An International Pharmaceutical Supply Chain Consortium

GMP Audit Manual

Data Governance and Data Integrity

Authors:

Elayne Kimmett, Biogen

Cathlin Shapiro, Bristol Myers Squibb

Jayne Nicholas, Bristol Myers Squibb

Dan Ewald, Boehringer Ingelheim

Gayle Heffernan, Daiichi Sankyo

Neelima Raval, Daiichi Sankyo

Jim Henderson, Eli Lilly

Lucien Sergile, Eli Lilly

Norma Amilpa, Eli Lilly

Darlene Looney, Johnson & Johnson

Jennifer Baughman, MilliporeSigma

Dale Herbranson, West Pharma

Barbara W. Unger, Unger Consulting

Ben Mills (Reviewer for BSI)

Table of Contents

1. PURPOSE

This audit manual provides an approach for GMP auditing and self-assessment of pharmaceutical manufacturers, contract manufacturers and laboratories for data integrity elements. This includes the manufacture and testing of human and veterinary medicinal products regulated by FDA, intermediates, active pharmaceutical ingredients (APIs), excipients and raw materials critical to product quality. The target audience for the audit manual is GMP auditors and stakeholders including those who have limited experience with data governance and data integrity expectations and enforcement practices.

The audit manual is to be used in conjunction with the *ISPE GAMP Records and Data Integrity Guide.* We refer the reader to this ISPE Guide to provide background and context for the content of the Audit Manual. The audit manual is not intended to 'teach' data integrity concepts. A broad view of computer system classification, validation and controls may be found in the ISPE publication, *GAMP 5, A Risk-Based Approach to Compliant GxP Computerized Systems (2008).*

This audit manual defaults to the ALCOA+ principles where data must be Attributable, Legible, Contemporaneous, Original, Accurate, Complete, Consistent, Enduring and Available as described in the ISPE guide. This Audit Manual is consistent with the ISPE guide in the use of definitions and concepts.

The manual presents items and topics that should be considered during audits and self-assessments focused on assessing data integrity. It is not intended to be used as a simple, non-inclusive, checklist with yes or no answers, but to provide areas for investigation. All topics will not be assessed in each audit, but this manual provides an opportunity to build a tailored organized audit plan addressing specific needs. Audits may incorporate the evaluation of different aspects of data integrity based on the audit plan.

The concepts described in the computer validation section of this manual also apply to GCP / GLP areas and to medical devices. We have chosen, however, to focus only on pharmaceutical GMPs in this manual. Audit schemes and plans will differ with respect to the regulations governing these areas, (21 CFR 210/211, 312 / 314, 58 and 820, 620 respectively). The concepts herein can be applied to non-GMP sites as appropriate.

2. SCOPE

This audit manual addresses the integrity and trustworthiness of GMP records within the regulated pharmaceutical industry. This includes the manufacture and testing of human and veterinary medicinal products regulated by FDA, intermediates, active pharmaceutical ingredients (APIs), excipients and raw materials critical to product quality. Audits of software vendors are not within the direct scope of this manual.

Standards used in development of this manual include the predicate regulations within 21 CFR that identify records requirements, 21 CFR 11 that addresses Electronic Records and Electronic Signatures, the EU GMP Guide including Annex 11 that specifies requirements for Computerized Systems, and ICHQ7 that specifies records requirements. Other global health authorities have published guidance in this area and we encourage the audience to read and evaluate these as part of audit preparation. Global regulations and guidance may be found in the Data Integrity Library developed and published by Rx-360.

3. AUDIT MANUAL STRUCTURE

The manual is divided into three major sections addressing Computer System Validation, QC Laboratories, and Manufacturing. Each of these sections are divided into subsections. While there is some duplication among the sections, duplication has been limited as much as possible. It is important to read the audit manual in its entirety because topics apply broadly and have not been completely repeated in all three sections. Topics including data governance and process mapping are explained in detail in the ISPE Data Integrity Guide and should be utilized to enhance the utility of the audit manual.

4. COMPUTERIZED SYSTEM VALIDATION

Computerized system validation (CSV) is the documented process of assuring that a computerized system does exactly what it is designed to do in a consistent and reproducible manner.

Computer Systems should be designed with data integrity assurance in mind. Thus, the system should be designed, configured and validated in a way that takes into account the principles of ALCOA+, specific health authority requirements, and business requirements. Integrity of any electronic data is best ensured at the development stage, because remediation after implementation is difficult, complicated and often unsuccessful. This

approach is analogous to the Quality-by-Design concepts used to optimize development of manufacturing processes. Both require significant effort up front, with big payoffs during routine use.

