Parenteral Drug Association

Technical Report No. 80

Data Integrity Management System for Pharmaceutical Laboratories

PDA Data Integrity Management System for Pharmaceutical Laboratories Technical Report Team

Authors and Contributors

Maryann Gribbin, Faith & Royale Consulting, (Co-Lead)

Anil Sawant, PhD, Merck Sharpe & Dohme, (Co-Lead)

Denyse Baker, Parenteral Drug Association

Peter Baker, U.S. Food and Drug Administration

Dennis E. Guilfoyle, PhD, Johnson & Johnson

Kir Henrici, Faith & Royale Consulting

Crystal Mersh, Quality Executive Partners Inc.

Raghuram Pannala, PhD, Sciegen Pharmaceuticals Inc.

Carmelo Rosa, PsyD, U.S. Food and Drug Administration

Jonathan Rose, Patheon Pharmaceutical Services

Siegfried Schmitt, PhD, PAREXEL Consulting

Ronald Tetzlaff, PhD, PAREXEL Consulting

John T. Davidson, Merck Sharpe & Dohme

Thomas Arista, U.S. Food and Drug Administration

Data Integrity Management System for Pharmaceutical Laboratories

Technical Report No. 80

ISBN: 978-1-945584-05-3

PDA®
Parenteral Drug Association

Table of Contents

FIGURES AND TABLES INDEX

1.0 Introduction

A primary responsibility of pharmaceutical manufacturers is to provide safe and efficacious products of appropriate quality to patients and consumers by assuring decisions are based on accurate, reliable, truthful, and complete data. Data integrity is a mandatory requirement and key concern of health authorities. At the time of this writing, data integrity citations, especially those related to computerized systems in laboratory and manufacturing environments, have resulted in a number of significant, well-publicized enforcement actions from the U.S. Food and Drug Administration (FDA) and other regulatory authorities, including the United Kingdom Medicines and Healthcare products Regulatory Agency (MHRA), and European Medicines Agency (EMA). These enforcement actions have taken the form of warning letters, import alerts, statements of GMP noncompliance, notices of concern, and refusals to accept and/or approve applications. Many of these actions involve failing to document or report alterations, deletions, fabrications, and/or misrepresentations of data in quality control laboratories. The range of data integrity findings spans the spectrum from unintentional errors in data reporting and lack of controls necessary to ensure data authenticity to intentional acts involving failure to report data and/or falsification of records.

The spike in enforcement actions, in part, is linked to improved detection capabilities, which have become more prevalent as technological enhancements have extended the level of automation in both pharmaceutical quality control and microbiology laboratories. The extensive use of computer systems and digital media for product testing, as well as in ancillary support systems, provides more visibility to data integrity gaps than was evident with static paper records.

The consequences of failing to uncover data integrity problems through self-discovery or internal audit programs before they are found by regulatory agency inspectors can impact the outcome of the inspection in ways that could be very damaging to a business. Similarly, the business impact on contract manufacturers, contract laboratories, and suppliers can be very serious if they fail to uncover and disclose data integrity problems before regulators or their customers' auditors do. One of the responsibilities of regulatory agency investigators is to verify the accuracy, reliability, and integrity of data submitted in written form or other media prior to, during, or after an inspection, or as part of a drug submission for market authorization, annual report, mandatory quality defect report (e.g., Field Alert), or Adverse Event Report. The regulatory investigators (also referred to as inspectors in some regulatory regions) may detect and document inconsistencies between the information provided and available for review that may suggest data integrity problems that the company will need to correct. Such inconsistencies can be used by the health authority as the basis for a regulatory action or formal written communication. From the regulators' perspective, noncompliance with good data integrity practices is not based solely on the intent to mislead authorities to believe that all laboratory activities are performed according to current good manufacturing practices (CGMP) when they are not. Requirements for appropriate laboratory records and documentation began with the first GMP regulations and expectations have been clarified in other publications such as the FDA Guide to Inspections of Pharmaceutical Quality Control Laboratories published in 1993 ***(1).***

In some instances, a regulatory agency may decide to ban products from entering its jurisdiction and order or recommend that the potentially affected product be removed from the market.[1] Regulatory agencies and organizations that oversee a manufacturing site's adherence to CGMPs have made significant efforts to communicate their expectations to both industry and their inspectorates about managing data and ensuring its integrity. Some of these expectations can be found in the U.S. FDA *Draft Guidance for Industry on Data Integrity and Compliance with CGMP (*April 2016), World Health Organization (WHO) *Guidance on Good Data and Record Management Practices* (May 2016), Draft PIC/S Guidance *Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments* (August 2016), MHRA *GXP Data Integrity Definitions and Guidance* (March 2018), *Guidance for Industry, Part 11, Electronic Records; Electronic Signatures—Scope and Application* (August 2003),

[1] Some regulatory agencies have the legal authority to order product removal from the market, while others can only recommend such actions.

and *EU Annex 11: Computerised Systems* (June 2011) ***(2–8).*** Even older health authority publications on traditional audit practices may also be helpful in identifying and preventing data integrity issues in laboratories. Some examples include: FDA Guide to Inspections of Pharmaceutical Quality Control Laboratories ***(1)*** and the European Medicines Agency (EMA) Questions and Answers: Good Manufacturing Practice–Data Integrity ***(9).***

This increased focus on data integrity by health authority investigators has resulted in the need for firms to modify and harmonize strategies to address data integrity gaps in a manner that promotes transparency, accuracy, and reliability of data as well as detection of data integrity breaches.

Industry can use technology shifts, along with the new awareness that stems from recent regulatory sanctions, to enhance their efforts to improve processes and establish mechanisms for detection and mitigation of gaps that impact data integrity in paper, hybrid, and computerized systems. The overall goal of ensuring data reliability is to protect patients as well as provide competitive sustainability.

1.1 Purpose

This technical report, developed by subject matter experts from the global pharmaceutical industry and regulatory agencies, summarizes data integrity risks and the best practices, including audit approaches, that can be utilized to develop a robust data integrity management system for laboratory settings with both manual and electronic processes that firms can follow to achieve compliance and mitigate risks. Current regulatory trends indicate breaches in data integrity and a need for additional guidance regarding the regulatory expectations. The intent of this report is to outline regulatory requirements and expectations, along with best industry practices to ensure data integrity, to highlight common gaps in laboratory data management practices, and to recommend methods of remediation.

