TRIAL MASTER FILE
TMF
REFERENCE MODEL

Guidance for the Management of e-Mail Communications in Clinical Studies

Version Date: **31-Jul-2020**

This document is freely distributable

Project Lead

Name	Organization
Jamie Toth	Daiichi Sankyo, Inc.

Lead Authors

Name	Organization
Russell Joyce	Heath Barrowcliff Consulting
Mark Mercer	CGI
Jamie Toth	Daiichi Sankyo, Inc.

Contributors

Name	Organization
Shah Ashraf	Transperfect
Mary Ann Brooks	Baxter Healthcare Corporation
Kathie Clark	Ennov
Dickson D'souza	IQVIA
Cynthia Pinto	GSK
Tiffany Steward	Astellas
LoriAnn Verna	JustInTimeGCP
Jennifer Wilson	Syneos Health

Version History

Version	Steering Committee Approval Date	Changes
1.0	31-Jul-2020	Initial version/new document

Table of Contents

Purpose 5
Filing e-Mails 6
File-As-You-Go vs File Periodically During the Conduct of the Study vs File at Study Closure 6
e-Mail Formats 7
Filing Locations / Classification 7
Filing Responsibility 8
Use of eTMF Mailboxes 9
e-Mail Subject Lines 9
Attachments 9
Embedded links 10
Changes to the Subject Matter of an e-Mail 10
Periodic Review of e-mails 11
Communications Containing Unblinding Information 12
GDPR Implications 12
Document Dates 12
Archiving 13
Regulations, Guidance, and References 14
Appendix 1: e-Mail Repository Options 17
Appendix 2: Preservation Format Options for e-Mail 19
Recommended format for archived records 19
Recommended format for live (active) records 19
Acceptable to regulatory inspectors 19
Potentially acceptable to regulatory inspectors 19
Appendix 3: Definitions 20

Purpose

This guidance is intended to provide recommendations to the life sciences industry on the management of e-mail communications generated throughout the conduct of a clinical study, particularly e-mail communications that enable:

- evaluation of the conduct of the study;
- key decisions made during the study;
- the integrity of the study data; and
- "compliance of the investigator, sponsor and monitor with the standards of Good Clinical Practice and with all applicable regulatory requirements".[1,5,6]

All e-mail communications should be assessed for relevance on a case by case basis. Those determined to be relevant should be retained in the (e)TMF.

If an e-mail is the sole source or evidence of confirmation of an agreement or an approval for processes or for decisions for a particular course of action (e.g. medical advisor approval of subject eligibility), the e-mail should be filed as an essential document in the (e)TMF[1,.3]. An e-mail is relevant if it contains agreements or significant discussions and key decisions[1,5,6] regarding e.g.

1. study administration and conduct;
2. protocol instructions, clarifications, and violations;
3. safety information and reporting;
4. awareness of issues arising during the study, especially exceptional or critical circumstances;
5. study committees or boards and regulatory authorities; or
6. processes or decisions made where there is no SOP or policy to support that process or decision.

Where a vendor is contracted to undertake any of these tasks, the vendor should file and store all associated communications.

An e-mail is not relevant if it is ephemeral, transient, or trivial in nature, not business critical, of only such short-term value, or does not support or contribute to the decision-making process or clinical study outcomes e.g.

1. invitations to meetings;
2. cover transmittals (e.g. 'Please find enclosed…');
3. information for logs or reminding sites to upload information; and
4. duplicate (or extracted) information already held elsewhere in the (e)TMF.

It is important that both sent and received e-mails are filed in the (e)TMF[2] and that the filed e-mail includes (where relevant) the entire e-mail thread[3].

Filing e-Mails

File-As-You-Go vs File Periodically During the Conduct of the Study vs File at Study Closure

EMA guidance requires that "the TMF should have all documentation added in a timely manner during the study."[4]

It is for each organization to define its own approach to the filing of e-mails; this may be to file them

- contemporaneously throughout the duration of the study ("file-as-you-go");
- periodically during the conduct of the study; or
- at study closure.

