used on the information and communication device owned by the subject.
Taiwan Computerized Systems	6.11.b	Where a service provider is involved, this should be addressed in the contractual arrangements.
Taiwan Computerized Systems	6.8.c	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.
Taiwan Computerized Systems	8.1.1.c	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.

Copyright eClinical Forum

Regulatory mapping for eCF Requirement ID C39

Signed electronic records shall contain information associated with the **signing** that clearly indicates all of the following:
- The **name** of the signer
- The **date** and time when the signature was executed
- The **meaning** (such as creation, confirmation or approval)
- Electronic signatures are permanently linked to their respective record
- If the record is subsequently altered, then the signature no longer applies

Regulation	Paragraph	Description
FDA 21 CFR Part 11	50a	(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: (1) The printed name of the signer; (2) The date and time when the signature was executed; and (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.
FDA 21 CFR Part 11	70	Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.
FDA 21 CFR Part 11 Q and A	Ea	In general, electronic signatures and their associated electronic records that meet all applicable requirements under part 11 will be considered to be equivalent to handwritten signatures. Part 11 specifies that signed electronic records must contain the printed name of the signer, the date and time when the signature was executed, and the meaning associated with the signature.
FDA 21 CFR Part 11 Q and A	Eb	In addition, electronic signatures must be linked to the respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.
FDA 21 CFR Part 11 Q and A	Ec	Any changes made to the record, including those subsequent to the electronic signature, must be reflected in the audit trail.
PMDA EDC Management Sheet version 2	83	Information included in the electronic signature: - Name of the signer - Date and time of the signature - Meaning of the signature (authorship, review, approval, etc.)
PMDA EDC Management Sheet version 2	85	Explanation of the signature/record linking:
EMA Computerised Systems	4.8.a	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.
EMA Computerised Systems	4.8.c	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.
EMA Computerised Systems	A5.3.2.a	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.
MHLW ERES (Japan)	4.3	Signed materials by electromagnetic records shall contain information associated with the signing that clearly indicates all of the following: - The printed name of the signer - The date and time when the signature was executed - The meaning (such as creation, confirmation or approval) associated with the signature.
MHLW ERES (Japan)	4.4	Electronic signatures executed to electromagnetic records shall be linked to their respective electromagnetic records to refrain from injustice operation that the signatures cannot be excised, copied, etc. by ordinary means.
EU Annex 11	14	Electronic records may be signed electronically. Electronic signatures are expected to: a. have the same impact as hand-written signatures within the boundaries of the company, b. be permanently linked to their respective record, c. include the time and date that they were applied.
EU Electronic Identification	25	Legal effects of electronic signatures 1. An electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures.

Copyright eClinical Forum

Regulation 910-2014		2. A qualified electronic signature shall have the equivalent legal effect of a handwritten signature. 3. A qualified electronic signature based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic signature in all other Member States.
EU Electronic Identification Regulation 910-2014	26	An advanced electronic signature shall meet the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and (d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.
FDA EHR Guidance	V.C.2.f	Use of electronic signatures for records that are subject to 21 CFR part 11 must comply with relevant requirements in that regulation (see 21 CFR 11.2).
FDA Electronic Informed Consent Q&A	Q6a	In order to be considered equivalent to full handwritten signatures, electronic signatures must comply with all applicable requirements under 21 CFR part 11.
JPMA EDC Guidance	4.1.1.3.6e	The signature (including handwriting signature) and CRF is linked properly.
JPMA EDC Guidance	4.1.1.4c	The EDC system shall clearly specify the signature time, intended data and meaning of signature. And ensure that the signatures cannot be excised or copied. Signed electronic records shall contain information such as signer, the date and time when the signature was executed and meaning of signature.
JPMA EDC Guidance	4.1.1.4d	When using handwriting signature, ensure that the link between intended electronic records and handwriting signature is certainty.
JPMA EDC Guidance	4.1.1.4e	Clearly identified signature time and intended electronic records and if electronic records are modified, electronic signature shall be executed on the modified records.
JPMA EDC Supplement	3.2.3	An electromagnetic record with an electronic signature shall contain explicit information on all of the following items: - First and last name of the signer, - Date and time of when the signature was executed, and - Roles of the signature (e.g. creation, confirmation, approval) The same information must be included in each copy of the eCRF.
MHRA GXP Data Integrity Guidance	6.14	The use of electronic signatures should be appropriately controlled with consideration given to: - How the signature is attributable to an individual. - How the act of 'signing' is recorded within the system so that it cannot be altered or manipulated without invalidating the signature or status of the entry. - How the record of the signature will be associated with the entry made and how this can be verified. - The security of the electronic signature i.e. so that it can only be applied by the 'owner' of that signature.
PRC Electronic Signature Law	13b	Electronic signatures are considered reliable, when all of the following conditions are satisfied: (3) Any alteration made to the electronic signatures after the signing is discernible; (4) Any alteration made to the contents and format of the electronic data is discernible.
PRC Electronic Signature Law	5.2	Data that can guarantee a complete, unaltered status of the contents once they come into being. The completeness of electronic data will not be affected by the adding of endorsements or altered forms that take place in the process of the interchange, preservation, and presentation of the data.
Taiwan Computerized Systems	4.8	Electronic signatures should be in compliance with local regulations.
Taiwan Computerized Systems	8.2.3.2.b	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.