Health Authority requirements and guidance for data integrity should be included in the user requirements in addition to business functionality requirements. Regulatory requirements should include predicate rule requirements in addition to expectations in specific data integrity guidance or as identified in enforcement actions.

Confirmation that Computer systems are validated for their intended use generally includes documentation of user requirements (including hardware and software), functional and configuration specifications, design specifications, governing procedures, documentation and testing. Data integrity requirements are embedded in system life cycle requirements and specification documents maintained within the quality system. A full review is not expected, rather, verify its existence and review a sampling of documentation.

Computer Networks, their components and interfaces are qualified to support the applications that reside on the platform:

- Qualified network monitoring tools are used
- Anti-malware software and intrusion detection systems are maintained.

If the firm states that computer systems are ‘validated’ and are Part 11/Annex 11 compliant, confirm that they have, at a minimum, documented user requirements, configuration specification, design specifications, functional specifications and testing as appropriate (including negative testing such as approvals and system access). If not, ask for an explanation of why the systems should be considered validated or ask for documentation that assures the system is validated for its intended use. Also, determine if the system is periodically assessed for the need to re-validate part or all of the system. The periodic assessment should document the evaluation of features such as: all change controls, deviations, help desk tickets related to system performance, and updates from the vendor.

Evaluate the inventory of systems that generates and records GMP data. Ask how the firm decided that the systems did or did not include GMP records. The GMP system inventory should be a controlled list, not one generated specifically for the audit. The controlled list should include, but not be limited to the following:

- Risk based prioritization
- System classification (often presented as a GAMP classification 1, 3, 4 or 5)
- System criticality
- Software and version
- Date of initial validation report sign-off

- Date released into production use
- System Status (e.g., under validation, in production, retired)
- Criticality of requirements: are requirements that are critical to data integrity identified? Do they receive heightened priority in testing and/or regression testing?
- Traceability: are requirements traceable to design/configuration elements and to code (if custom coded)?
- Frequency of periodic assessment of the need to revalidate all or part of the system. All previous information on the versions of the system should be noted.
- Identification of whether systems are networked or stand-alone.

The following elements are supporting information that should be easily accessible for each system:

- Computer infrastructure qualification (E.g. servers, networks)
- Current system description detailing the physical and logical arrangements
- Current process owner (in department using system, data owner) and system owner (system support, administration, maintenance and security) and system supplier
- Data and data flows (to identify electronic records generated by the system and the use of electronic signatures), audit trails, metadata
- Interfaces with other systems or processes for example:
    - Is the interface validated?
    - Is it included in the Periodic Review of the system?
    - Is there a defined owner of the interface?
    - Has the risk of interface failure been documented by Business QA?
    - How is failure of an interface detected, and who receives the failure notification?
- Hardware and software prerequisites
- Business continuity plan
- Disaster recovery plan
- Backup, restore and archive

4.1 PURCHASING CONTROLS FOR COMPUTER SYSTEM CONTRACTED SERVICES

- This section provides general overview of areas to be covered including:
    - Supplied products and components, software vendors are not in scope
    - Supplied Services
    - Consultants

- If they are used, how are 3rd party hosting facilities qualified?
    - Who approved the hosting facility, when, and on what criteria was the qualification based?
    - How is ongoing oversight provided?
- Review the SOC (Service Organization Controls) for the suitability of the hosting facility (such as certification for security, availability, processing, integrity, confidentiality and privacy).
- Formal agreements and responsibilities of the parties shall be described for suppliers and service providers who might provide, install, configure, integrate, validate, maintain, modify or retain a computer system or related service for data processing or storage. Suppliers and developers of Customized/Configurable systems, Commercial Off The Shelf or other computer services should be evaluated / audited to determine their competence and reliability. Evaluation and the need for audit should be risk-based and documented. This may include Quality Agreements, Supply Agreements and Master Service Agreements.
- Determine whether IT/Product/Service procedures are governed by a Quality System, compliant with ALCOA+ principles. How are they maintained and reviewed?

4.2 SYSTEM DEVELOPMENT LIFECYCLE

- Does the System Development Lifecycle (SDLC) have SOPs and Work Instructions that govern the system lifecycle including validation?
- Are there separate procedures for “Core” applications, versus “Project Specific” applications?
- Are testing tools (Automated, Manual and/or Performance testing) utilized? Are they qualified or validated? Evaluate documented evidence of performance and integrity testing, for some configured systems, such as web-based interfaces and interactive response technology systems.
- Are any programming/coding standards, including code review process used? Verify the person who verifies/checks the code is not the person who wrote the code.
- Is the source code tested with associated data and maintained? How long is the source code information and history stored and available? How long is each version supported?
- Are both the SDLC and system functions (e.g., administrator, security, access, audit trail, reporting, and electronic signature functions) addressed in the Validation Documentation used to create and validate the system?
- Are controlled, validated tools used for Source Code Control, Change Management, Bug Tracking, and System Requirements/System Documentation?