There are clear benefits to filing e-mails in the (e)TMF as contemporaneously as feasibly possible including (among others) the advantages of

- a centralized, auditable, and inspectable location;
- a well-organized, contextualized repository for all e-mails;
- the application of automated and appropriate access and restriction permissions;
- clarity concerning responsibility for the filing of e-mails;
- communication is not potentially subject to [automated] e-mail client deletion rules;
- contemporaneous capture of e-mails irrespective if future staff changes; and
- improved alignment with regulatory expectations for an up-to-date and inspection ready TMF.

Whichever the approach adopted, organizations will need to establish requisite supporting policies, procedures and resources.

The TMF Reference Model group strongly recommends a "file-as-you-go" strategy to ensure that the TMF is continuously up-to-date and inspection ready at all times. Where this is not in place or not possible, organizations should nonetheless define in the TMF Plan the location of relevant communications in the (e)TMF and periodically perform completeness and quality checks to ensure that relevant communications filed are in scope.

- are readily available[1,7,11];
- are searchable;
- are chronologically ordered[9];
- are correctly titled and indexed;
- are properly filed by zone, section, and artifact;
- record significant discussions, activities and key decisions; and
- are governed by appropriate policies, SOPs, or other formal guidance documents.

Both operationally and during inspection [preparations], these measures will assist search, retrieval, and access to relevant communications.

e-Mail Formats

For legal purposes, it is recommended (where possible) to retain e-mails in their native format (e.g. MSG for Outlook e-mails, EML for Google-mail, Thunderbird etc.) along with all associated metadata to preserve provenance, authenticity, integrity, and evidential value. This holds true for the initial e-mail and for each subsequent response because most e-mail applications allow the responder to modify the preceding message(s) in a thread, including header information e.g. recipient, date, time, subject line. These "after-the-fact" modifications potentially impact on the authenticity and integrity of the e-mail diminishing evidential weight[13, 14].

Header and other information that need to be captured to identify each component of the e-mail and demonstrate provenance and preserve integrity include

- date and time;
- sender and recipient(s);
- subject line field;
- metadata e.g. Size, Route, IP address, ID, Content-Type, MIME-Version, Server Thread etc.;
- message text / content;
- signature block (where applicable); and
- attachments (if relevant).

For regulatory inspection purposes, it is acceptable to retain e-mails in non-native format (e.g. in paper format or PDF format) although caution should be exercised to maintain the integrity of the e-mail as much as possible.

Each organization should determine the filing format(s) acceptable for the retention of e-mails in the eTMF. Not excluding the aforementioned, consideration should also be given to

- the longevity and (re-)usability of the format;
- the preservation and traceability of attachments[3];
- text searchability[11];
- the relationship between the e-mail and associated artifact; and
- validation of the conversion from native to non-native format.

If working with third parties, e-mail format (as well as handling, storage, management, and transfer process) should be agreed in advance and documented in the TMF Plan.

Filing Locations / Classification

Each organization should provide guidance on where to file relevant communications. In certain circumstances, an e-mail may contain information that does not readily align to an artifact or classification and presents difficulty to classify in context of the TMF e.g.

- An e-mail that is the sole source or evidence of confirmation of an agreement or approval for processes or decisions for a particular course of action (e.g. medical advisor approval of subject eligibility); such e-mails should be filed as an essential document[1].

- An e-mail between a Principal Investigator and the sponsor related to the safety of the patient taking the study drug together with a concomitant medication not otherwise specified in the protocol, which could potentially be filed under “safety”, “site management”, or even “protocol deviation” or “protocol amendment”.
- An e-mail containing a Health Authority clinical study application approval, which could be filed under “regulatory” either as “relevant communication” or “regulatory authority decision”.
- Notification of database edit checks that indicate errors in the user interface, which might be filed under “data management” either as “relevant communication” or “edit check testing” unless the database is live and essentially uncovers an issue that should have been detected during UAT, in which case the filing location will differ.

In such circumstances and in the absence of any specific guidance, it is essential to consider the purpose of the e-mail (as it relates to reconstruction of clinical study events) when deciding the most appropriate filing location. Where appropriate, it may be prudent to record the decision to provide requisite documentary evidence and to ensure readily retrieval at the time of audit or inspection.

Regulations do not stipulate the location or format in which relevant communications should be retained only that organizations should take care to ensure that e-mails

- remain complete and legible[7]; and
- can be made available upon request[1,7,11].

Options for retaining relevant communications in a digital format are listed in “Appendix 1: e-Mail Repository Options”.