Copyright eClinical Forum

Regulatory mapping for eCF Requirement ID C40

There are sufficient system and/or process controls to ensure the **privacy of subjects**. In the event of a **security incident** that exposes privacy data, the Sponsor and/or Investigator shall notify the relevant Data Protection or other applicable authority.

Regulation	Paragraph	Description
Japanese APPI	Article 26	A business operator handling personal information shall protect personal information as a situation related to the security of personal data such as leakage, loss, damage, etc. of the personal data it handles, which is likely to harm the rights and interests of individuals. When something stipulated by the Commission rules occurs, it must be reported to the Personal Information Protection Commission to that effect as stipulated by the Personal Information Protection Commission rules.
EMA Computerised Systems	4.9	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).
EMA Computerised Systems	A1.c	The sponsor has a legal responsibility under 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.
EMA Computerised Systems	A4.11	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.
FDA DHT for RDA in CI	IV.A.3	Safeguards should be in place to manage cybersecurity risks, prevent unauthorized access to the DHT and the data it collects, and ensure privacy and security.
FDA DHT for RDA in CI	IV.Bb	Sponsors should describe how access to the DHT or the data collected from it is controlled to ensure privacy and security. The description should include methods for access control, when feasible, to ensure that only appropriate individuals are able to use the DHT or enter information.
FDA Electronic Informed Consent Q&A	Q10b	If the entity holding the subjects personal information is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or acting as a business associate of a HIPAA-covered entity, the requirements in the HIPAA Privacy, Security, and Breach Notification Rules apply.
FDA Real World Data	III.Cd	Sponsors also should ensure that a registry adheres to applicable jurisdictional human subject protections requirements, including protecting the privacy of patient health information, when designing a registry or considering use of data from an existing registry.
FDA Real World Data	III.Ce	Sponsors should address whether the registry has privacy and security controls in place to ensure that the confidentiality and security of data are preserved.
EU GDPR	Article 32.2	In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
EU GDPR	Article 33.1	In case of data breach, the controller shall not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority.
EU GDPR	Article 33.5	The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.
USA HIPAA	164.408a	A covered entity shall, following the discovery of a breach of unsecured protected health information ... notify the Secretary.
ICH E6 GCP R3 Good Clinical Practice	II.1.6	The confidentiality of information that could identify participants should be protected in accordance with applicable privacy and data protection requirements.
ICH E6 GCP R3 Good Clinical Practice	II.9.4	Clinical trials should incorporate efficient and robust processes for managing records (including data) to help ensure that record integrity and traceability are maintained and that personal information is protected.
ICH E6 GCP R3 Good Clinical	III.2.12.7	The investigator/institution should implement appropriate measures to protect the privacy and confidentiality of personal information of trial participants in accordance with applicable regulatory requirements on personal data protection.