For the purpose of this report, the term "data integrity" means the degree to which data are complete, consistent, accurate, trustworthy, and reliable and that these characteristics of the data are maintained ***(3)*** to support the quality of drug products throughout their lifecycle from the point of development through commercialization. The reliability of such data is necessary to support clinical trials, product development, manufacturing, testing, and regulatory reporting requirements, all of which are dependent on the processes and controls in place from the point of data creation to ensure data cannot be altered, deleted, omitted, or in any way modified to misrepresent what actually occurred. Data integrity is the cornerstone of establishing and maintaining confidence in the reliability of data.

1.2 Scope

This technical report focuses on the management of data integrity within pharmaceutical quality control analytical and microbiology laboratories and is also applicable to analytical development and R&D laboratories. It provides the framework and tools necessary to establish a robust data integrity management system to ensure data integrity for paper, hybrid, and computerized systems within the laboratory.

2.0 Glossary of Terms

Many of the terms used in this report are defined by multiple regulatory bodies. Because regulatory definitions can form the basis of enforcement actions and, in the United States, prosecutions, regulatory definitions from the MHRA, WHO, FFIEC, and FDA are provided, when available. In the absence of a regulatory definition, the technical report team selected a definition either from an existing PDA technical report, another reputable source, or one reached by consensus of the team.

Archival

MHRA (Archive): A designated secure area or facility (e.g., cabinet, room, building or computerised system) for the long-term retention of data and metadata for the purposes of verification of the process or activity ***(5).***

WHO: The process of protecting records from the possibility of being further altered or deleted, and storing these records under the control of independent data management personnel throughout the required retention period ***(3).***

Audit Trail

FDA: 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. An audit trail is a chronology of the "who, what, when, and why" of a record ***(2).***

MHRA: 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 ***(5).***

WHO: The audit trail is a form of metadata that contains 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 ***(3).***

Backup

FDA: A true copy of the original data that is maintained securely throughout the records retention period. The backup file should contain the data (which includes associated metadata) and should be in the original format or in a format compatible with the original format ***(2).***

MHRA: A copy of current (editable) data, metadata and system configuration settings maintained for recovery including disaster recovery ***(5).***

WHO: A copy of one or more electronic files created as an alternative in case the original data or system are lost or become unusable. Backup differs from archival in that back-up copies of electronic records are typically only temporarily stored for the purposes of disaster recovery and may be periodically overwritten. Such temporary back-up copies should not be relied upon as an archival mechanism ***(3).***

CGMP Record

FDA: When generated to satisfy a CGMP requirement, all data become a CGMP record. You must document, or save, the data at the time of performance to create a record in compliance with CGMP requirements, including, but not limited to, §§ 211.100(b) and 211.160(a). FDA expects processes to be designed so that quality data is created and maintained and cannot be modified ***(2).***

Complete Data

FDA: FDA requires complete data in laboratory records, which includes raw data, graphs, charts, and spectra from laboratory instruments and associated metadata. (§§ 211.194(a) and 212.60(g)(3) ***(2).*** A complete record of all data secured in the course of each test, including date and time the test was conducted and all graphs, charts, and spectra from laboratory instrumentation, properly identified to show the specific component, drug product container, closure, in-process material, or drug product, and lot tested ***(2).***

Corruption (Data)

FFIEC: Errors in computer data that occur during writing, reading, storage, transmission, or processing, which introduce unintended changes to the original data ***(10).***

Data

MHRA: Facts, figures and statistics collected together for reference or analysis. All original records and true copies of original records, including source data and metadata and all subsequent transformations and reports of these data, that are generated or recorded at the time of the GXP activity and allow full and complete reconstruction and evaluation of the GXP activity ***(5).***

WHO: Data means all original records and true copies of original records, including source data and metadata and all subsequent transformations and reports of this data, which are generated or recorded at the time of the GXP activity and allow full and complete reconstruction and evaluation of the GXP activity. Data should be accurately recorded by permanent means at the time of the activity. Data may be contained in paper records (such as worksheets and logbooks), electronic records and audit trails, photographs, microfilm or microfiche, audio- or video-files or any other media whereby information related to GXP activities is recorded ***(3).***

Data Integrity

FDA: 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) ***(2).***

MHRA: 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 ***(5).***

WHO: The degree to which data are complete, consistent, accurate, trustworthy and 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, such 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 ***(3).***

Data Lifecycle

MHRA: All phases in the life of the data (including raw data) from initial generation and recording through processing (including transformation or migration), use, data retention, archive/retrieval and destruction ***(5).***

WHO: All phases of the process by which data is created, processed, reviewed, analyzed and reported, transferred, stored and retrieved and monitored until retirement or disposal. There should be a planned approach to assessing, monitoring and managing the data and the risks to those data in a manner commensurate with potential impact on patient safety, product quality and/or the reliability of the decisions made throughout all phases of the data life cycle ***(3).***

Dynamic Record Format

FDA: The record format allows interaction between the user and the record content ***(2).***

MHRA: An electronic record which the user/reviewer can interact with ***(5).***

WHO: Records, such as electronic records, that allow for an interactive relationship between the user and the record content ***(3).***

GXP

WHO: Acronym for the good practice guides governing the preclinical, clinical, manufacturing, testing, storage, distribution and post-market activities for regulated pharmaceuticals, biologicals, and medical devices, such as good laboratory practices, good clinical practices, good manufacturing practices, good pharmacovigilance practices and good distribution practices ***(3).***

Human Factors

A science discipline that examines human psychological, social, physical, and biological characteristics to evaluate the design, operation, or use of products or systems for optimizing human performance, health, safety, and/or habitability ***(11).***

Hybrid Approach

WHO: The use of a computerized system in which there is a combination of original electronic records and paper records that comprise the total record set that should be reviewed and retained ***(3).***

Manual Integration

Process used by a person to modify the integration of peak area by modifying the baseline, splitting peaks, or dropping a baseline as assigned by the chromatography software to overrule the pre-established integration parameters within the chromatographic software.

