What is a Risk Based approach for Audit Trail Review?

Do the guidances allow for a risk based approach?
Agenda

- Data Integrity focuses on the electronic systems
  - And the technical controls they provide
- Data Integrity Guidances:
  - what do they say about Audit Trails?
- Electronic dynamic data review vs static report review
- Periodic Review
- Applying a risk based approach or 100% review
Gathering & Sharing Regulatory Information

Regulatory Bodies
FDA/MHRA etc

Industry Groups
ISPE/GAMP

Customer QA

Sales and Specialists

Professional Services

Product Functionality and Design
Disclaimer

- This presentation is for informational purposes only and should not be taken as advice regarding any particular course of action to be followed.
- Waters does not make any representations or warranties, express or implied, to any party, regarding use of the information contained in this presentation to make decisions regarding the implementation and maintenance of effective quality control systems and quality assurance testing programs, including but not limited to the applicable Good Manufacturing Regulations that apply to the manufacture of regulated products.
**integrity**

/ɪnˈtɛgrɪti/

1. the quality of being honest and having strong moral principles.

   *synonyms:* honesty, uprightness, probity, rectitude, honour, honourableness, upstandingness, good character, principle(s), ethics, morals, righteousness, morality, nobility, high-mindedness, right-mindedness, noble-mindedness, virtue, decency, fairness, scrupulousness, sincerity, truthfulness, trustworthiness

   *antonyms:* dishonesty

2. the state of being whole and undivided.

   *synonyms:* unity, unification, wholeness, coherence, cohesion, undividedness, togetherness, solidarity, coalition

---

**Awareness**

**Audit Trail**

**Interfacing**

**Compliance**

**Data Quality**

**Regulations**
What is Data Integrity?
Why the new focus on Data Integrity?

Data integrity is not a new problem, more control / documentation can be implemented with computerized systems.

### Paper Documents vs. Computerized Systems

<table>
<thead>
<tr>
<th>Paper Documents</th>
<th>Computerized Systems</th>
<th>Improvements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notebooks are issued to users</td>
<td>User accounts issued to users</td>
<td>Computerized systems can have access controls</td>
</tr>
<tr>
<td>Bound notebooks with preprinted pages</td>
<td>Authentication, maintain raw data</td>
<td>Authentication provides increased assurance actions are performed by that user, raw data cannot be over written</td>
</tr>
<tr>
<td>Stamps with automatic data/time</td>
<td>System Generated Audit Trails</td>
<td>System control: for ALCOA (no back dating)</td>
</tr>
<tr>
<td>Initial, date, and user correction comments</td>
<td>System Generated Audit Trails</td>
<td>System control: for ALCOA (user/date associated to action cannot be altered)</td>
</tr>
<tr>
<td>Reviewed to ensure complete and accurate</td>
<td>Metadata is available for review</td>
<td>Review includes metadata</td>
</tr>
<tr>
<td>Handwritten signatures</td>
<td>Electronic Signatures</td>
<td>System control: for ALCOA (no back dating)</td>
</tr>
<tr>
<td>Archival of Data in climate controlled warehouse</td>
<td>Electronic archival</td>
<td>Information can be archived restored and reviewed quickly</td>
</tr>
<tr>
<td>Disaster Recovery is PDF of records</td>
<td>Redundant copies of original data and metadata</td>
<td>Data and metadata is available, complete accurate information</td>
</tr>
</tbody>
</table>
Why the New Focus on Data Integrity?

Electronic Systems Improve Traceability

Provide the **controls to prevent** but also **capability to detect** undesirable users actions

- Tools for QA and regulators
  - Access levels
  - System polices
  - Audit Trails