Copyright eClinical Forum

Practice		
ICH E6 GCP R3 Good Clinical Practice	III.3.16.1a	The sponsor should ensure the integrity and confidentiality of data generated and managed.
ICH E6 GCP R3 Good Clinical Practice	III.4.a	Processes to ensure the protection of the confidentiality of trial participant data.
NMPA PISS	9.2	Notification of safety incidents Requirements for personal information controllers include: a) The relevant information of the incident should be promptly notified to the affected personal information subject by email, letter, telephone, push notification, etc. When it is difficult to inform the personal information subject one by one, it is necessary to adopt a reasonable and effective way to issue warning information related to the public; b) The content of the notice should include but is not limited to: 1) the content and impact of security incidents; 2) Disposal measures taken or to be taken; 3) Advice on the prevention and risk reduction of personal information subjects; 4) Remedial measures provided for the subject of personal information; 5) Contact information of the person in charge of personal information protection and the work organization of personal information protection.
PMDA Points to Note in CR and PMS	4.C.5.A	The investigator shall take measures to connect the investigator or the clinical trial collaborator to the subject, etc., in order to prevent a third party from participating when the investigator or the study collaborator evaluates the efficacy and safety of the drug via a video call system. ... In addition, the investigator and other investigators and clinical trial collaborators should consider the privacy of the subjects, etc., such as making sure that the voice is not leaked and heard by other patients.
PMDA Points to Note in CR and PMS	4.C.5.B	As a general rule, in the contract between the person who prepared the information and communication equipment, etc., and the company that developed the information and communication equipment, etc., the secondary use of the data obtained from the clinical trial should be prohibited. If it is not possible to prohibit it, appropriately explain to the Subject, etc., that the data under clinical trial may be used for secondary use for the improvement of information and communication equipment, etc., and obtain consent for the purpose and scope of provision of the secondary use. In addition, the same should be done when the application is installed and used on the information and communication device owned by the subject.
Taiwan Computerized Systems	4.9	The confidentiality of data that could identify trial participants should be protected, respecting privacy and confidentiality rules in accordance with Personal Data Protection Law.

Copyright eClinical Forum

Regulatory mapping for eCF Requirement ID C41

There is a process to evaluate and mitigate the **risk** and impact **of changes** to the computerised system taking into account changes to protocol (i.e. amendments and addendums), users, & roles on an ongoing basis.

Regulation	Paragraph	Description
FDA CSUCI	F5b	The effects of any changes to the system should be evaluated and some should be validated depending on risk. Changes that exceed previously established operational limits or design specifications should be validated. Finally, all changes to the system should be documented.
FDA CSUCI	S08	- Change control
EMA Computerised Systems	4.6.a	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.
EMA Computerised Systems	4.6.b	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.
EMA Computerised Systems	4.6.e	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.
EMA Computerised Systems	A3.1.c	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.
EMA Computerised Systems	A6.1	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. ... As many systems are designed with different configuration options, it should be ensured that the systems are configured in a GCP compliant manner.
EMA RBM in CT	3d	Risk management tools: can be paper based or built with the use of information technology. The tools can allow detection, identification, prediction, tracking, analysing with the generation of metrics. Broadly the tools support the risk management system and the decision making.
EU Annex 11	1	Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system.
EU Annex 11	10	Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure.
FDA and MHRA Data Integrity Discussions	P10a	A key issue often identified during inspections is that sponsors, CROs, and other third parties do not have adequate controls in place to ensure that the eSystems approved for release in the study (e.g., eCRF, ePRO, and IRT) are consistent with the currently approved protocol (initial or subsequently amended).
FDA Mobile Medical Applications	F2	FDA believes all manufacturers of medical device software should have in place an adequate quality management system that helps ensure that their products consistently meet applicable requirements and specifications and can support the software throughout its total life cycle. Adequate quality management systems incorporate appropriate risk management strategies, good design practices, adequate verification and validation, and appropriate methods to correct and prevent risks to patients and adverse events that may arise from the use of the product.
ICH E6 GCP R3 Good Clinical Practice	III.3.10.1.1	The sponsor should identify risks that may have a meaningful impact on critical to quality factors prior to trial initiation and throughout trial conduct. Risks should be considered across the processes and systems, including computerised systems, used in the clinical trial (e.g., trial design, participant selection, informed consent process, randomisation, blinding, investigational product administration, data handling and service provider activities).
MHLWCS	4.3	The Development Project Manager should conduct the following activities... (2) Risk assessment to assure product quality
MHLWCS	6.1	The Marketing Authorization holders, etc. should establish a document concerning the operations management of computerized systems.

