General Meeting

11 May 2020
Agenda

- Welcome
- Steering Committee Voting Results
- TMF Reference Model Survey Results
- Impact of MHRA GMP Data Integrity Guidelines
- Upcoming Events
New / Renewed Steering Committee Members

Donna Dorozinsky
President & CEO at Just in Time GCP

Lisa Mulcahy
Owner, Principal Consultant at Mulcahy Consulting, LLC.

Fran Ross
TMF Practice Director at Advanced Clinical

Jamie Marie Toth
Head of TMF Operations at Daiichi Sankyo, Inc.

Todd Tullis
Director of Product Management at Veeva Systems

New ............ and renewed .................................................................
Trial Master File Reference Model

TMF Reference Model Survey Overview

David Ives
Overview of Respondents

307 Respondents

- 58% - US
- 27% - EU
- 8% - Asia Pacific
- 5% - Canada
- 1% - Africa
- 1% - Latin America
- <1% - Middle East

- 55% - Sponsor
- 23% - CRO
- 9% - Vendor
- 8% - Consultant
- 3% - Other
- 1% - Site
Has your organization adopted the Model as is, without any change?

- Yes, adopted as is: 32.4%
- No, adapted with changes: 61.8%
- Other (please specify): 5.9%
There continues to be a trending increase in unique artifacts although the number of respondents within the 201–400 range remains consistent with prior years.
What format is your TMF of record?

- All TMF in paper: 3.5%
- All eTMF: 41.5%
- Combination of paper and eTMF: 54.5%
- Other (please comment): .5%

150% increase in all eTMF operations since the last survey!
How does your organization approach certified copy requirements?

- **We do not have a certified copy procedure**: 40.5%
- **We have a certified copy procedure that applies to any document filed to the TMF that was not created in the TMF**: 30.0%
- **We have a certified copy procedure that applies only when an original is irreversibly replaced**: 29.5%

Approach to certified copies remains quite varied
<table>
<thead>
<tr>
<th>Option</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>We do not retain any draft documents in the TMF</td>
<td>43%</td>
</tr>
<tr>
<td>We would only retain draft documents if the final was missing</td>
<td>7%</td>
</tr>
<tr>
<td>We maintain evidence of change control in other systems e.g. collaboration tools</td>
<td>17%</td>
</tr>
<tr>
<td>Our eTMF is a collaboration tool and maintains drafts of many documents as minor versions</td>
<td>18%</td>
</tr>
<tr>
<td>Our eTMF is a collaboration tool but minor versions are purged once a document is finalized.</td>
<td>7%</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>10%</td>
</tr>
</tbody>
</table>

Still relatively few utilize eTMF for collaboration
Overall what is your organizational view of TMF? (please select the one that most closely aligns)

- It is an end state repository for documents to meet compliance: 25.0%
- It is a project management tool that is used to support efficient and effective study management: 18.0%
- Currently viewed as an end state repository but we are working toward it being project management tool: 32.5%
- It is an active repository but it is not used to support efficient and effective study management: 21.5%
- Other (please specify): 3.0%

Majority still working toward eTMF being supportive of study management
Do you retain paper content scanned into your eTMF?

- Yes, we retain all paper: 16.6%
- Yes, we retain some paper: 45.9%
- No, we do not retain any paper: 24.8%
- Other (please specify): 12.7%

Majority still retaining some paper
The primary reasons listed for not filing blinded records in eTMF was related to not comfortable with risk and system security or workflows.
COVID-19 Impact will continue to accelerate the shift.
Do you require inspectors to complete training prior to issuing credentials?