**Agencies have lost the trust that analysts behave with honesty and integrity**
Inspection Themes

CSV

Technical Controls

Procedural Controls

No Validation or Change Control

Delete Privileges

Unsecured Data

Sharing Accounts

DATA MANIPULATION

No Audit Trail

Poor Review of Electronic Data including audit trails

All Data: Good and Bad

Poor OOS or Lab Error Investigations

©2016 Waters Corporation
Data Integrity Guidances

**U.S. FOOD & DRUG ADMINISTRATION**

*Updated in 2015, DRAFT April 2016*

**PIC/S**

*Pharmaceutical Inspection Co-Operation Scheme*

*PI-041-1 (DRAFT 2), August 2016*

**EUROPEAN MEDICINES AGENCY**

*August 2016*

**OECD**

*For GLP, April 2016*

**MHRA**

*Medicines & Healthcare Products Regulatory Agency (UK)*

*GMP Data Integrity, March 2015*

*GxP Data Integrity, DRAFT July 2016*

**World Health Organization**

*Released June 2016, As WHO_TRS_996 Annex 5*

**PDA**

*Parenteral Drug Association*

*March 2016*

**ISPE**

*Coming soon*
Annex 11 Audit Trails

9. **Audit Trails**

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.*

- Audit trails tell us WHO did WHAT, WHEN automatically
- Audit trails tell us WHY as defined by the user
- They have two primary purposes:
  - Give a history to the data, to help decide if it can be trusted
  - They should deter wrongdoing (think of CCTV)
    - Without review, they are not a deterrent
**Annex 11 and NIST: Review of Audit Trails**

- **Audit trails** need to be available and convertible to a generally intelligible form and **regularly reviewed**. (A11 § 9)

- From a NIST publication*
  - Audit trails are a technical mechanism that **help managers maintain individual accountability**. ..Users are less likely to attempt to circumvent security policy if they know that their actions will be recorded in an audit log.
  - “Determine how much review of audit trail records is necessary”

* Introduction to Computer Security: The NIST Handbook
**Question 7: How often should audit trails be reviewed?**
- reviewed with each record and before final approval of the record.
- BUT: does not apply to all audit trails??
  - include, but are not limited to, the following:
    - the change history of finished product test results,
    - changes to sample run sequences,
    - changes to sample identification,
    - changes to critical process parameters. (not “processing” parameters)
- routine scheduled audit trail review based on the complexity of the system and its intended use.

**Question 8: By WHOM?**
- Personnel responsible for Record Review
MHRA draft GxP Guidance: Audit Trail Review SUMMARY

- From March 2015 GMP
  - It should be possible to associate all changes to data with the persons making those changes, and changes should be time stamped and a reason given.
  - Users should not have the ability to amend or switch off the audit trail.

- A paper based audit trail to demonstrate changes to data will be permitted. Where they achieve equivalence to integrated audit trail, or replace by end 2017.

- Not necessary for audit trail review to include every system activity.
As such, manufacturers and analytical laboratories are **not expected to implement a forensic approach to data checking on a routine basis**, but instead design and operate a system which provides an acceptable state of control based on the data integrity risk, and which is fully documented with supporting rationale.

**Routine data review** should include a **documented audit trail review**
- Could be through an exception report..abnormal **data which requires further attention or investigation**

**QA should have sufficient knowledge...to review relevant audit trails, raw data and metadata as part of audits**
WHO Guidance: Audit Trail Review Summary

- ...may include discrete event logs, history files, database queries or reports

- Regular review of audit trails may reveal incorrect processing of data and help prevent incorrect results from being reported and identify the need for additional training of personnel;

- key personnel, ..should be trained in measures to prevent and detect data issues.
  - This may require specific training in evaluating the configuration settings and reviewing electronic data and metadata, such as audit trails, for individual computerized systems

- All GxP records held by the GxP organization are subject to inspection by health authorities. This includes original electronic data and metadata, such as audit trails.
WHO Guidance: Audit Trail Review Summary

- Risk based...frequency roles, responsibility and approach
  - *periodic review* of audit trails that track system maintenance activities,
  - ...audit trails that track changes to critical GxP data...would be expected to be reviewed *each and every time the associated data set is being reviewed and approved* – and prior to decision-making.

- Data review should be documented.
  - For electronic records, this is *typically signified by electronically signing the electronic data set that has been reviewed and approved*.

I sign this data to attest that I performed/ reviewed / approved this data according to SOP 12345
New expectation for Audit Trails

Audit trails records should be in an intelligible form and have at least the following information:

- Name of the person who made the change to the data;
- Description of the change;
- Time and date of the change;
- Justification for the change;
- Name of any person authorising the change.