Metadata

FDA: The contextual information required to understand data. A data value is by itself meaningless without additional information about the data. Metadata is often described as data about data. Metadata is structured information that describes, explains, or otherwise makes it easier to retrieve, use, or manage data ***(2).***

MHRA: Metadata is 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) ***(5).***

WHO: Metadata are data about data that provide the contextual information required to understand those data. These include structural and descriptive metadata. Such data describe the structure, data elements, interrelationships and other characteristics of data. They also permit data to be attributable to an individual ***(3).***

Original Record

MHRA: The first or source capture of data or information, e.g., original paper record of manual observation or electronic raw data file from a computerised system, and all subsequent data required to fully reconstruct the conduct of the GXP activity. Original records can be static or dynamic ***(5).***

Peak Integration

Process used to by a chromatographic system to determine the peak area (based on height and width) and obtain the quantitation of the peak of interest. The measurement is based on the integral technique of splitting the peak into a large number of rectangles, which are then summed to provide an estimate of the total area under the peak ***(12).***

Raw Data

FDA: Any laboratory worksheets, records, memoranda, notes, or exact copies thereof that are the result of original observations and activities of a nonclinical laboratory study and are necessary for the reconstruction and evaluation of the report of that study. Raw data may include photographs, microfilm or microfiche copies, computer printouts, magnetic media, including dictated observations, and recorded data from automated instruments ***(13).***

MHRA: The original record (data) which can be described as the first-capture of information, whether recorded on paper or electronically. Information that is originally captured in a dynamic state should remain available in that state ***(5).***

Static Record Format

FDA: A fixed-data document such as a paper record or an electronic image ***(2).***

MHRA: A "fixed" record such as paper or pdf ***(5).***

WHO: A static record format, such as a paper or pdf record, is one that is fixed and allows little or no interaction between the user and the record content ***(3).***

Systems (in computer or related systems)

FDA (attributed to ANSI): People, machines, and methods organized to accomplish a set of specific functions. Computer or related systems can refer to computer hardware, software, peripheral devices, networks, cloud infrastructure, operators, and associated documents (e.g., user manuals and standard operating procedures) ***(2,14).***

WHO: A computerized system collectively controls the performance of one or more automated processes and/or functions. It includes computer hardware, software, peripheral devices, networks and documentation, e.g., manuals and standard operating procedures, as well as the personnel interfacing with the hardware and software, e.g., users and information technology support personnel ***(3).***

True Copy

FDA: 21 CFR 211.180(d) requires records to be retained "either as original records or true copies such as photocopies, microfilm, microfiche, or other accurate reproductions of the original records" ***(8).*** Electronic copies can be used as true copies of paper or electronic records, provided the copies preserve the content and meaning of the original or raw data, which includes associated metadata and the static or dynamic nature of the original records ***(2).***

MHRA: A copy (irrespective of the type of media used) of the original record that has been verified (i.e., by a dated signature or by generation through a validated process) to have the same information, including data that describe the context, content, and structure as the original ***(5).***

WHO: A true copy is a copy of an original recording of data that has been verified and certified to confirm it is an exact and complete copy that preserves the entire content and meaning of the original record including, in the case of electronic data, all essential metadata and the original record format as appropriate ***(3).***

2.1 Acronyms

ALCOA	Accurate, Legible, Contemporaneous, Original and Attributable
ALCS	Analytical Laboratory Computerized Systems
COTS	Commercial Off-The-Shelf (software)
CPC	Critical Process Control
CQA	Critical Quality Attribute
CGMP	Current Good Manufacturing Practice
CSV	Comma Separated Values
EDC	Electronic Data Capture
GXP	Inclusive of Good Laboratory Practice, Good Clinical Practice, Good Manufacturing Practice, Good Distribution Practice and Good Pharmacovigilance Practice
ICH	International Conference on Harmonisation
LIMS	Laboratory Information Management System
PQS	Pharmaceutical Quality System
QA	Quality Assurance
QC	Quality Control
QU	Quality Unit
USP	United States Pharmacopeia

3.0 Regulatory Trends for Data Integrity Issues in Pharmaceutical Laboratories

Regulations and guidelines require analytical and microbiological laboratories to have the appropriate controls and procedures, governed by a robust and reliable Quality Unit organization, to ensure paper documentation and electronic data are properly managed ***(15–17).*** Laboratory management and personnel must be properly trained on CGMPs on a regular basis, including on good data management practices, and have the necessary resources to maintain a sustainable CGMP environment. Regulations specifically require each person engaged in a CGMP-related function to be properly trained in the operations they perform and in CGMPs ***(18).*** A review of recent inspection findings and regulatory actions initiated by various health authorities demonstrates that these expectations have not been attained consistently, though the regulations have remained largely unchanged for the past 30 years. The breaches in data integrity found during inspections in recent years have triggered the need to publish additional guidance documents describing more clearly the regulatory expectations in CGMP-related systems (e.g., laboratory, quality, production, utilities, packaging, and facilities/ equipment). These guidances emphasize the importance of good laboratory and manufacturing documentation practices and greater collaboration among regulatory agencies around the world and across the industry.

The common trends identified in regulatory observations between 2012 and 2017 are similar for both analytical and microbiological laboratories and include the following:

- **Failure to perform required testing:** Citations have been issued for sterility testing of finished product, in-process, active pharmaceutical ingredient (API), environmental monitoring, water, and media fills where the required sampling, incubation, and/or testing were not performed, while records were generated as if the sampling or testing had been performed. Regulators have cited firms for failing to perform testing of in-process and finished drug products, while COAs indicate that the final testing had been conducted.

- **Falsification of critical data:** Citations have been issued for falsification of sampling information or test result data in worksheets/logbooks/test reports, including fabricated results for samples not attained and/or incubated, and for reporting failing results as passing.

- **Deletion of data:** Citations have been issued for deletion or overwriting of electronic data generated in the laboratory. A review of many systems' audit trails shows the deletion of chromatographic injections or critical test data information.

- **Deficiencies in deviation reports and investigations of data integrity issues:** Citations have been issued for deficiencies such as inadequate root cause (e.g., did not address data manipulation and falsification), failure to expand the scope of the investigation to assess potential impact of poor data integrity practices on other functional areas, lack of an action plan describing how corporate management and the Quality Unit will prevent data manipulation, lack of a comprehensive assessment of all products manufactured, and lack of data to support applications.

- **Falsification of CGMP records:** Citations have been issued for evidence of falsification of CGMP records, including modification of records, omissions, or reporting inaccurate results. In order to provide more specific context, an analysis of individual citations listed in recent FDA Warning Letters was completed and indicates five common data integrity trends found during the inspection of quality control laboratories. See references ***(19–24).*** For example, in a 2013 criminal plea agreement, the defendant pled guilty to the introduction into interstate commerce of adulterated drugs, with intent to defraud or mislead, failure to file timely required reports, making false statements ***(25).***