- Is real time transaction logging employed? What is the Recovery Time Objective and Recovery Point Objective (RTO, RPO), which provides the amount of time that the business can be without the service, without incurring significant risks or significant loss. A recovery point objective, or "RPO", is defined by business continuity planning. It is the maximum targeted period in which data might be lost from an IT service due to a major incident.
- Who decides the scope of data that can be lost with a single catastrophic failure? Can data be manipulated or deleted?
- Testing should identify acceptance criteria, the actual results (not simply PASS/FAIL), screen shots of test evidence (where applicable) or reports and identify the person performing the test and the date the test was performed. It should include either initials or a handwritten signature and date unless the documentation is capable of electronic signatures.

4.3 SECURITY

System access and controls should be defined in a local procedure. How is the system and database secured (e.g., encryption, partitioning)?

System Access:

- How is access granted?
- How is access revoked?

System Control:

During the audit, ensure the roles and privileges are provided in a report format generated from the system.

- Are there different levels of access that have role-based security?
- Verify system roles and privileges match access roster.
- Each user should have a unique username and password (alpha/numeric combination) for both the application software and the operating system.
- Work performed should be traceable to a unique individual including any 3rd party contractors performing work on or within the system.
- User and administrator privileges should be reviewed for the ability to modify or delete data.
- Passwords should be changed periodically with automatic lockout if not changed.
    - Is reuse of passwords limited?
- Does the application have an audit trail for changes to security roles?

- User Privilege Levels – Each data acquisition system should have appropriate and defined user levels based on the role the user will have in the system (user levels can include analyst, supervisor, manager and administrator or other as defined by the specific software). Privileges assigned to each level should be clearly defined and commensurate with the requirements for each user type (including the ability to create methods, modify integration parameters, reprocess data and modify data).
- Who has access to electronic system upgrades and system site support? Evaluate access levels internally and externally. Who are the local administrators (primary and secondary) managing the system under the system owner? Is the system owner and process owner of the system defined?
    - Remember to consider that default administrator accounts and password are often provided in the user guide. How has this been controlled? Is this verified after outside company, vendor/supplier, performs system maintenance?
- Who approves the system roles/ access? How is access added, periodically reviewed or removed?
- Check the list of user rights for the systems being audited. For example, QC Systems (HPLC, FTIR), manufacturing, process automation, etc. Reference security controls section.
- Identify the Technical System Owner and Process Data Owner. No conflict of interest over results generated should be in place. System administrators should not report to the Quality Unit or the department generating the data.
- How is the system accessed (e.g., through a LAN, single sign-on or through a network directory)?
- Are antivirus, firewalls, intrusion detection, and other systems in place to secure the infrastructure? Is it tested and monitored (for events such as malware attacks)?
- Are there any interfaces with other systems and is the data secure and moved in a manner that prevents data manipulation? How is it secured?
- Are Staff automatically blocked from accessing the systems after a defined number of incorrect attempts? Are workstations set to automatically log off after a period of inactivity (e.g. 5-15 minutes)?
- Mechanisms should be in place to ensure that files cannot be accessed outside the application software (e.g. via the operating system) and copied, edited, moved, renamed or deleted. The file should have a fixed path and folder for saving data that cannot be manipulated by the analyst.
- When an individual changes roles within the company, is the change reflected in their system access? Determine how this is controlled and implemented. For example, compare the admin roles with their job functions in the company.

- Determine time interval when an individual leaving the group or company must be removed from system access
- During an audit, it is useful to identify individuals who recently left the group or company and compare their date of termination/movement with the date that their computer system access was removed.
- From an audit perspective, it is useful to identify if the Company has a policy governing retirement of computer systems and their associated data.