Filing Responsibility

Organizations should clearly define in the TMF plan the person(s) responsible for filing relevant communications in the (e)TMF to establish a consistent approach; this also includes e-mail communications. Whether defined at zone, section, or artifact level or by other criteria, the person(s) responsible should have ultimate authority for ensuring that e-mails are filed correctly and in a timely manner. It is not recommended to assign responsibility to a central group without ensuring appropriate oversight.

The TMF Reference Model group recommends that relevant communications are filed in the (e)TMF by

- EITHER the originator of the communication (the default procedure);
- OR the primary recipient of the communication if the originator does not have access to the (e)TMF.

Use of eTMF Mailboxes

Some eTMF systems enable e-mails to be filed directly to the eTMF. Where this is the case, it is recommended to develop a validated process to curate e-mails to prevent an overabundance of e-mails in the eTMF, not all of which will be relevant.

e-Mail Subject Lines

Organizations should develop guidance on e-mail subject lines to aid search and retrieval. It is recommended to use unambiguous and meaningful subject lines to clearly identify the subject matter and to ensure the recipient is immediately aware of that subject matter. A concise and focused subject line permits eTMF users and inspectors alike to readily understand the purpose of an e-mail without opening it e.g.

- Temperature Excursion *Study ABC Site 1234*
- ABC Global Labs New Head of Central Laboratory *Protocol XY-2345*
- IRB Decision, Protocol Amendment *Study A-987*
- Data Management Decision on Database Revisions *Study 2020-643*

Where possible, it is best to avoid replication of elements of the "folder path" or metadata in the subject (e.g. study identifier; site number; zone, section, artifact name) unless these are necessary for the recipient to understand the e-mail (e.g. it may be decided to exclude italicized elements in the examples above).

Attachments

If an e-mail contains an attachment that is **already filed** within the eTMF, the e-mail referencing the attachment does not need to be filed again as part of the e-mail. However, if the content of the e-mail message is relevant, file the e-mail including the attachment as a relevant communication:

If an e-mail contains an attachment that **is not filed** within the eTMF, consider the following

1. if the content of the e-mail message is relevant and the attachment is relevant, file the e-mail including the attachment as a relevant communication and file the attachment separately to its relevant artifact;
2. if the content of the e-mail is not relevant but the attachment is relevant, file only the attachment separately to its relevant artifact;
3. if the content of the e-mail message is relevant, but the attachment is not relevant, file the e-mail including the attachment as a relevant communication; and
4. if the content of the e-mail message is not relevant and the attachment is not relevant, there is no need to file either the e-mail or the attachment.

Attachments embedded within the body of an e-mail risk being lost during rendering (e.g. to PDF for archiving purposes) and so should be added as an attachment separately. Attachments should comply

with the requirements agreed in the TMF Plan or the organisation's specific SOP e.g. not password protected and in an acceptable file format.

Embedded links

It is recommended to avoid the use of embedded links in e-mails because of the difficulties of maintaining traceability between the e-mail and contents in the embedded link.

If an e-mail contains embedded links to documentation or web-based resource that **are not filed** within the eTMF, consider the following

1. if the e-mail message contains information that is relevant and the content in the embedded link is relevant, file the e-mail including the embedded link as a relevant communication **and** file the content too (downloaded from the embedded link) separately to its relevant artifact;
2. if the e-mail message contains information that is not relevant, but the embedded link is relevant, file only the content (downloaded from the embedded link) separately to its relevant artifact;
3. if the e-mail message contains information that is relevant but the content in the embedded link is not relevant, file the e-mail including the embedded link as a relevant communication; and
4. if the e-mail message contains information that is not relevant and the content in the embedded link is not relevant, there is no need to file either the e-mail or the content.

Changes to the Subject Matter of an e-Mail

Care should be taken to ensure that e-mails relate to one study only and one subject matter only within that study and that subsequent messages stay "on topic".

Continuous exchanges of e-mails [known as "threads"] between two or more individuals may present problems particularly if

- the subject matter changes;
- relevant attachments or embedded content are included in the thread; and
- the e-mail branches (i.e. differing participants join and leave the thread throughout the duration of the e-mail conversation).

This means that the end point of any e-mail thread will differ dependent on diversification of the subject matter and the participants (see Fig 1).