- Yes: 80.5%
- No: 19.5%
Please share some insight regarding the types of findings you have received following an Audit/Inspection using your eTMF or (select all that apply)

- Not Applicable (no findings or findings not yet received): 22.99%
- Finding regarding TMF Completeness: 55.17%
- Finding regarding TMF Timeliness (i.e. non contemporaneous TMF): 42.53%
- Finding regarding TMF Quality (document content): 22.99%
- Finding regarding eTMF Quality (e.g. metadata or formatting): 22.99%
- Finding regarding eTMF System navigation: 12.64%
- Finding regarding eTMF System access: 3.45%
- Finding regarding eTMF System training: 3.45%
- Finding regarding TMF Filing Structure used: 10.34%
- Finding regarding CRO Oversight: 29.89%
- Other (please comment): 13.79%
Have you undergone a joint inspection with a partner (sponsor/CRO) where both organizations were equally subject of the inspection?

Yes 41.38% (36)

No 58.62% (51)
Is eTMF data or metrics used by your Risk Based Monitoring (RBM) program?

- **19.3%**: Yes, our RBM program uses data / metrics from eTMF
- **24.8%**: Not currently, but will in the future
- **26.6%**: We do not use eTMF data / metrics for RBM
- **27.5%**: We do not have a RBM program
- **1.8%**: Other (please specify)
Do you measure metrics on CRO performance too?

- Yes: 52.3% (56)
- N/A - I am not a sponsor or do not use CROs: 24.3% (26)
- No: 23.4% (25)
Questions?

I LOVE TMF

TMF IS MY FAVORITE
Data Integrity Guidelines – Audit Trails
MHRA and FDA

Lisa Mulcahy, Marie–Christine Poisson, Paul Fenton
Guidances

**MHRA:** March 2018  
- ‘GXP’ Data Integrity Guidance and Definitions  

**FDA:** December 2018  
- Data Integrity and Compliance With Drug CGMP, Questions and Answers – Guidance for Industry  
What is Data Integrity?

- **MHRA**
  
  Data integrity is 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.

- **FDA**
  
  Data integrity refers to the completeness, consistency, and accuracy of data. Complete, consistent, and accurate data should be attributable, legible, contemporaneously recorded, original or a true copy, and accurate (ALCOA). Data integrity is critical throughout the CGMP data life cycle, including in the creation, modification, processing, maintenance, archival, retrieval, transmission, and disposition of data after the record’s retention period ends. System design and controls should enable easy detection of errors, omissions, and aberrant results throughout the data’s life cycle.
What is Data Integrity?

Data Integrity is not about falsifying data / files / records or identifying false data / files / records. It’s not about just the data/ file/record creation

It is about the data / files / records AND also the the metadata and the audit trail associated with the creation, management, movement, of the file/record. For example – transfer of records from one location to another.

“There are many ways that data can become damaged or inaccurate. It can be damaged in transit, as it is transferred over a network or to a storage device. It can become corrupted because a computer's hardware failed. It can become a victim of a poorly configured computing system, such as new software or security programs. It can become a victim of bad agents using malware. Or, it can become damaged as a result of good old human error”

http://bwcio.businessworld.in/article/Understanding-The-Importance-Of-Data-Integrity/10-02-2020-183773/
Audit trail means a secure, computer-generated, time-stamped electronic record that allows for reconstruction of the course of events relating to the creation, modification, or deletion of an electronic record. … Documentation should include change justification for the reprocessing.

Audit trails include those that track creation, modification, (movement) or deletion of data (such as processing parameters and results) and those that track actions at the record or system level (such as attempts to access the system or rename or delete a file).
DI as it Applies to eSystems and Audit Trails

**MHRA**

- **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.
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.
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.

The relevance of data retained in audit trails should be considered by the organisation to permit robust data review/verification. It is not necessary for audit trail review to include every system activity (e.g. user log on/off, keystrokes etc.).
Routine data review should include a documented audit trail review where this is determined by a risk assessment. When designing a system for review of audit trails, this may be limited to those with GXP relevance. Audit trails may be reviewed as a list of relevant data, or by an ‘exception reporting' process. An exception report is a validated search tool that identifies, and documents predetermined ‘abnormal’ data or actions, that require further attention or investigation by the data reviewer.