4.4 ELECTRONIC SIGNATURES

- Is the electronic signature secure from being deleted, copied, transferred or altered (such as; the signature cannot be cut and pasted)?
- The information contained in the electronic signature meets all the electronic record controls and requirements (e.g., audit trail and authority checks).
- Do electronic signatures require two distinct identification components (such as; username and password)?
- Do electronic signatures identify the meaning of the signature, such as review or approval? Is there a governing procedure that defines the meaning of an electronic signature?
- Does the electronic signature have the same legal binding authority as the handwritten signature?
- Electronic Signature must have all components (it is not simply signing on a pad with a stylus)
- Unique for each person -User ID and Password (most secure is alphanumeric and symbol) and electronic signatures cannot be reused or reassigned to another person.
- A separate electronic signature is required to access the Operating System and each system accessed through the OS.
- If a change is performed, the reason for the associated change is noted (e.g., deletion)
- When an individual executes a series of signings during a single continuous period of system access, the first signature will require all the electronic signature components. Subsequent signings will require at least one electronic signature component that is designed to be used by, is only executable by, and is known only to the owner of the electronic signature (e.g., password).
- Are password(s) stored in documentation that is accessible to unauthorized persons?
- A procedure identifying the periodic review of users should verify that all users are current.

4.5 POST VALIDATION

- Are critical/major deviations or issues/discrepancies documented during validation and remediated prior to proceeding into the production phase? If not, what is the justification for proceeding into the live environment?
- Are changes to the hardware and software (including vendor patches or updates) managed under a formal Change Control system once placed into production? Review the list of all changes made to computer systems over the past two years and identify a change control for a specific system to review.
- Have incidents been recorded as a result of a Change that has not followed the change management process?
- Does the formal change control of the system include a risk assessment and determine which test(s) will be executed in order to ensure security and functionality of the system?
- Is there a periodic review process in place, for critical GMP systems? Remember to evaluate system interfaces.
- What are the procedures for customers (purchasers/users of the vendor's software, system or services) to report needed enhancements, problems and issues and what are the response times and escalation processes? Are data changes given any added review, such as Business QA, to determine if they are scientifically valid?
- Who controls the system changes (e.g., System administrator, IT help desk)? What kind of changes can they make? Evaluate some period of system tickets to ensure staff aren't making changes outside the Quality System documentation. Look for the term 'data fix'.
- Who has access to system upgrades and system site support? Who are the local administrators (primary and secondary) managing the system. Who has administrator privileges?
- Evaluate Service Provider access, (EU Annex 11 and ICH Q7), because they can be granted administrator privileges. Service owner must be engaged when working on the system. Verify that individuals who control system access have the knowledge, training and expertise to perform this role. Ensure that documentation is available to support granting of access and removal of access. Evaluate the oversight of onsite/remote service providers. Who provides them access? Who rescinds the access? Can they access remotely? Ask for documented evidence of this for one of the last service provider visits. Does anyone evaluate what activities service provider performed within the system before they leave the site to determine that nothing inappropriate was done (e.g., changing roles and access) or changing parameters?

4.6 BACKUP and ARCHIVAL of ELECTRONIC DATA and RECORDS

For the definitions of Backup and Archival of Electronic Data and Records please refer to the definitions in the ISPE GAMP Records and Data Integrity Guide.

- How frequently are backups performed? What media or alternate storage locations are used? How are backup media secured on-site and off-site? How are backup failures documented and managed? Is data verified? What files are backed up? Are all original data (including metadata) backed up? Does the backup/archive contain the audit trail and all appropriate metadata?
- Archived Data and Data backed up (verified at a defined frequency based on risk).
- Thumb drives and CDs should not be considered as secure long-term storage modalities for systems that are not part of the network. They may best be used to transfer data / metadata between systems not connected to a secure network. If used as long-term storage, evaluate the data that ensures their stability during the retention period. Thumb drives and CDs used for this purpose should be secured, authorized and approved.
- Backup and archiving should be driven by a procedure. How often are the backup schedules reviewed?
- Has the backup and recovery procedures been qualified/validated?
- Is data vulnerable (data deletion/modification) prior to data archival?
- Backup and archival data storage site(s) should be secure and protected from environmental mishaps (e.g., temperature/ humidity, water, fire).
- A record or Log book should identify items placed on the media for backup and archival. (e.g.,Title, identification, initials and dates on the media label)
- Is there a Business Continuity Plan with a succession plan and a Disaster Recovery Plan that is exercised or verified periodically? Has the plan been tested, if not, how is it ensured that it will work? If not tested periodically justification should be provided.
- Disaster Recovery plan should be tested at a defined frequency based on risk. A procedure should define content of a disaster recovery plan. Elements should include:
    - Security of the data storage system
    - Room or server cabinet locked with limited access, room design with cables overhead (not in the floor to avoid problems with flooding)
- Is there a fire protection system?
- Climate (temp and humidity) controlled and linkage to the appropriate building management system or BMS. Audible and visual alarms present? How does the firm respond to environmental excursions outside of the control limits?
- Electric supply cannot be easily disconnected.