Care should be taken regarding the management of e-mail threads and attachments to ensure that all relevant information is retained without unnecessary duplication.

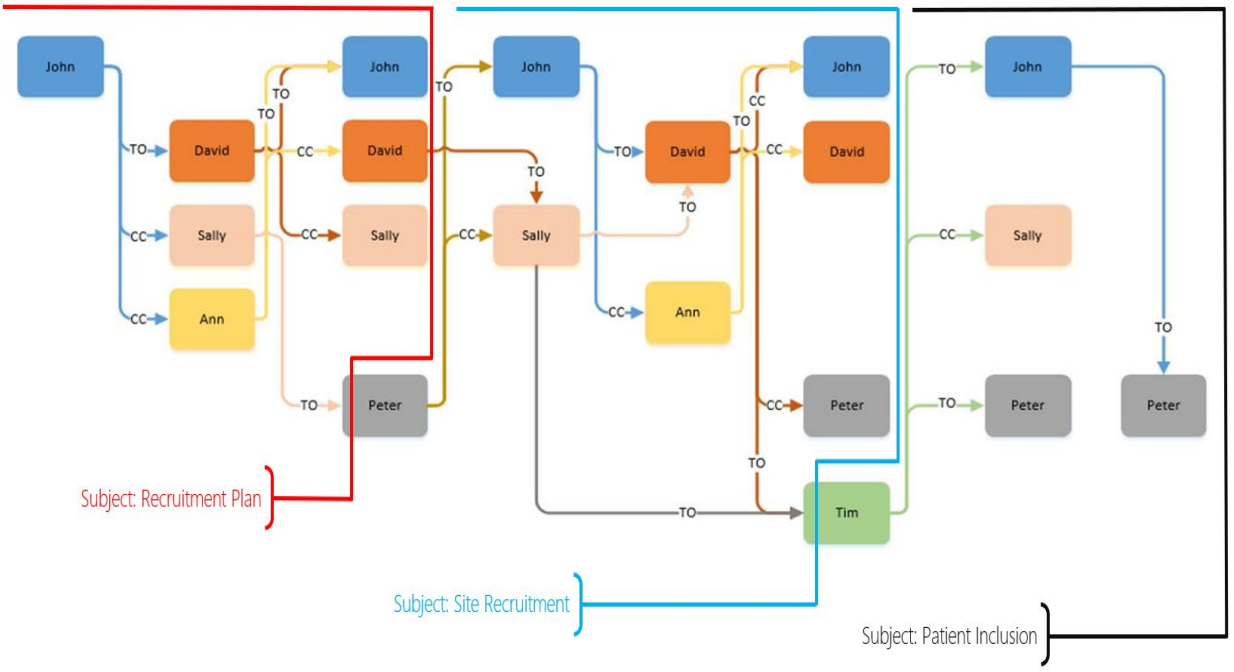

Fig 1: Diversifying e-mail threads

Unless the originating e-mail and each subsequent reply in the e-mail thread are retained individually in real time, it can be difficult and onerous to later track and determine the final e-mail in the thread and any relevant attachments or embedded links that need to be retained. Where necessary, this should be the responsibility of

- EITHER the originator (preferable)
- OR the person designated as responsible in the TMF plan

Where it is necessary to change the subject matter during the course of an e-mail thread, it is recommended to start a new e-mail with a subject line related to the subject matter.

If an e-mail thread has become especially lengthy and complex, it is advisable to resolve the issue in person via a conversation and record the outcome of the discussion in formal meeting minutes, which should be filed in the (e)TMF.

Periodic Review of e-mails

Organizations should establish formal procedures to periodically examine the (e)TMF for the presence of relevant communications. This can be approached in various ways including periodic checks that relevant communications have been filed

- for health authorities, IRBs/IECs etc.;
- in specific zones and sections of the (e)TMF (a low number may be a “red flag”);
- by colleagues assigned responsibility for filing specific classes of e-mail;

- in accordance with guidance (e.g. for attachments); and
- in the correct locations.

Consideration should be given to using the results from these spot checks to

- enhance [third party] oversight;
- introduce necessary process improvements; and
- develop metrics to determine outliers in relation to e-mail filing volume and accuracy and improve TMF inspection readiness.

Communications Containing Unblinding Information

Organizations should develop guidelines on the management of e-mails that contain information (either in the e-mail message or as an attachment) that might potentially unblind a study.