- **Failure to ensure that laboratory records included complete data:** derived from all tests necessary to ensure compliance with established specifications and standards. Regulators have found that laboratories fail to maintain critical test result data pertaining to products tested (which may include incoming raw material, in-process testing, released test results, stability results, or data generated during the testing of exhibit batches). This deficiency is often cited during API inspections as "Failure to maintain complete data derived from all laboratory tests conducted." Investigators find that out-of-specification (OOS) test results are excluded, not reported, or not investigated. Unexplained missing or deleted chromatographic data also have been reported under this category. During the review of FDA Warning Letters published between 2012 and 2017, unexplained deletions of laboratory test results often were associated with repeated test analysis with no justification nor explanation. Incomplete data sets should be detectable through audit trails which are reviewed on a routine basis. Failure to ensure that laboratory records be complete is not a new issue. A case filed in 2012 in a federal district court, shows the U.S. Government and a regulated pharma firm entering an agreement that listed, among other violations found by the government a failure to include in laboratory records a complete record of all data secured in the course of each test, including all graphs, charts and spectra from laboratory instrumentation ***(26).***

- **Failure to configure computerized systems to meet the requirements for the security and control of data,** in particular, permitting unauthorized system access, allowing for the deletion of electronic and printed raw data (including information related to undesirable or failing results), and/or failing to configure and/or enable audit trails. This category of citations was referenced in more than 15 FDA Warning Letters between 2012 and 2017, primarily spotlighting the failure to properly configure laboratory systems used for high performance liquid chromatography (HPLC), gas chromatography (GC), and ultraviolet (UV) and infrared (IR) analysis that leaves them vulnerable to data manipulation. In some cases, an actual breach in data integrity was described, while in others, only the failure to properly secure and configure the system was cited. Regulators have found electronic data manipulated or computerized systems misused primarily due to limited or inappropriate controls in place. For example, analysts performed "pre-analysis, sample trial injections, unauthorized or unofficial" HPLC or GC injections and modified or altered a computer's time-and-date stamp of the "official sample" to make it seem as if the "official sample" was tested at the time the pre-analysis, sample trial, unauthorized, or unofficial injections were performed. Trial sample analyses of samples under test are never acceptable. Standard, blank, and placebo trial analyses may be required for equilibration or system verification purposes. These analyses must be labeled appropriately, included with the sample of data set, and distinguishable from the sample analyses.

  These modifications or alterations may go undetected by the Quality Unit. One common root cause may be that the Quality Unit does not have adequate procedures, training, and understanding of how to review original electronic data and metadata, such as audit trails, that track these actions. A poorly configured computerized system includes, but is not limited to, systems where laboratory staff or managers may have administrator-level access that allows them to eliminate failing, atypical, and unsatisfactory results; alter peak areas; change system settings (e.g., date, time, etc.); or eliminate injection sequences. System configuration to ensure data security should be challenged during system validation.

- **Failure to document laboratory records contemporaneously and/or deliberate falsification of manual records:** Regulators have found inconsistencies when comparing laboratory documentation records against the electronic data files (e.g., dates recorded on sample-receiving records are inconsistent with the date stamped on the HPLC chromatograms) as well as failure to document sample/weights, dilutions, standard lot numbers, etc. ***(21).***

- **Performing unreported sample test injections:** This deficiency was cited specifically in four FDA Warning Letters, based on unauthorized testing of chromatography samples outside the quality system. Trial analyses and deletion of data were found to be closely related; specifically, the deletion of data or the failure to configure systems to detect the deletion of data.

- **Failure to validate analytical methods:** This deficiency was cited in two FDA Warning Letters, calling into question the accuracy of any data collected using a test method that had not been validated.

Title 21 CFR 11.10(f) requires that systems enforce the sequencing of steps and events, i.e., each step should be recorded before the next step or event occurs. Complying with this requirement would result in system design (technical and/or procedural) that forces users to record the data for the step (e.g., of processing lab data) prior to the next step (e.g., of processing the lab data again to obtain a second result). Despite this requirement, consultants have found the following examples where processing of data is being performed in temporary memory or data is being buffered and then selectively sent to the database for "permanent recording" after the data set has been sanitized as example issues ***(27):***

- Some standalone instruments (i.e., instruments that are connected to a local computer but not to a network), also sometimes referred to as locally-managed laboratory instrument systems, allow the entire analysis of a sample through to result generation in temporary memory prior to recording (i.e., saving the data into permanent memory). Enabling audit trails (system and method audit trails) should detect these issues, which is discussed in more detail in **Section 6.4.**

- Certain data flows are not being correctly designed in that multiple inputs to LIMS (e.g., weights from balances, KF moisture readings, etc.) are incorrectly entered into LIMS in temporary memory where the user can edit values prior to committing the data to the LIMS database. For example, this would allow persons to alter the weights that would, in turn, alter the moisture results. In the absence of contemporaneous corroborating source data, such as printouts from the balance and KF, this data integrity issue may not be detectable. The data flow should instead be designed to enforce the recording of the weight in the LIMS at the time of the weighing, and prior to the second step of the generation of the moisture reading, etc. Further discussion of the indirect measures to aid in detecting this is included in **Section 6.2.**

These examples are not all-inclusive but are representative of issues uncovered by regulatory agencies during recent inspections and found by consultants during remediation efforts.

4.0 General Considerations for the Control of Data Integrity in the Laboratory

Laboratory data is generated, processed, recorded, and maintained in electronic (also referred to as digital), paper, or manual systems or in a combination of these (hybrid). The following general principles are foundational to establishing robust data integrity:

- Controls should be established to cover the entire data lifecycle from data collection to use in GXP reports and archiving.
- The data lifecycle extends through retention, archival/retrieval, and destruction.
- The data lifecycle should be re-evaluated for risk and the appropriateness of risk mitigation controls every time the laboratory evolves from a manual to a hybrid and/or electronic instrument or experiences a change in the data capture process or the workflow in the laboratory.

4.1 Original Records

Original records include source data and all metadata needed to be "complete" and to allow for full reconstruction of conduct of the GXP activity. Original records for most laboratory systems include source electronic data and any subsets that are printed. Some equipment, such as pH meters and balances, may create a paper printout or static image of electronic reading during data acquisition as the original record. However, electronic records from certain types of laboratory instruments are dynamic records, and a printout or a static record does not preserve the dynamic format that is part of the complete original record ***(2).*** A firm must justify the choice of record (paper or electronic) based on whether the data is static or dynamic. In the case of dynamic data, it is required to maintain electronic records.

Original records include source data and all metadata and must be recorded contemporaneously with the GXP step or event, whether the process and data are manual/paper or automated/electronic. Specific attention should be given to implementing controls that prevent and detect the alteration, corruption, or deletion of the data in temporary memory or transient locations, including proper security and verification of the complete data flow. When reviewing microbiological analysis, it should be understood that the original physical petri plates, contact plates, test tubes, agar strips, and items of these types used during product or environmental testing are not considered the analytical records because the initial results can change over time even during post-analysis storage (even under refrigeration). The visual analytical data after the prescribed time of incubation should be observed (retrieved) from these materials and recorded either manually onto a paper document or into a digital system (e.g., LIMS) without alteration or corruption.