Copyright eClinical Forum

		(6) Change management 2) Impact assessment on changes
PMDA Points to Note in CR and PMS	4.2.C.3	When using commercially available mobile devices and wearable devices, updates by manufacturers to software, operating systems, and algorithms for data processing may affect data collection. In the case of renewal, the sponsor shall evaluate the risk of the update content applicable to the information and communication equipment, etc., and take appropriate measures according to the results of the evaluation and the content thereof.
Taiwan Computerized Systems	4.6.a	Risks should be considered at both the system level e.g. standard operating procedures (SOPs), computerized systems and staff, and for the specific clinical trial e.g. trial specific data and data acquisition tools or trial specific configurations or customizations of systems.
Taiwan Computerized Systems	4.6.b	Risks in relation to the use of computerized 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, analyzed, and mitigated or accepted, where justified, throughout the life cycle of the system.
Taiwan Computerized Systems	4.6.e	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.
Taiwan Computerized Systems	8.3.1	The investigator/institution should have adequate facilities for a clinical trial. This also applies to the computerized 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. ... As many systems are designed with different configuration options, it should be ensured that the systems are configured in a GCP compliant manner.

Copyright eClinical Forum

Regulatory mapping for eCF Requirement ID C43

There is a process to periodically review and affirm the **continued suitability** of the computerised system taking into account the potential cumulative risks and impacts of changes to the system, requirements, version releases and computing environment of the system.

Regulation	Paragraph	Description
FDA 21 CFR Part 11	10a	(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.
FDA 21 CFR Part 11 Q and A	Q7b	Changes to electronic systems (including software upgrades, security and performance patches, equipment or component replacements, and new instrumentation) should be evaluated and validated throughout the life cycle of the system depending on risk.
FDA CSUCI	F5a	The integrity of the data and the integrity of the protocols should be maintained when making changes to the computerized system, such as software upgrades, including security and performance patches, equipment, or component replacement, or new instrumentation.
FDA CSUCI	F5b	The effects of any changes to the system should be evaluated and some should be validated depending on risk. Changes that exceed previously established operational limits or design specifications should be validated. Finally, all changes to the system should be documented.
PMDA EDC Management Sheet version 2	36	Procedure of validating trial-specific setup: Written procedure of validating trial-specific setup
EMA Computerised Systems	A2.9	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.
EMA Computerised Systems	A6.1	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. ... As many systems are designed with different configuration options, it should be ensured that the systems are configured in a GCP compliant manner.
EMA eTMF Guideline	3.2b	The clinical trial contract/agreement and other documents and procedures agreed between all parties should outline the arrangements for the TMF in some detail, such as: - when an eTMF is being used, the details of the system and change control management;
MHLW ERES (Japan)	3.1	Following items shall be established by electromagnetic records system and its operating procedures. In this case, ensuring the system reliability by computerized system validation of the electromagnetic records system is premised.
EU Annex 11	10	Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure.
EU Annex 11	11	Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.
EU Annex 11	4.2	Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.
FDA DHT for RDA in CI	IV.A.2	To select the appropriate DHT for a clinical investigation, the sponsor should identify the minimum technical and performance specifications of the DHT. If applicable, the sponsor should identify a specific product or products (e.g., model and/or version) that meet the minimum technical and performance specifications for a DHT to remain fit-for-purpose.
FDA and MHRA Data Integrity Discussions	P14b	SOPs should cover the setup, installation, and use of eSystems. The SOPs should also describe eSystem validation and functionality testing, data collection and handling, system maintenance, system security measures, change control, data backup, recovery, contingency planning, and decommissioning.
EU GDPR	Article 32.1d	A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
ICH E6 GCP R3 Good Clinical Practice	III.4.3.4d	Periodic review may be appropriate to ensure that computerised systems remain in a validated state throughout the life cycle of the system.