- Are the electronic records preserved in human readable format for the required regulatory retention period and verified over time? Is information archived? Where? How is it secured and protected from environmental hazards such as flood/water and fire?
- Do SOP(s) describe how data is backed up that includes the process (e.g., tapes, disks, cloud), frequency and actions to be taken if a backup failure occurs?
- Ensure that the firm has a way to retrieve data from legacy systems and has tested the process.
- Has the backup of data and metadata been tested? If failures occurred, how were they addressed?

4.7 GxP SPREADSHEETS

- Spreadsheets should be assessed if they are classified as managing GxP data.
- GxP Spreadsheets, when used, should be considered electronic data and should be retained, and be subject to backup and archival.
- Spreadsheets should be controlled throughout their lifecycle including development, validation, use, access control/password protection, revision/change and retirement.
- Spreadsheets should be maintained and used within an environment (e.g. Finbury Solutions' DaCS or Agilent OpenLAB) providing 21 CFR Part 11 controls, such as, access control, audit trails, and electronic signatures). Calculation cells should be mapped, locked and be subject to change control.
- Spreadsheets should not be stored on individual staff desktops. The spreadsheet should be in a limited access folder for specific staff access.
- 'Single use' spreadsheets are generally not controlled and should be carefully evaluated for GxP applicability. Is the data for these independently verified?
- Review of spreadsheet generated data not maintained and used in an environment identified earlier in this section, may necessarily include a review of the embedded calculations against a 'master' to ensure no changes have been made.
- Spreadsheets are also used to track GMP activities against timeline critical systems, such as Preventative Maintenance/calibration and stability schedules, these are considered to be a GMP tool that should be controlled and secured.

5. QC LABORATORY

5.1 GENERAL LABORATORY CONTROLS

- Data Integrity Risk assessments should be available for each computerized system identifying any gaps and associated actions taken for their remediation.

- If interim short- term remediation actions are implemented, they should be described and justified and long-term remediation plans should be identified with a target timeline.
- Gauge staff knowledge of Data Integrity when possible.
- Determine if all solutions used in an analytical procedure (e.g. samples, standards) have traceable preparation records
- Cross-check stability testing dates with dates when samples were pulled from chambers. Any late testing should have proper justification and impact evaluation.
- Cross-check that individuals sign/approve results contemporaneously with the activity. For example are the time intervals during and between activities realistic?
- Check trash cans and recycle bins in computers. Are records being discarded or deleted?
- Check training records on Good Documentation and Data Integrity Practices.
    - For example, are worksheets and notebooks located in the immediate area to ensure contemporaneous documentation?
- It is useful to request a list of all notebooks or worksheets issued in the past two years and their status. Ensure that worksheet and laboratory notebook numbers are sequential and controlled, reconciled and archived.
- Any controlled laboratory forms (such as laboratory notebooks and worksheets) must be version controlled including issuance, should be numbered, reconciled, and archived.
- Documentation procedures should be developed to address, at a minimum:
    - Good Documentation Practices (ALCOA+ principles apply).
    - Naming conventions for data.
    - Control of folders where electronic data are saved. Identify who has access to name these folders.
    - System access controls - see “Security” section 4.3.
    - Data generation including ‘test’ injections and their requirements / management and justification (all data should be retained, secured and accounted for).
    - Data processing including but not limited to manual integration or other manual processing.
    - Data review including a defined periodic review of defined audit trails, particularly for “modified” and “deleted” data. Data are to be reviewed in the format in which it is originally collected, thus most laboratory data review will be a review of electronic data unless otherwise justified. Consider that a single description of ‘electronic data review” will generally not have sufficient detail so that it can be applied to all systems. Identify critical records and their review frequency.