4.2 Human Factors

The reliability of laboratory results can be influenced by the personal and professional background of the microbiologists, analysts, and laboratory technicians who perform these analyses. PDA uses the following definition of human factors: A science discipline that examines human psychological, social, physical, and biological characteristics to evaluate the design, operation, or use of products or systems for optimizing human performance, health, safety, and/or habitability ***(11).*** A full human-factor analysis or explanation of why people intentionally or unintentionally falsify documentation or omit information is not the focus of this technical report, but human factors should not be ruled out when trying to determine the root cause of a breach in the integrity of data or questionable practices that may affect the quality of pharmaceutical drugs produced.

The psychological subset of human factors which may include attitude, perception or reality, religious background, socioeconomic factors, coercion, and fear of persons in positions of authority, etc. are especially challenging to discern in the workplace ***(28).*** A person's developmental history and past life experiences, as well as current/recent stressful events or scenarios, may affect or influence its behavior and decisions. For example, a person experiencing a stressful family situation, loss of a significant one, illness (e.g., depression, anxiety), or undergoing social economic challenges may not have the correct mindset or mental stability to make basic sound decisions. These factors could trigger or pressure a person to engage in inappropriate behaviors or cause careless errors. Therefore, every organization should have the appropriate controls and systems in place that will allow early detection of behaviors or patterns that are not within the expected norm and that may affect the quality of pharmaceutical drugs produced.

One of the roles of regulatory investigators is to determine if a facility is operating in a state of control and in compliance with required regulations. This is done by verifying the integrity of data generated by a firm. Regulators and independent company auditors both evaluate pharmaceutical laboratory practices, among other CGMP aspects, and document data anomalies. However, it would be unreasonable to expect that regulators and auditors will detect all possible forms of data integrity practices that may be occurring in a pharmaceutical laboratory. Breaches in the integrity of data is not limited to one system or area. A review of the literature calls attention to a variety of data integrity problems that have been documented in several pharmaceutical analytical and microbiology laboratories located around the world ***(29).*** In addition to the examples discussed in this report, these published observations can serve as a point of reference and a training tool to assist in identifying where to look when performing a regulatory inspection or an internal audit.

5.0 Data Integrity in the Pharmaceutical Microbiology Laboratory

5.1 General Considerations and Risks

The approaches used to investigate the occurrence of suspected data integrity issues that have recently occurred in a pharmaceutical microbiology laboratory can be challenging and, in some cases, may be very different than those used to evaluate similar occurrences in an analytical chemistry laboratory. Many microbiological methods are performed manually; subsequently, the recorded results are often based on the visual observations by an individual scientist performing the tests.

Listed below are a few examples of regulatory observations, Warning Letters, or other institutional accounts that note data integrity problems associated with microbiological laboratory records. These are only examples and are not intended to be an all-inclusive list of concerns:

- Company failed to record and report reliable and accurate data for the environmental monitoring (EM) results; for example, contamination in Grade A rooms were recorded and reported as having no viable microorganisms present when, in fact, microbial contamination was present. Specifically, the settle agar plates used in these areas were falsely reported as having "no colonies present" but were found to contain 16 colony-forming units (CFU), more than could be reasonably overlooked.
- Company failed to implement an adequate quality assurance system as evidenced by: product sterility test failures that occurred and were not reported, investigated, or documented; five batches of viral harvests that were rejected due to contamination, yet no reports were initiated; and a company practice that product sterility test failure(s) were investigated only if more than one test jar per batch of the first or second harvests failed for sterility.
- Company used a contract laboratory to perform microbiological testing; however, the company audit checklist used to evaluate the suitability of this laboratory was completed by the contract laboratory, not the company, with no follow-up verification.
- Private testing laboratory claimed to have conducted microbiological testing, yet it did not have the laboratory equipment (i.e., incubators) and/or media necessary to perform the analysis.
- Company used an "unofficial" notebook to record microbial contamination in the plant's water system; however, there was no official investigation or documentation regarding the water system contamination with a known pathogen (*Pseudomonas aeruginosa*). [Comment: This type of observation relates to both the microbiology laboratory and operators' behaviors. Periodically, deceptive individuals will use the same technique to mislead, misrepresent, and/or obscure emerging microbial problems in manufacturing equipment that can impact product quality.]
- Company recorded results that the growth promotion test on the media used for simulation studies supported growth meeting the standard set by USP Chapter <71> Sterility Tests when, in fact, the microorganisms did not grow ***(30).*** In another case, filamentous fungi were seen growing in all five spiked media tubes, indicating contamination, yet laboratory records claimed that all five distinct species of microorganisms were actually growing per the USP standard.

Again, while this list is not exhaustive, it does present actual inspection observations made by several regulatory auditors during their documentation of data integrity anomalies in pharmaceutical microbiology laboratories.

5.1.1 Interviewing Analysts

One critical element in conducting an audit for data integrity problems in a microbiological laboratory is interviewing the individuals who perform the QA/QC tests, in particular, the laboratory analysts or technicians. When reviewing analytical results recorded on worksheets or data printouts from the LIMS, for example, it is extremely difficult to detect data that should have been recorded but was not. Much of what analysts learn comes from on-the-job training, yet unofficial dialogue with coworkers or supervisors is rarely captured or documented. For instance, when a senior analyst instructs a junior analyst on how to handle the appearance of "unwanted" microorganisms found growing on analytical petri plates (such as, "Write the numerical count of the suspected colonies on the lid of the petri dish but don't record it on the official worksheet until the supervisor has a chance to review it."), this "unofficial" practice will not be found in the company's standard operating procedures (SOPs). An auditor can best assess the potential for inappropriate practices, first, by verifying the acceptance criteria described in SOPs and, then, by inquiring of the analysts or technicians if they have been instructed to adjust or modify data or divert from the laboratory SOPs in any form. Without conducting such face-to-face interviews, this kind of microbiological data manipulation would be extremely difficult to detect.