Where data summaries are used for internal or external reporting, evidence should be available to demonstrate that such summaries have been verified in accordance with raw data.
Review of Audit Trails

- Review audit trails as part of data review process
  - Find anomalies before batch release
  - Focus of user behaviour that affect results
  - Peer Review / Manager review / QA review?

- Periodic Review of overall/system level audit trails
  - System level activity without correct documentation, change control, testing or approval
    - Eg. changing system policies, user access or deletion of data

- Inspectors **WILL** look at the audit trails in electronic data systems

**Biggest Issue:** Audit trails are often more a log of all activity (to comply) and not designed for easy review
## Review of Audit Trails

### Print Audit Trails

- Include data relevant audit trails in regular reports
- Periodically print out System level audit trails to “review”
- Sign reports as “evidence” of review

### Review Audit Trails Electronically

- Use the tools (if any) built into the CDS
- Review as PART of the data/integration/method review
- Write a clear SOP defining which audit trails to review and when
  - Only flagged or suspicious results?
- Signing results includes declaration of electronic review
Adding audit trails to reports

<table>
<thead>
<tr>
<th>SampleName</th>
<th>Sample Set Id</th>
<th>Instrument Method Id</th>
<th>Processing Method Id</th>
<th>Altered</th>
<th>Processing Locked</th>
<th>Result #</th>
<th># of Results Stored</th>
<th>Integration</th>
<th>Result Codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diluent</td>
<td>1098</td>
<td>1100</td>
<td>1394</td>
<td>Yes</td>
<td>False</td>
<td>1</td>
<td>1</td>
<td>Auto Integration</td>
<td>109 Q49</td>
</tr>
<tr>
<td>Assay Standard</td>
<td>1098</td>
<td>1100</td>
<td>1394</td>
<td>Yes</td>
<td>False</td>
<td>2</td>
<td>2</td>
<td>Auto Integration</td>
<td>109 Q49</td>
</tr>
<tr>
<td>Assay Standard</td>
<td>1098</td>
<td>1100</td>
<td>1394</td>
<td>Yes</td>
<td>False</td>
<td>2</td>
<td>2</td>
<td>Auto Integration</td>
<td>109 Q49</td>
</tr>
<tr>
<td>Assay Standard</td>
<td>1098</td>
<td>1100</td>
<td>1394</td>
<td>Yes</td>
<td>False</td>
<td>2</td>
<td>2</td>
<td>Auto Integration</td>
<td>109 Q49</td>
</tr>
<tr>
<td>Assay Standard</td>
<td>1098</td>
<td>1100</td>
<td>1394</td>
<td>Yes</td>
<td>False</td>
<td>2</td>
<td>2</td>
<td>Auto Integration</td>
<td>109 Q49</td>
</tr>
<tr>
<td>Assay Standard</td>
<td>1098</td>
<td>1100</td>
<td>1394</td>
<td>Yes</td>
<td>False</td>
<td>3</td>
<td>3</td>
<td>Manual Integration</td>
<td>109 Q49</td>
</tr>
<tr>
<td>Assay Standard</td>
<td>1098</td>
<td>1100</td>
<td>1394</td>
<td>Yes</td>
<td>False</td>
<td>2</td>
<td>2</td>
<td>Manual Integration</td>
<td>109 Q49</td>
</tr>
<tr>
<td>Assay Sample</td>
<td>1098</td>
<td>1100</td>
<td>1394</td>
<td>Yes</td>
<td>False</td>
<td>1</td>
<td>1</td>
<td>Manual Integration</td>
<td>109 Q49</td>
</tr>
<tr>
<td>Assay Sample</td>
<td>1098</td>
<td>1100</td>
<td>1394</td>
<td>Yes</td>
<td>False</td>
<td>1</td>
<td>2</td>
<td>Manual Integration</td>
<td>109 Q49</td>
</tr>
<tr>
<td>Assay Sample</td>
<td>1098</td>
<td>1100</td>
<td>1580</td>
<td>Yes</td>
<td>False</td>
<td>2</td>
<td>2</td>
<td>Manual Integration</td>
<td>109 Q49</td>
</tr>
</tbody>
</table>