  - Data approval should be described and documented either electronically (electronic signature) or using a manual paper based system (e.g., one person performs the review and another person approves the data).
- Have data flows diagrams been established for all laboratory equipment and supportive laboratory systems? If not, how have points of risk been identified? Consider the manual or automated transfer of data from an electronic system into a spreadsheet used for calculations and then a transfer back to LIMS or a lab execution system (e.g. NuGenesis (ELN)). Multiple points of risk exist for this type of process.
- Data verification and second person review of critical calculations or documenting of raw data for instruments which do not have printouts or data acquisition systems should ensure verification is occurring contemporaneously.
- Good Documentation Practices should be evaluated during the laboratory tour.
- Verify the laboratory notebooks follow Good Documentation Practices.
- Interview QC staff about job functions, investigation processes, data integrity and overall tasks associated with job function and or data generation processing, second person verification, review, and approval.
- Determine if there are systems with shared log-on's accounts. The use of post-it notes on the back of instruments, or under the keyboard can be suggestive of poor practices. Check the cabinet drawers under the instruments.
- Are activities documented at the time they are performed?
- Are there loose papers in drawers, pockets or waste containers that contain notes, calculations, or reminders? Are forms or other controlled documents, with or without raw data, found in the general lab area (including trash cans, work stations, or drawers)?
- Are analysts located close to their documentation as they work? Are procedures or test methods readily available for the analyst to use and are they used during testing?
- Does the sample management and data lifecycle reflect the concepts of data integrity? Is there appropriate traceability (e.g., Chain of Custody) of the samples from manufacture, receipt in the laboratory, analytical testing, data processing, review and approval, to the issuance of the CoA captured? Is a program implemented to ensure associated retain samples are taken as appropriate? Is there accountability for destruction of samples?
- Documentation is completed per ALCOA+ principles in accordance with local QMS procedures in lab notebooks/ documentation with required secondary verification, review, or in an electronic system such as LIMS, that has been validated ensuring the principles of data integrity have been evaluated, with appropriate data authorization by a qualified laboratory person in charge. Procedures describing the review life cycle, roles and responsibilities should be implemented and trained

on by the appropriate laboratory personnel.

- The list of GMP computerized systems should include all GMP laboratory computer systems as noted in Section 4.
- Are there any systems in the laboratory where data is manually or automatically transferred between systems? What controls are in place to mitigate any data integrity issues? This includes the situations where data may be manually transferred from an electronic system to a spreadsheet for purposes of calculations and then hand entered into LIMS. Verification or validation of the data transfer process should be tested and completed.

5.2 DATA GENERATION

- Evaluate invalidated laboratory results, their investigation and their justification.
- Were retests performed with passing results? Investigate to ensure this wasn't just 'testing into compliance'. What percentage of OOS results are invalidated?
- All injections need to be identified. Each injection purpose can be acceptable or unacceptable depending on the nature of that injection and how the results are managed. There should be no unofficial live sample injections prior to beginning an official sequence.
- Are data saved immediately as acquired or do they exist in a 'buffered' state (inclusive of RAM (Restricted Access Media) for Chromatography Data Systems or stand -alone systems for temporary storage) where modification can occur undetected?
- Verify how data are saved:
    - Automatically
    - Save only to a predefined secured pathway/folder
    - Save as: If analyst interactions are required ensure they don't have the ability to not save data which is the same as deleting data.
- Who has access to electronic system upgrades and system site support?
- If data collection is interrupted has an assessment been performed to determine the cause? Can intentional and unintentional data loss be detected?
    - Can data collection be aborted?
    - Can data collection be hidden by reducing the results scale?

5.3 AUDIT TRAILS AND CRITICAL META-DATA

- Critical data and meta-data that permit reconstruction of activities (who, when, date and time, what, and why) are often referred to as an 'audit trail'. Appropriate risk based audit trails should be identified for each system to ensure that complete data are reviewed prior to critical data approval. Audit trails for critical testing and lot release testing should be reviewed for each analysis. Data should not be able to be modified, deleted or otherwise obscured (such as with annotation tools like

Adobe Pro®). All data must be retained and considered in the data review process.

- Is there a governing procedure for data review including audit trail review?
- Audit Trails – The audit trail feature must be enabled (turned on) for software systems and should not be able to be disabled (turned off) after initial system configuration.
- Date / Time stamps are a component of an audit trail, and should be automatic in their collection, and should not be modified or editable by anyone including system administrators. There can be exceptions for the administrator to work with proper controls for originally setting the date/time and managing a power failure or system crash.
- Every system may be different on how to access an audit trail (check record history, check reports, database queries)
    - Can it be modified (changed or deleted or data overwritten)?
    - Is the audit trail accessible?
    - Have critical audit trails been identified for review requirements? Are the correct personnel reviewing the audit trails, and are they trained to identify and review any modifications/alterations to the data prior to data approval and or release? Are systems in place to investigate if issues are identified? Is the audit trail accessible? Have a data reviewer demonstrate how they access the audit trail.
    - People with direct interest in the data should not have the same system access as those authorized to make changes to the data.
- Check audit trails for samples with names such as “test”, “trial”, “demo” or “retest” or events such as “modify”, “delete”.
- Periodic audit trail evaluation of ADMINISTRATOR activity should be performed. These reviews should be noted in an SOP, be independent and occur at defined intervals.