Copyright eClinical Forum

ICH GCP	5.5.3b	When using electronic trial data handling and/or remote electronic trial data systems,the sponsor should: b) Maintains SOPs for using these systems. ADDENDUM The SOPs should cover system setup, installation, and use. The SOPs should describe system validation and functionality testing, data collection and handling, system maintenance, system security measures, change control, data backup, recovery, contingency planning, and decommissioning. The responsibilities of the sponsor, investigator, and other parties with respect to the use of these computerized systems should be clear, and the users should be provided with training in their use.
ICH GCP	5.5.3h	ADDENDUM (h) Ensure the integrity of the data including any data that describe the context, content, and structure. This is particularly important when making changes to the computerized systems, such as software upgrades or migration of data.
JPMA EDC Guidance	4.1.1.6.1	The revised system shall be ensured its quality by CSV in accordance with CSV policy. The revising means followings, - EDC systems version up. (Program change such as functionality addition, modification and elimination to the system, and environment change.) - Revising input form of electronic CRF. (In case of protocol amendments or bug fix.) - Program addition, modification and elimination due to automatically query output.
JPMA EDC Supplement	1.5.1.5a	Revision of an ePRO system includes upgrading of the system version, modification of the data entry screen, and addition, correction, deletion of programmed automatic queries, etc. In any case, reliability of the system must be ensured through CSV.
MHLWCS	6.1	The Marketing Authorization holders, etc. should establish a document concerning the operations management of computerized systems. (6) Change management 2) Impact assessment on changes
MHLWCS	6.6	The Operation Manager should have the designated persons conduct the following operations in accordance with the Operations Management Standard Code; (1) Operation to assess the impact of the change in computerized system and appropriate actions based on its results
MHLWCS	7.1	The Marketing Authorization Holders, etc. should have the designated persons conduct the followings operations... (1) Operation to conduct periodic internal audit in order to verify that the computerized systems are controlled in accordance with this guideline. (2) Operation to report results of the internal audit to the Quality Assurance Manager, Manufacturing Control Manager or Responsible Engineering Manager in written form. (3) Operation to record the results of internal audit and to retain records.
NMPA Clinical Trial DM Guide	6.1.1.3	Computer system life cycle process and quality control If using a computer system, must meet the test and let staff needs. In every step of the life cycle of the system are required to perform quality control to ensure that all requirements are documented, tested and met. For example: - Requirements: To ensure system operation and maintenance covers all users as well as technical, commercial and regulatory requirements. - System verification process: ensure compliance with the procedures defined verification and record complete and accurate. - Change control: system life cycle process all changes are subject to evaluation and testing.
Taiwan Computerized Systems	8.1.9	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.
Taiwan Computerized Systems	8.3.1	The investigator/institution should have adequate facilities for a clinical trial. This also applies to the computerized 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. ... As many systems are designed with different configuration options, it should be ensured that the systems are configured in a GCP compliant manner.

Copyright eClinical Forum

Regulatory mapping for eCF Requirement ID C44

The eTMF **audit trail** shall additionally capture the **accessing** of records.

Regulation	Paragraph	Description
EMA eTMF Guideline	4.1.3f	In this situation there should be procedures and controls in place that demonstrate at all times when versions of documents were made available to the investigator/institution and when these documents were accessed (e.g. through an audit trail) and implemented by the investigator/institution.

Copyright eClinical Forum

Regulatory mapping for eCF Requirement ID C45

There are processes to **address** incidents for the computerised system that identify, assess, resolve, and close: actions, **software anomalies** (bugs), **IT issues**, and **Help desk** issues.