If e-mails containing unblinding information are not filed contemporaneously, a process needs to be established to ensure that they are filed after the blind is lifted and before the (e)TMF is archived.

Any e-mail containing unblinding information should be filed in the (e)TMF with the relevant artifact and access should be strictly controlled and restricted at study, country and site level as applicable. Access to communications containing unblinding information should not be able to be accessed by blinded users until the study blind is lifted. Once the study blind is lifted, appropriate controls must be in place to ensure that audit trails are maintained and a demonstrable and repeatable process in place for when unblinding communications are filed in the (e)TMF.

GDPR Implications

Organizations should develop guidelines and measures to safeguard personally identifiable information that may be contained within e-mails retained in the (e)TMF.

Document Dates

The document date assigned to an e-mail should match the date of the e-mail or (where a thread is filed) the last e-mail in the thread. This is particularly important for ensuring that Health Authorities can view e-mails in date order to reconstruct the study.

Commercially available eTMF systems may often assign dates in the format DD-MMM-YYYY as metadata and permit sorting via those metadata fields.

For e-mail communications filed outside of a commercially available eTMF, it is recommended to file e-mails in chronological order using the following formats:

- YYYY-MM-DD for the date e.g. 2020-10-28 for 28th October 2020; and
- HH-MM for the time format (where required) using the 24-hour clock e.g. 23-16 for 11.16pm.

To organize e-mails in chronological order by subject matter, apply the date (and time if required) as the suffix in the title e.g. Protocol Amendment v4.1 2020-10-28[-23-16].

To organize e-mails in chronological order irrespective of subject matter, apply the date (and time if required) as the prefix in the title e.g. 2020-10-28[-23-16] Protocol Amendment v4.1.

Archiving

If electronic communications are retained in a separate repository, regulations do not stipulate the format in which relevant communications should be archived, only that organizations should take care to ensure that the archive maintains all documents (including relevant e-communications) so that for the duration of the required retention period they

- remain complete and legible period of retention[7];
- can be made available upon request[1,7,11]; and
- are non-modifiable[12].

Once the study is archived, the GCP Archivist[15,16,17] should have custody of relevant communications stored outside of the eTMF and a signpost provided in the TMF index to show the archive location.

Options for archiving relevant e-mails in a digital format are listed in “Appendix 2: Preservation Format Options for e-Mail”.

Regulations, Guidance, and References

EMA/INS/GCP/856758/2018 Good Clinical Practice Inspectors Working Group Guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic)

1. Relevant communication that is necessary for reconstruction of key trial conduct activities and decisions should be retained. […] Electronic communication […] should be readily available and may be retained electronically." [Sec 3.5.3]
2. "It should be ensured that both sent and received communication is filed in the TMF. One or more separate central repository may be used (e.g. for e-mail), as long as they are clearly defined as being part of the TMF." [Sec 3.5.3]
3. "Care should be taken regarding e-mail 'chains' and attachments to ensure that relevant strands of conversations and their associated documents are maintained." [Sec 3.5.3]
4. "the TMF should have all documentation added in a timely manner during the trial" [Sec 3.5.4]

ICH GCP E6(R2)

5. Relevant communications [include] other than site visits: letters; meeting notes; notes of telephone calls" that "document any agreement or significant discussions regarding trial administration, protocol violations, trial conduct, adverse event reporting. [Sec 8.3.11]

MHRA GCP Guide 2012

6. "Communication […] important […] in reconstructing trial conduct, with […] organization s relying on solely on e-mail communication to confirm sponsor approval of processes, documents, and decisions. Only relevant communication that is necessary for the reconstruction of key activities and decisions […] or […] contains other significant information, must be retained." [Sec 10.3.2]
7. "[The archive] must be appropriate to maintain documents such that they remain complete and legible throughout the required period of retention and can be made available upon request" [Sec 10.7.8]
8. "Where data have to be migrated to a new media or to a new format , then the transfer should be validated and fully documented so that it can be subject to audit, to ensure that there has been no loss, change or corruption to the data or metadata and that authenticity is maintained." [Sec 10.7.9]
9. It is recommended that documentation is filed in date sequential order (usually with most recent on top) [Sec 10.2.4]

MHRA Blog 30th Jul 2015

10. "[A] common area [for inspection findings] on documentation is communication associated with key decision making and trial conduct. […] the communication section in the TMF is often very sparse or lacks the relevant communications. […] it's often the case that a number of e-mails can be provided to explain the issue but its unclear why they were not present in the TMF".