5.4 DATA PROCESSING

- Data that is processed must preserve both the original and re-processed results.
- There should be adequate traceability of any defined parameters used within data processing activities.
- Data processing should be performed using approved protocols or methods and not be performed subjectively.
- Review the audit trail for any evidence of a change in the data acquisition sequence.
- An SOP should describe when manual integration is permitted and if additional review and approval are required. The audit trail should document and justify all modifications. All chromatograms and associated data should be saved; none

should be overwritten. All data (for example, this would include documentation of all unprocessed and processed data) should be reviewed to ensure manual integration actions were taken per governing SOP.

- HPLC processing methods (including integration parameters) must be defined and controlled. Manual integrations must be justified and approved. All injections in the same sequence must be processed with the same defined methods and integration parameters (e.g., including when processing standards that are used for quantitation of the samples). Any sequence or processing method changes must be justified.

5.5 DATA REVIEW

- Some information and events may suggest problems, and warrant further investigation: Never having OOS results, never having microbiological counts (always 0, always even or always odd numbers) or have a very narrow data variation among several batches may require further questioning.
- Data should be reviewed in the format in which it is collected (e.g. static or dynamic). Thus, printed chromatograms or other reproductions are not sufficient for review of electronic data.
- Data Review should include review of critical data and metadata (audit trails).
- Data review should be described in an SOP and should be of sufficient detail to ensure that the assessment is consistent among reviewers. Review should consider all data generated as part of the analysis and include an evaluation of the specified audit trail considering any modification or changes made in the methods or results. There should be a documented and approved justification explaining why the change or modification was made.
- Verify that adequate procedures are in place for System Suitability & Sample Analysis Check. Sequence A (System suitability) and Sequence B (Sample Analysis) should be defined. If the lab does not check system suitability prior to sample sequence, ensure their procedure requires an investigation should system suitability failure occur and sample data is reviewed.
- Cross-check the analysis of one particular batch with the audit trails of involved computerized systems to ensure that everything was reported. Check tests conducted immediately before and after to ensure all data are accounted for.
- Verify equipment logs and any other supporting data is in agreement regarding lot numbers, dates and results.
- If a computerized system does not have an audit trail or unique password capability, the paper segment of the hybrid system should be evaluated as part of data review.

- Look for data stored in unapproved folders or on the C-drive/recycle bin. Determine the folder naming convention and identify if analysts can initiate and name new folders where data may be 'hidden'.

5.6 PAPER BASED AND HYBRID SYSTEMS

The following questions are applicable for hybrid based systems in both the QC Laboratory and in Manufacturing:

- For those systems that the auditee identifies as 'hybrid', the controls and their adequacy should be identified, justified and communicated. If the controls are meant to be used on an interim basis, while new software or equipment is on order, this should be identified and a timeline specified for full remediation.
- If a computerized system does not have an audit trail or unique password capability the paper segment of the hybrid system should be evaluated as part of data review, along with the electronic data
- The 2018 MHRA 'GXP' Data Integrity Guidance and Definitions (March 2018) states that *"Where systems do not meet the audit trail and individual user account expectations, demonstrated progress should be available to address these shortcomings. This should either be through add-on software that provides these additional functions or by an upgrade to a compliant system. Where remediation has not been identified or subsequently implemented in a timely manner a deficiency may be cited."*

5.7 STAND ALONE SYSTEMS

Stand-alone systems are connected to an external computer used for instrument control and data acquisition but are not controlled by a central validated system (i.e. Empower). Examples of stand-alone systems can include FTIR, UV/Vis spectrophotometers, Karl Fisher, plate readers, capillary electrophoresis, and NIR. These are generally GAMP Category 3 systems.

Stand-alone systems that meet data integrity requirements of ALCOA + include but are not limited to the following:

- Logical controls to restrict access to authorized personnel, see Security section 4.3.
- Prevent the deletion of data and unauthorized modification of data.
- Provide a means to automatically store data, either on a secured local drive (e.g. C:\data) or on a secured network drive including secured pathway and folders.
- Data that are managed and stored either in a flat file or a relational database (Relational data base are encrypted and provide more data integrity controls).