Regulation	Paragraph	Description
EMA IRT Reflection Paper	2.2.1a	With regards to the validation, as a minimum, the following should be in place: - Regardless of what clinical research activities are undertaken by the IRT, the sponsors should assure themselves that the IRT provider has adequately validated the system. This system should be subject to a robust change control procedure. The expectations would be the same for any in-house system. - A user requirements specification (URS) or equivalent should be produced and approved by the sponsor. Any subsequent validation documents produced by the provider should be mapped back to the URS. This should be down to the level of mapping individual test scripts back to the requirement tested. - Client user acceptance testing (UAT) should always be offered to sponsors. This is an opportunity for the sponsor to test the system and this should be undertaken, preferably with test scripts written by the sponsor. - All incidents affecting functionality should be fixed prior to release and this should be documented appropriately. It is acceptable for some bug fixes to be remedied at a later stage if they do not affect the initial calls into the system, for example an end of study visit (with the exception of early withdrawals); however, it is expected that a plan for fixing such incidents should be in place prior to the system going live. There should be clear traceability of the testing of these fixes right back to the URS. - It is recommended that key steps should be subject to review and sign off by an independent department (QA), which could be at the IRT provider or outsourced. - There should be a formal sign off of the system prior to use.
EU Annex 11	4.7	Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered. Automated testing tools and test environments should have documented assessments for their adequacy.
ICH E6 GCP R3 Good Clinical Practice	III.3.16.1xix	Ensure that there is a process in place for service providers and investigator(s)/institution(s) to inform the sponsor of incidents that could potentially constitute a serious noncompliance with the clinical trial protocol, trial procedures, applicable regulatory requirements or GCP.
ICH E6 GCP R3 Good Clinical Practice	III.3.16.1xv	Ensure that there is a process in place for service providers and investigators to inform the sponsor of system defects identified.
ICH E6 GCP R3 Good Clinical Practice	III.4.3.4i	Unresolved issues, if any, should be justified and, where relevant, the risks identified from such issues should be addressed by mitigation strategies prior to and/or during the continued use of the system.
ICH E6 GCP R3 Good Clinical Practice	III.4.3.7a	Where appropriate, there should be mechanisms (e.g., help desk support) in place to document, evaluate and manage issues with the computerised systems (e.g., raised by users), and there should be periodic review of these cumulative issues to identify those that are repeated and/or systemic.
MHLWCS	6.7	The Operation Manager should have the designated persons conduct the following operations in accordance with the Operations Management Standard Code; (1) Operation to assess impact of the deviation (system problem) on quality of the products, to take appropriate measures immediately, to investigate root causes, and to implement necessary actions to prevent recurrence. (2) In case where the computerized system resumes its operations after the deviation (system failure), operation to verify that the recovery process has been executed properly. (3) Operation to record the deviation(system failure) control, to receive confirmation from the Operation Manager, to obtain approvals from the Operation Manager and the manager who is responsible for the deviation management in the whole GMP area, and to retain records.

Copyright eClinical Forum

Regulatory mapping for eCF Requirement ID C46

A detailed diagram and description of the transmission of electronic data (data flow) should be available in the protocol or a protocol-related document.

Regulation	Paragraph	Description
FDA CSUCI	S02	- System setup/installation (including the description and specific use of software, hardware, and physical environment and the relationship)
EMA Computerised Systems	4.7	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.
EMA Computerised Systems	5.1	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.
ICH E6 GCP R3 Good Clinical Practice	III.3.16.1c	The sponsor should pre-specify data to be collected and the method of its collection in the protocol (see Appendix B). Where necessary, additional details, including a data flow diagram, should be contained in a protocol-related document (e.g., a data management plan).
Taiwan Computerized Systems	4.7.a	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.
Taiwan Computerized Systems	5.1	The sponsor should maintain a list of physical and logical locations of the data (e.g., servers), functionality and operational responsibility for computerized systems and databases together with an assessment of their fitness for purposes. When multiple computerized systems / databases are used, a clear overview should be available. System interfaces should be described, defining how the systems interact, including validation status, methods used, and security measures implemented.

Copyright eClinical Forum