MHRA, TMF Q&A (Question 20), ExL Events 7th TMF Summit, London, Oct 2018

11. "…make e-mails available and preferably not in one large non-searchable file dump" (Link)

UK SI 2004/1031 Regulation 31A(9) and 31A(6)

12. "The same controls must be in place for managing the eTMF as for managing paper TMF i.e. controls in terms of security, control over unauthorized edits and access or ease of retrieval of documents."

Regina v Rowe and Bhatt (Canterbury Crown Court Feb 2003)

13. A UK legal case regarding the evidential value of e-mail and in which it was alleged that e-mails and other computer documents relied upon by the prosecution had been forged. For more information see Regina v Rowe and Bhatt.

BS 10008:2014 Evidential Weight and Legal Admissibility of Electronic Information

14. BS 10008:2014 the British Standard that outlines best practice for the implementation and operation of electronic information management systems, including the storage and transfer of information. It
    - helps organizations verify and authenticate information to avoid the legal pitfalls of information storage;
    - outlines best practice for transferring electronic information between systems and migrating paper records to digital files;
    - gives guidelines for managing the availability and accessibility of any records that could be required as legal evidence.

Regulation EU 536/2014

15. The sponsor shall appoint individuals (archivists) within its organisation to be responsible for archives. Access to archives shall be restricted to those individuals. [Article 5)]

EU Directive 2005/28/EC

16. The sponsor shall appoint individuals within its organisation who are responsible for archives […] Access to archives shall be restricted to the named individuals responsible for the archives. [Ch 4, Art 19]

EMA/15975/2016 -Guideline on GCP compliance

17. Withdrawal of essential documents from archives should be under the control of the named individuals responsible for archiving. [, § 6.1 Archiving of the sponsor TMF]

Appendix 1: e-Mail Repository Options

Repository	Details
Native personal e-mail repository	● Communications tool, not a records management application ● Organization ally challenging ● Multiplicity of e-mails across fragmented repositories ● Personal and inconsistent approach to record keeping ● Poor visibility and information sharing ● Exponential costs for legal discovery and legal hold ● Least likely to be readily available upon request
Native shared e-mail repository	● Communications tool, not a records management application ● Resource heavy to manage ● Organization ally challenging ● Complex routing schemes required ● Increased e-mail traffic and multiplicity of forwarded e-mails
Network repository	● Limited records management functionality ● Inconsistent, user-defined structures and organization ● Possible multiplicity of e-mails in fragmented repositories ● Poor security and access models
(Semi-) Automated e-mail archive	● e-Mails held in separate, largely unstructured repositories ● Indexing based not on context or content but on unreliable metadata e.g. keyword search or broad-based generic classification e.g. date received or radio-button classification ● Can present search and retrieval challenges ● Not necessarily readily available ● Limited records management functionality
Integrated eTMF	● Single source repository for all related documents ● Automatic capture of metadata (e.g. to, from, sent date/time) ● Automatic handling of attachments ● Full records management functionality Dependent on eTMF functionality is may also be possible to: ● Drag and drop functionality to file single and multiple e-mails ● Preview files in eTMF while working in e-mail client ● Use e-mail client rules to automatically file e-mails to eTMF

Repository	Details
Bona fide digital archive repository	● Long-term accessibility and readability preserved ● Single source repository for all related documents ● Automatic capture of metadata (e.g. to, from, sent date/time) ● Automatic handling of attachments ● Technology watch functionality to safeguard against obsolescence

Appendix 2: Preservation Format Options for e-Mail

Recommended format for archived records

Preservation Format (i.e. PDF/A and variants)

- The body of the e-mail is converted to PDF/A and stored as the PDF/A file
- Header information is extracted and added to the PDF/A file's XMP metadata
- PDF/A-1 adds any attachments to the end of an e-mail as additional pages
- PDF/A-2 allows attached PDF/A files to be embedded i.e. integrated as PDF/A files

F/A-3 allows any file type to be embedded i.e. integrated into the archive-ready file in both source and PDF/A formats.