5.1.2 On-site Laboratory and Sampling Review

There are several procedural steps when handling, shipping, and storing microbiological samples that can dramatically and negatively impact final analytical results. Specific examples of managing samples that can diminish recovery of microbiological or endotoxin results and, thus, should be avoided through procedures and adequate employee training, are listed below:

- Collecting in-process product or water samples in an inappropriate container that may bind (or remove) a bacterial endotoxin from the sample may later reduce the true level of bacterial endotoxins within that test portion.
- The excessive use of disinfectants to spray the sampling port(s) prior to taking the sample may result in the disinfectant dripping into the sample bottle and reducing the actual bioburden of the product sample. Sampling from the sample ports should closely simulate the common practices performed during routine production operations.
- When using in-line sample collection manifolds for collecting intermediate-stage product manufacturing, the manifold needs to cool down after heat sterilization so it does not kill the microbes collected for laboratory testing.
- Product sample collection bags should not be held directly under a UV light within a storage cabinet. Exposure to UV light will kill the microbes present before the sample collection bags are delivered to the laboratory for testing.
- Microbiological sample bags should not be stored in a freezer or extremely cold refrigerator, which may injure or stress indigenous microbes. Microbial samples should be placed within a controlled environment to preclude any harmful or deleterious impact on the samples; then, analyses should commence as soon as reasonably possible.

Finished products or in-process samples that are undergoing sterility testing in a Class 100 clean room (or isolator) should be disinfected using an antimicrobial solution and a validated contact time. Disinfectant vapors or solution passing through the product packaging or container-closure and into or onto the product prior to sample analysis may prevent or kill microbes in the media-enrichment test environment, which may inhibit recovery of product contaminants. For example, if the product sample was contaminated prior to the package disinfection step, a vulnerable container-closure system prepared with excessive disinfectant would likely result in false negative data. The sample container disinfection process should be included in laboratory qualification studies and the suitability tested to ensure that residual disinfection solution does not alter the integrity of the sample results.

Because microbiological results are not captured in a chromatograph, as with HPLC or GC analysis, opportunities to directly review any anomalies between the raw and recorded data are few. One way to verify the accuracy of the test data documentation is to set aside all available microbial petri plates, broths, identification strips, etc., in a secure area or refrigerator just after they have been removed from the incubator and analysis is complete. A careful review of the raw data against the analytical worksheets or LIMS data entries should reveal any discrepancies and provide an opportunity to catch any problems with either personnel training or equipment recording, and thus improve, laboratory procedures.

Another technique may prove effective in checking data from samples stored in refrigerators and freezers. The original test vessels from completed analyses of all positive samples (in-process or finished product bioburden test results, sterility test results, water testing, EM, personnel, etc.) usually contain microbial isolates. Conducting an inventory of the stored samples can provide a starting point to determine if there are differences between what was actually recovered during sample analysis and the data recorded on worksheets or in the LIMS. While taking inventory of samples stored in freezers and refrigerators, be sure to note the product name, lot numbers, tracking numbers, microbial identification, etc., marked on the exterior of test tubes and petri dishes. This collected information will provide a list that can later be compared to the results recorded on batch records, worksheets, and LIMS. The information gathered from reviewing the stored sample plates and tubes can indicate whether a company's SOPs are effective or if the analysts are following procedures correctly when there are objectionable microorganisms that need to be investigated. If the number and types of actual microbial isolates found from the stored samples do not match those in the company's quality control records, these data integrity issues may be due to intentional misreporting of the data.

5.1.3 Worksheet Review

Microbiology data often relies on less automated recordkeeping that can be manipulated, often without clear traceability to the original record, when recording forms and worksheets are not well controlled or reconciled. In order to cross-check and confirm data in worksheets, entries in linked documentation should be reviewed (e.g., logbooks of equipment, batch records). Control over the issuance of original paper records, forms or worksheets should provide mechanisms that allow the original records to be distinguished from copies and reconciled. An expert microbiologist recommends reviewing analytical worksheets carefully during an inspection for the following indications of possible falsification: (a) lab reports containing more tests than can reasonably be run per day or per week or by an individual analyst; (b) backlogged sample worksheets reviewed and approved as a batch at the end of the month; (c) worksheets completed by personnel not present in the lab the day of the tests; (d) worksheets reviewed and approved by someone other than an authorized reviewer/approver; (e) changes in handwriting or signatures; (f) changes in reporting format, e.g., <1 CFU being replaced by zero; (g) results with counts reported as merely meeting specifications; (h) a change in frequency of OOS result reporting; (i) perfectly filled-out worksheets, indicating a risk that they are a second copy; (j) use of media before it passes growth promotion; (k) missing worksheets or worksheets out of numerical order; (l) discrepancies between investigation reports and worksheets; and (m) results from a single batch reported twice ***(31).***

5.1.4 Contract Laboratories

Companies that do not have the laboratory space, specialized equipment, or capacity to conduct high-volume microbiological analyses may outsource this type of testing to contract laboratories. In such cases, the company is responsible for thoroughly investigating the reputation and quality control performance of any new or unfamiliar contract laboratory with which they engage in a quality agreement. Before signing an agreement, it is recommended that a manufacturer (a) confirm that the contract laboratory complies with CGMP regulations regarding laboratory qualifications and can perform the required compendial testing for microbial recovery and bacterial endotoxins ***(30,32–34);*** (b) conduct an on-site audit; and (c) submit a sample batch for testing to ensure the quality of testing and data integrity. The company may wish to submit a blinded challenge of test samples that should produce OOS results. Documentation that the laboratory management is qualified to interpret microbiological sample results is required, especially if those individuals will be used as subject matter experts for data review or in the event the lab management needs to conduct a laboratory investigation for questionable sample results.

Reports written based on samples tested by a contract laboratory should include complete analytical worksheets from the analysis performed (e.g., raw material, in-process product intermediates, EM samples, water, finished products). All of the original data (including calculations) and all of the positive (growth promotion results) and negative controls used during analysis should be included in the response report as they are equally important to the final product analysis results. The full investigation report of any OOS must also be provided. A certificate of analysis with a summary of the analytical results does not provide all of the information needed to verify sample test data or to satisfy a regulatory audit.

Two laboratory areas that the sponsor or owner company must carefully oversee are: (a) monitoring of source data, including electronic data and metadata, at the contract site, and (b) establishing contractual provisions to ensure the contract site does not delay, deny, refuse, or limit the ability of the sponsor or owner company to inspect their source data. As observed by experienced consultants, some contract sites only allow the sponsor company to review printouts, refusing access to their source electronic data and metadata. Risk-based reviews of critical source data and metadata and reconciliation of source data with reported information is essential for a meaningful data integrity audit.

If a company obtains services from more than one contract laboratory—a common practice, particularly when special laboratory equipment or expertise is needed—it should thoroughly investigate the reputation and quality control performance of each laboratory engaged. Though rare, the possibility exists for a contract laboratory to falsify data or adjust reported analytical results for microbiologically compromised samples, threatening the company's product and reputation as well as patient safety. Another potential risk is that each contract laboratory uses a different microbial identification platform (e.g., genotypic vs. phenotypic) that may generate different species names for the same isolate. This can make it difficult for the investigation of any analytical OOS results to find the true potential source of product contamination with manufacturing EM isolates that may have used yet another type of microbial identification system.