Sample History
User: System Date: 8/15/2011 7:17:54 PM IST  Reason: save
  Modified Vial(SampleName): Gemfibrozil Sample -> Assay Sample
User: System Date: 7/17/2014 6:03:25 PM IST  Reason: for demo
  Modified Vial(Batch_Number): <No Value> -> 1
  Modified Vial(Batch_Number1): <No Value> -> 1
  Modified Vial(Column_ID): <No Value> -> 1
  Modified Vial(Column_ID1): <No Value> -> QC/LC/001
  Modified Vial(Molecular_Wt1): <No Value> -> 1.000
  Modified Vial(Molecular_Wt2): <No Value> -> 1.000
  Modified Vial(SampleWeight): 1.00000 -> 50.00000
Empower Traceability

- Original Processing Method
- Sample Sets
- Standards Used for Calibration
- Calibration Curves
- Original Instrument Method
- eCord Information
- LC/GC System Used
- Sample History
- Product Code/Stage Reagent LIMS ID
- Traceable Chain of Custody
- Unchanged Raw Data File

©2016 Waters Corporation
Result Audit Viewer Tool

One Stop Solution:
- Project Audit Trails
- Method History and Differences
- Sample History
- Sample Set History
- Acquisition Log /Injection Log
Audit Trails VS Message Center

- Audit Trails are designed to record changes to records by Humans:
  - Who changed what, when and WHY
  - Critical to record authorised or unauthorised changes

- Message Center in Empower a (and other CDS?):
  - NOT AN AUDIT TRAIL
    - Instrument/System messages from either the instrument or the software
    - Very useful for troubleshooting: ‘What’ happened ‘when’
    - Missing “who” and no “why”

- Acquisition and Injection Logs in Empower:
  - Are part of Audit Trail
    - Record human initiated changes to instrument parameters during run
    - Are permanently tied to the channel/chromatogram
    - Viewable in Reports or Result Audit Viewer
## Acquisition Log

### Details

1. **Details:** System: Alliance with 2487  Method: Test  Channel: 2487Channel1  Calibration ID: 1934  Calibration Source: Auto
2. **Details:** Result Set: Sample Set 1  Sample Set Method: SS 1  Method: Test  Processed How: Processing Method  Result Set ID: 1033  Sample Set ID: 1022
3. **Details:** Method: Test  Type: Processing  Version: 1
4. **Version:** 1  **9/21/2016 11:10:28 AM EDT**  User System
5. **Acquired By:** System  Injection: 1  **Date Acquired:** 9/21/2016 11:01:37 AM EDT  **Run Time:** 3.50  **Acq Method Set:** test  **Injection Volume:** 5.00  **Barcode / BCD:** Auto Additions: Injection Id: 1024
6. **User changed flows to:** 1.10 (%A 40.0 %B 60.0 %C 0.0 %D 0.0) and limits to: Low 0.00, High 4000.00 at 0.95 minutes
7. **User changed flows to:** 1.10 (%A 40.0 %B 60.0 %C 0.0 %D 0.0) and limits to: Low 0.00, High 4000.00 at 0.95 minutes

### Acquisition Log

<table>
<thead>
<tr>
<th>Date</th>
<th>Action Type</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/21/2016 11:17:30 AM EDT</td>
<td>Created Calibration</td>
<td>Audit Trail Record</td>
</tr>
<tr>
<td>9/21/2016 11:17:30 AM EDT</td>
<td>Created Result Set</td>
<td>Audit Trail Record</td>
</tr>
<tr>
<td>9/21/2016 11:10:28 AM EDT</td>
<td>Created Method</td>
<td>Audit Trail Record</td>
</tr>
<tr>
<td>9/21/2016 11:10:28 AM EDT</td>
<td>N/A</td>
<td>Processing Method Properties</td>
</tr>
<tr>
<td>9/21/2016 11:01:37 AM EDT</td>
<td>N/A</td>
<td>Acquisition Log</td>
</tr>
<tr>
<td>9/21/2016 11:01:37 AM EDT</td>
<td>N/A</td>
<td>Injection Log</td>
</tr>
<tr>
<td>9/21/2016 11:01:37 AM EDT</td>
<td>N/A</td>
<td>Injection Log</td>
</tr>
</tbody>
</table>