Recommended format for live (active) records

Original / native format (e.g. MSG for Outlook, NSF for Lotus Notes, EML for Google Mail, etc.)

- Captures header Preservation Format Options for e-mail metadata
- Preserves provenance and integrity
- Ensures legal admissibility
- Permits re-use

Acceptable to regulatory inspectors

Non-native digital format (e.g. PDF, XML, HTML, RTF, TXT)

- May be possible to retain header metadata, but often only in text format in associated file
- May require certification as a "true copy"
- Acceptable to regulators
- Metadata capture limited
- Will compromise evidential weight
- Does not permit re-use

Potentially acceptable to regulatory inspectors

Print to paper

- May require a process to confirm "true copy" status
- Potentially acceptable to regulators
- Metadata capture limited, if any
- Will compromise evidential weight
- Does not permit re-use

Appendix 3: Definitions

Term	Definition
Archive *(noun)*	The designated physical facility (or technology) and supporting resources necessary for the secure retention, maintenance and retrieval of materials gathered by an organization to preserve the corporate memory.
Archive *(verb)*	The process of submitting records or documents to an archive for long-term retention and preservation.
Attachment	One or more documents affixed to an e-mail message.
Audit Trail	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 and Definitions; Revision 1: March 2018 [Sec 6.13]*
Content	Information in any form contained within a document or within a record keeping system.
Data Integrity	The degree to which data are complete, consistent, accurate, trustworthy, reliable and that these characteristics of the data are maintained throughout the data life cycle. The data should be collected and maintained in a secure manner, so that they are attributable, legible, contemporaneously recorded, original (or a true copy) and accurate. Assuring data integrity requires appropriate quality and risk management systems, including adherence to sound scientific principles and good documentation practices. *[MHRA GXP Data Integrity Guidance and Definitions; Revision 1: March 2018 Sec 6.4]*
Document / Documentation	All records, in any form (including but not limited to written, electronic, magnetic, and optical records, and scans, x-rays, and electrocardiograms) that describe or record the methods, conduct, and/or results of a trial, the factors affecting a trial, and the actions taken. *[ICH GCP E6 (R1) Sec 1.22]*
Embedded Link	A hyperlink link contained within the e-mail communication typically activated by clicking on a highlighted word or icon at a particular location on the screen to take the reader to another location e.g. a file or webpage.
Electronic Record	Information recorded in electronic form that requires a computerised system to access or process.

Term	Definition
e-mail Thread	An e-mail message that includes all preceding replies starting with the original e-mail and enables the reader to follow the e-mail conversation. The replies are usually arranged in reverse chronological order from the original e-mail to the most recent, the topmost e-mail being the most recent reply.
Essential Documents	Documents which individually and collectively permit evaluation of the conduct of a trial and the quality of the data produced. *[ICH GCP E6 (R2) Sec 1.23]*
Filing	The process of saving live (or active) records to a specified repository (e.g. eTMF) for the purposes of enabling re-use of the record and retaining evidence of the conduct of an activity, the decision-making process.
Format	A method by which to encode information in a digital storage medium. File formats enable computer programmes to retrieve, interpret and process digital information. The file format is indicated by the extension affixed as a suffix to the file name e.g. .MSG, .DOC, .XLS, .PDF etc.
Metadata	Data that describe the attributes of other data, and provide context and meaning. Typically, these are data that describe the structure, data elements, inter-relationships and other characteristics of data. It also permits data to be attributable to an individual (or if automatically generated, to the original data source). Metadata forms an integral part of the original record. Without metadata, the data has no meaning. *[MHRA GXP Data Integrity Guidance and Definitions; Revision 1: March 2018 Sec 3]*
Native Format	The format of information in the software application in which it was originally created and saved e.g. .MSG for Outlook e-mails.
Preservation	The suite of ongoing processes and activities applied to electronic information to ensure its long-term accessibility, readability, and (if required) usability. The aim of preservation is to protect records from deterioration resulting from format, software, hardware, and operating system obsolescence. *[HSRAA Guide to Digital Archiving]*
Repository	A [centralised] computer storage application or location in which an aggregation of records is maintained in a logically organized structure e.g. network directory, eTMF.
Subject Matter	The subject line of the e-mail introducing the theme of the ensuing conversation.