Reviewers should have sufficient knowledge and system access to review relevant audit trails, raw data and metadata.
How does DI Apply to eTMF Systems and Audit Trails?

Pharma Prospective
- Marie-Christine Poisson-Carvajal
  Head of TMF & Registry Operations

Technology Perspective
- Paul Fenton
  President & CEO of Montrium, Inc.
Standard reports in our eTMF are available to all users and can be run at any time. Reports are generated in Excel format with defined column headers and no merged cells so users can query, sort and filter effectively.

Audit trail and workflow history data is used to produce all Standard Metrics & Reports. Examples include:

- Reason for a placeholder addition to the Study Specific Document List (e.g. wizard, event, manual, automated expiration, etc.)
- Date and time an action was performed and the user who performed the action (e.g. activation, QC rework, deactivation, etc.)
- System entry date
- Type of due date (planned or actual)
- Reason for satisfying a placeholder, sending a document for QC rework and their additional comments
- Location of Document in the system (e.g. group inbox, user inbox, etc.)

Audit trail data (including workflow history) is aggregated together to produce meaningful reports to help manage and monitor a study TMF. Examples include:

- # of documents activated within a specific timeframe
- Total time a document was in a specific workflow task state (e.g. time from receipt in In-Line QC to Activation)
- Median days a group of documents were in a specific workflow task (e.g. median days from draft to activation)
- # of days a task has been in a specific workflow state (e.g. # of days a document has been in QC Rework)
- Includes privileged and system accounts
- User status (active/inactive), system role/privileges (BA, contributor, SO, DS, read only) and date user last accessed PTMF

Ad Hoc reports are run from the database by Business Administrators to perform in-depth analyses of audit trails to investigate potential quality issues and areas of risk detected by standard metrics.

- Some examples: Volume of documents de-activated, number of days placeholders are overdue, usage of artifacts
Challenges for eTMF Solutions

- What data to collect to demonstrate data integrity?
- Who should be able to access this data?
- How should they access it?

Today, systems may not currently capture all data required to demonstrate full chain of custody as this goes beyond the traditional requirements of audit trails.
The Exchange mechanism currently allows the transmission of audit trail information from eTMF systems.

This is currently limited to audit trails as defined by 21 CFR Part 11 and Annex 11 – Creation, Modification, Deletion of records.

Records in TMF systems typically remain static and all actions on an artifact prior to it becoming a record may be recorded in the system but not considered part of the audit trail.

We need to think carefully about what information we should store in the “audit trail” vs “activity log”.
We could expand the use of the `<AUDITEVENT>` tag to capture other actions or transactions that have occurred on an artifact.

We could standardize types of events such as artifact upload, artifact viewed (for blinded documents), artifact moved etc...

Entries could also be prior to an artifact being declared a record.

If standardized it would be easier to transfer data relating to data integrity.
TMF–related events coming up

- VIRTUAL DIA, Washington, June 2020 – a few TMF sessions (No10 year birthday party 😞)
- IQPC TMF Conference Bruges 14–17 Sep
- Exl TMF Summit London 19 – 21 Oct
- AGxP San Antonio, TX – 8–11 November
TMF RM General Meetings

- 22nd June
- Add to your calendar NOW or download the calendar file (.ics file) from our [homepage](#)
- Outlook Meeting Request no longer distributed
QUESTIONS?

Join the TMF Reference Model Discussion Group
https://tmfrefmodel.com/register

- Knowledge sharing
- Networking
- Too Much Fun!

Join the TMF Reference Model Project Team
(but be prepared to work!)
https://tmfrefmodel.groups.io/g/main
Wondering where to find details of the next meeting?

On TMF Reference Model website, click on calendar to see meeting details. Click 'Copy to my calendar' to add to your Outlook / Google calendar.
Meeting details

Wondering where to find details of the next meeting?

On Groups.io, click on Calendar to show group calendar. Click on an event to see dial-in details:

https://tmfrefmodel.groups.io/g/main/