- For systems connected to the network server:
    - If the data are directly saved to a secured network, the backup and archival process should be managed through an automated or manual process that is validated.
    - If the system is connected to the network and the data are saved locally, the backup and archival process must be validated.
- If a system is not connected to the network, backup and archival may be sporadic or not performed at all. Rationale must be provided if backup/archival are not performed.
    - If temporary methods are used for backup or archival (e.g. thumb drives, CD's, etc.,) ensure the security and stability of the storage medium has been validated. These media must be access controlled and stored in a secure location protected from environmental damage (e.g. heat, humidity, fire, flooding).
- For systems connected to the network, determine where the original data are stored, either local drive or a secure network server. If stored locally, review the backup/archival process and ensure it is validated. Ensure a risk-based approach was used and documented to determine the backup/archival frequency.
- Provides a process for regular backup and archival of all data including relevant metadata. The firm should evaluate and justify the backup / archival frequency. The evaluation should consider the amount of original data that could be lost in a catastrophic computer system failure. (See Backup and Archival section 4.6).
- Provide a secure computer-generated time-stamped audit trail for actions that create, process, modify, or delete electronic records.
- Older stand-alone systems may represent a higher potential for data integrity risk as these systems may not be capable of data integrity controls, for example:
    - Data storage or management, sometimes data can be accessed through the Windows operating system and data can be altered or changed without being recorded in an audit trail.
    - Ability to modify Date and time stamps may be available to analysts and operators.
- The 2018 MHRA 'GXP' Data Integrity Guidance and Definitions (March 2018) states that *"Where systems do not meet the audit trail and individual user account expectations, demonstrated progress should be available to address these shortcomings. This should either be through add-on software that provides these additional functions or by an upgrade to a compliant system. Where remediation has not been identified or subsequently implemented in a timely manner a deficiency may be cited."*

5.8 DATA INTEGRITY IN MICROBIOLOGY LABRATORIES

- Manual testing and recording operations can contribute to data integrity and data falsification. Reviewing data trends can be helpful to determine if the data are problematic (such as; purified water systems with no microbial excursions or clean rooms with no environmental monitoring excursions).
- Microbiological samples are often read and then rapidly discarded, so it is sometimes difficult to obtain evidence of falsification. Physical spot checks of samples in the incubator or trash container against recorded results can be helpful to establish sample history, control, testing, data collection and reporting.
    - For example, media growth promotion results patterns; there have been instances where only even numbers of colonies were recovered. Review of growth promotion testing should include checking that the specification limit calculations have been performed and applied correctly. Incorrect numbers, may indicate out of specification (OOS) results have not been reported.
    - Ensure that data is recorded exactly and, upon later retrieval, ensure that the data is the same as it was when it was originally recorded.

6. MANUFACTURING

Manufacturing should have the same data integrity controls as those described previously in laboratory systems. Data should be managed similar to laboratory data based on critical process parameters (CPP) and documented risk assessment. Such as: equipment/instrumentation which can be defined as; stand-alone equipment, in line (embedded controlling process), at line (connected for monitoring), off line (adjacent manufacturing lab) and equipment not connected to a data acquisition system.

It is important for the auditor to evaluate who has specific access level authority. Is the access control matrix (list of employees with privileges to access) current and approved? It must be ensured that employees requiring access have the lowest level of access needed to perform their job function. The following might be evaluated:

- Consider how recipes (both manufacturing and cleaning) are controlled and which individuals/departments have access to change them?
    - How are changes in the recipes documented?
    - What initiates a change in recipe and what functional groups make that determination? For example, if 200 people have access to change recipes it will be difficult to justify recipe control to a health authority.
    - How is the change in recipe assessed?
    - Does Quality provide any oversight?
- Ask the system administrator to show the system audit trail for changes made by the administrator/ADMIN over the past year.

- Consider that dates / times in PLCs should agree with dates of operation in equipment use log books.
- Evaluate filter integrity test units to determine if all data are retained and reviewed or whether all paper printouts are retained and reviewed. Can data be deleted or abandoned?

7. HOW TO ADDRESS CMOs AND CRITICAL SUPPLIERS OR CRITICAL SERVICE PROVIDERS

21 CFR 200.10 addresses contract facilities employed by pharmaceutical firms. It states: '*The Food and Drug Administration…regards extramural facilities as an extension of the manufacturer's own facility.'* Therefore, the audit information and concepts presented in this audit manual applies to a CMO, critical suppliers or critical service providers.

- Evaluate if an SOP and Data Integrity Program exist at the company/site
- Evaluate if an existing Quality Agreement delineates the requirements to ensure data integrity.
- Evaluate if a data integrity gap assessment has been performed by the supplier
- Evaluate system controls focusing on high risk areas and data in this Audit Manual including QC, Manufacturing, and Computerized System Validation
- Evaluate data transfer, release testing, supplier management and audit program
- Assess any security procedures and/or policies that govern system infrastructure (e.g. network).

For further information, you may contact:

Rx-360

info@rx-360.org

301-710-9399

Document Published March 2018.