**Acquired By:** System  
**Injection:** 1  
**Date Acquired:** 9/21/2016 11:01:37 AM EDT  
**Run Time:** 3.50 (Minutes)  
**Acq Method Set:** test  
**Injection Volume:** 5.00 (uL)  
**Barcode / BCD:** Auto Additions:  
**Injection Id:** 1024  
**Instrument Method Id:** 1018  
**Instrument Method Name:** test  
**Superseded:** No  
**# of Process Only Sample Sets:** 0  
**eCod Name:**  
**eCod Serial Number:**  
**eCod Injection Count (Lifetime to Date):**  
**eCod Sample Count (Lifetime to Date):**  
**eCod Maximum Pressure (Lifetime to Date):** (psi)  
**eCod Maximum Temperature (Lifetime to Date):** (°C)  
**Use Syringe Settings:**  
**Syringe Size A (uL):**  
**Nanoliter Adapter A:**  
**Syringe Size B (uL):**  
**Nanoliter Adapter B:**  
**User changed flows to:** 1.10 (%A 40.0 %B 60.0 %C 0.0 %D 0.0) and limits to: Low 0.00, High 4000.00 at 0.95 minutes  
**User changed flows to:** 1.10 (%A 40.0 %B 60.0 %C 0.0 %D 0.0) and limits to: Low 0.00, High 4000.00 at 0.95 minutes
How to document Data Review including Audit Trails

- Review chromatograms, methods and relevant Audit Trails in Empower application
- Document that process by SIGNATURE: WHO Guidance
  - Sign a report to document that you have followed the review SOP

I sign this data to attest that I performed/ reviewed / approved this data according to SOP 12345

SOP should document what to review (including manual entries) and how it should be done by your role

- Similar to other laboratory tasks where there is no proof of the activity (such as making mobile phases or sample preparation) other than a user attesting to their completion of the task
Reviewing and Signing all Results.. Even rejected results?

Right click > Report Viewer
Data Review SOP suggestions

- Should be performed on ELECTRONIC data in the application at least at Peer Review level
  - Not relying on paper /pdf or Empower reports entirely
- Define a Process
- Look at final results (summaries, averages, CofA)
  - Work back through the data from final quantitation, to areas and integration to SampleSet meta data to audit trails
- Specifically focus on suspect data
  - Define a list of warning signs..
    - Manual integration / multiple results / metadata changes
    - Results that only just meet specification
MHRA Draft GxP Guidance:
Periodic Review

- Even if a system is “configured to prevent data manipulation (prevention)”
  - “does not restrict a person from repeating the process by manipulating data to achieve a desired result”
  - Periodic reviews...may reduce risk from repeated events

- Periodic Audits are capable of detecting opportunities for data integrity failures

- Periodic system review might
  - Assess the effectiveness of ...organisational and technical measures
  - verify the effectiveness of existing control measures
  - consider the possibility of unauthorised activity
Periodic Review

- It’s like an internal audit on the compliance of the system
  - Find concerns BEFORE the audit
  - Find ways to improve the efficiency of systems and processes
  - **Documented evidence of actively searching for data integrity issues**
    - Eg Review System Audit Trail for correct use of Admin functionalities
- Review major and minor changes to determine if any retesting or additional testing of new functionality is required
  - Has it significantly expanded or changed use
  - **Is the system still in control and in a validated state?**
- How often?
  - Frequency may depend on maturity and criticality (3-18 monthly)
- **A formal report must be written about the review**
  - It’s a regulatory requirement
What would you look for in System Audit Trail?

- Deleting Data only by designated administrators and WHY
- Creating projects only by designated administrators
- Regular archiving of projects / altering access or status of projects
- Altering System Policies
- User creation patterns
- Password resetting activity
- Alteration of systems
- Changes to roles
Ensuring Adherence to Rules

What makes me drive slower/safer?
- Technical Controls
- Intense “Highway Review” procedure
Summary

- Computer audit trails should be automatically created and not be tampered with
- Most laboratory systems now are equipped with audit trails
  - But do you EVER review them

- How much review will ensure correct user behaviour
- Not practical to attempt on paper: need electronic review
- Don’t let the regulators be the first people to look at the electronic audit trail