Lending credibility to the concern about the honesty of private testing laboratories is a court case prosecuted by the U.S. Department of Justice for the FDA. In 2008, the FDA brought criminal charges against a private contract testing laboratory that was caught falsifying data for more than 350 sample worksheets. All 350 sample worksheets showed that the laboratory president performed all analytical steps at "1PM" each day. The worksheets indicated that the submitted nutritional supplement product samples were analyzed for yeast and mold. In most cases, the analytical results were made available on the same day the samples were received. The FDA investigators became suspicious of the results on the worksheets because the laboratory had none of the reagents, media, or equipment needed to perform these analyses. The unsuspecting manufacturers that sent their products to this contract laboratory were unaware and failed to detect that these sample results were fraudulent ***(25).***

A challenge that some license holders or product owners may have when auditing contracted facilities is limited access to records or information that may reflect a widespread systemic problem at the contracted site and may go undetected. These challenges should be anticipated early in the business and quality agreement discussions to ensure sufficient access to the appropriate records, procedures, and systems during record audits, especially when dealing with OOS or data integrity events. A dual responsibility exists to ensure that all products will be produced and tested according to the regulatory requirements, especially when regulators see contracted facilities as an extension of a manufacturing operation.

5.1.5 Equipment and Instrument Review

If not handled correctly, a variety of equipment and instruments used in a pharmaceutical microbiology laboratory (e.g., incubators, water baths, pH meters, EM devices, temperature monitoring systems, microscopes) can become the source of a data integrity problem; some of these will be discussed in greater detail later in this section. The general concern is that the results derived from the analyses conducted with equipment and instruments not calibrated or not used properly may generate erroneous results. The three examples that follow describe how the review of quality control shortcomings of laboratory or manufacturing equipment can be critical in detecting erroneous results. Lack of quality control could result in overlooking microbiological conditions or contamination that may compromise manufacturing monitoring and valid product testing.

- When water activity devices are not calibrated or maintained properly, the validity of the analytical data derived comes into question. For example, if the sensing head of a device is not cleaned properly before a subsequent product sample is placed in the chamber, regardless of the reason for the error, the impact on the analytical value of the final product for release or testing may be significantly altered. Whether or not the post-assay data had been manipulated or unintentionally changed, the analytical results may have been compromised, possibly affecting product disposition (good or bad). A full investigation is required to determine the potential impact.
- A laboratory's automated microbial identification system (e.g., Vitek II®, Biolog) generally stores a data file of all the microbial isolates it has identified from all product or environmental microbial isolates tested on it. These identification platforms should have tracking numbers that trace the

origin of the microbial isolate back to the product batch record, LIMS, OOS, investigation reports, or similar data. These microbial identification records can be used in an audit to verify the accuracy of the associated paper trail should there be any question of transparency.

- The dates for when instruments are unavailable due to needed repair or calibration are usually maintained in a logbook or digital spreadsheet. Comparing the records of nonfunctioning or absent laboratory equipment that might have been used for analysis against the microbiological worksheets may detect potential data integrity problems. The risk for using uncalibrated or nonfunctioning laboratory equipment is greatest when the workload becomes heavy or when tight deadlines are imposed. On the surface, this may appear to be a quality control issue; however, it can become a data integrity concern depending on the level of disrepair or calibration of the instrument used and the ultimate impact on the analytical results.

5.2 Testing for Environmental Monitoring, Sterility, and Bacterial Endotoxins

5.2.1 Environmental Monitoring Equipment

Some of the equipment used most frequently in the pharmaceutical microbiology laboratory and manufacturing facility are environmental monitoring (EM) devices used to collect volumes of air or surface contact from specific rooms (e.g., ISO-5 manufacturing areas used for filling sterile products or sterility test suite used to analyze finished drug products labeled as sterile). The neglect or mishandling of EM devices can cause misleading or incorrect analytical results about the microbial presence (bioburden) within the room being monitored.

5.2.2 Air Sampling Devices

In general, an air sampling device requires that a petri dish or a specifically designed plastic strip containing nutrient agar be placed into the device; the instrument is then turned on to draw a specific volume of air into contact with the agar surface. At the end of the air sampling dwell time, the petri dish or strip along with any captured microorganisms are removed from the device and placed in an incubator. Subsequently, the number of growing microorganisms on the media is counted. Examples of where data integrity problems can occur with air sampling devices include:

- **Visualization of the Petri Dish.** Signs of agar impingement and/or colonies growing within the agar medium, caused by the directed air being drawn into the device onto the agar surface, should be visible, ensuring that the agar petri dish was placed into the air handling device during the initial room setup or at another time, when appropriate.
- **Clogged Samplers.** Over time, the narrow opening of the EM sampler that funnels the air directly toward the turning petri dish will become clogged, essentially preventing the full volume of air to impinge on the agar surface. Though a maintenance or operational anomaly, this directly impacts the data integrity of the microbial evaluation of critical work areas. Routine cleaning of the device in that narrow opening is essential to ensure data integrity for this equipment.
- **Quality Control Logbook.** As with other laboratory equipment, recording if or when any of the air sampling devices are defective or out of service in the quality control logbook is essential. The dates during which a piece of equipment is listed as "out of service" would not be found in the sample batch records.
- **Settle Plates.** When settle plates are used to passively monitor the manufacturing or laboratory environment, plates located near surfaces directly exposed to UV light during monitoring may not be suitable. UV light may kill viable airborne microbial contamination, resulting in questionable results. Settle plates exposed too long become desiccated, and unwrapped settle plates exposed within an isolator during vaporized hydrogen peroxide (VHP) or other decontamination steps become unable to support growth. In either case, potentially viable airborne microbial contamination may not be recovered during exposure.
- **Final Counts.** Any manipulation or adjustment of final microbial counts without sound scientific justification, such as subtracting colony counts near the edge of the petri plates or the number of bacterial colonies appearing at the beginning time period for air sampling plates, is a concern for data integrity **(Figure 5.2.2-1).**

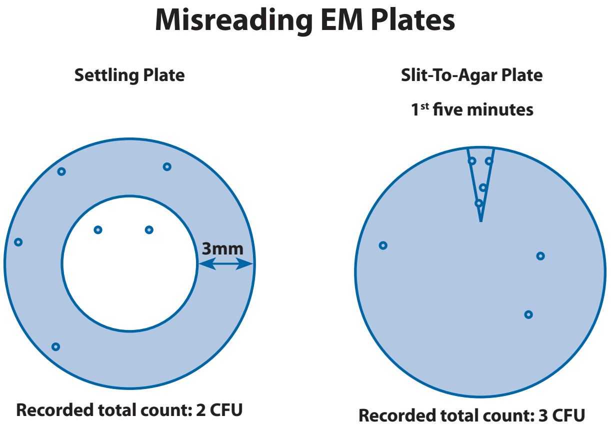


Figure 5.2.2-1 Misreading of EM Plates

5.2.3 Surface and Personnel Monitoring Equipment

Disinfectants should not be applied to a work surface or on an operator's gloved hands prior to sampling those surfaces using replicate organism detection and counting (RODAC) plates. Application of a disinfectant to a surface designated to be monitored before the test is performed will change the results of the assay, making the surface appear to be free of microorganisms or producing a lower bioburden. The manipulation of procedural requirements can obscure the reality of a contaminated facility or a person's poor aseptic technique resulting in the manufacture of a drug product under conditions that adulterate the finished product and impact patient health. Data integrity detection may need to occur at microbiological recovery stages long before an analyst opens the incubator door and transfers the tubes and petri dishes for colonies to be counted, otherwise, the data may be compromised and meaningless. In some cases, the surface monitoring is not done correctly, e.g., too short a contact time or performed improperly (for instance, only the finger tips are sampled but the fingers are not correctly rolled over the agar, or fingers are overlapping the plate).

5.2.4 Review of Sterility Test

The laboratory methods employed to conduct a sterility test on finished sterile pharmaceutical drug products or medical devices are delineated in international pharmacopeial sterility test chapters such as USP <71> ***(30).*** There are two analytical choices: (a) passing the aqueous product through a membrane filter to collect the potential microorganisms recovered from its contents, followed by rinsing to remove residual antimicrobial preservative(s) contained in the product; or (b) adding the product directly into the enrichment media. The essential step before employing these validated compendial procedures is to run a product suitability test in the presence of a set of required QC microorganisms to ensure that, under the test conditions, the product ingredients do not interfere with the recovery and growth of these challenge QC microorganisms. The design of the suitability test establishes the procedures used during routine testing to provide scientific proof that the method will work under routine product-testing conditions.

When the sterility test is properly performed as described in the compendia, and after determining the product suitability with that method, data integrity problems can result if sample handling and product testing is significantly altered or mismanaged from the approved SOPs. The following are risks for data integrity breaches in sterility testing:

- Before product containers (units) are transferred to the sterility testing suite or HEPA-filtered laminar flow hood, the outside of each container is usually subjected to a disinfection procedure: sprayed or wiped with a sporicidal solution to decontaminate the exterior of the container, preventing surface contamination from being transferred into the testing area. Any overexposure to the disinfection solution may penetrate the package or container and kill potential product contaminants before the sterility test is performed. This critical analytical step for certain product types (e.g., medical devices, combination products), if performed incorrectly, can result in a "false negative" sterility test that would allow the release of a potentially contaminated lot of parenteral or implantable products. This data integrity problem may not be obvious on a laboratory worksheet or detected in LIMS because the destruction of potential microbial results would have occurred before the product was tested.

- In a pharmaceutical microbiology laboratory, the preparation of the media and reagents used during sterility testing is an important step, which should be performed carefully to avoid mistakes. For instance, when analyzing products by the "direct inoculation" approach, the accidental use of a lower volume of test medium may create an inhibitory growth condition due to a higher concentration of the product or preservatives in the test medium compared to those levels proven acceptable during the suitability test. The early detection of low volume test tubes can be missed when the tubes are located in the middle of the holding rack.
- One observation that has been documented on several FDA Form 483s occurs when the membrane filter is transferred to the enrichment broth, or when a powdered product is added directly to the medium, and the membrane filter adheres to the top of the inner portion of the test tube above the liquid medium **(Figure 5.2.4-1).** This problem has been traced to the use of short, four-inch forceps rather than the recommended 10- or 12-inch forceps that may not allow the transfer of the membrane filter into the broth. A similar mishap may occur when hygroscopic powder products adhere to the neck of the inner tube, preventing the product from entering the enrichment media and allowing potential product contaminants to grow **(Figure 5.2.4-2).** A third example, documented during the inspections of contract laboratories performing sterility testing on sterile medical devices, involves ineffectively cutting up long catheters or complex devices, preventing the product from contacting the enrichment broth. The portions of the product protruding from the liquid broth may be the regions of the device that contain the indigenous microorganisms **(Figure 5.2.4-3).**

These examples reflect testing conditions that may have gone unrecorded or unobserved by a reviewing supervisor; however, their occurrence may result in false negative data to the final recorded laboratory result. The prevention of problems in the pharmaceutical microbiology laboratory that affect data integrity may need to be fixed at stages before observational or data entry is recorded on a worksheet or in LIMS.

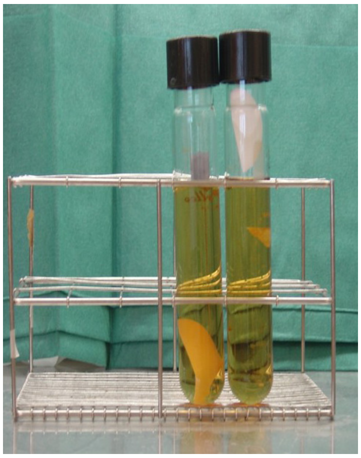


Figure 5.2.4-1 Membrane Location

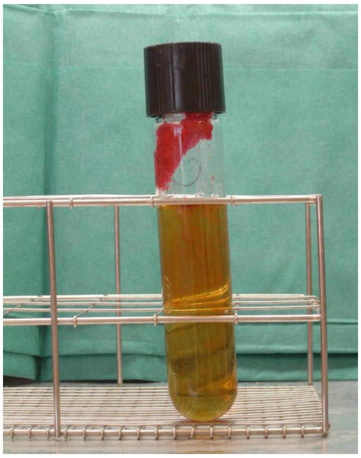


Figure 5.2.4-2 Hygroscopic Product

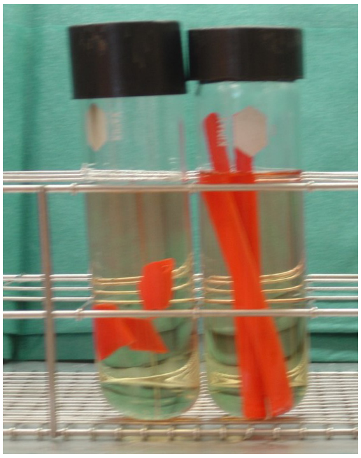


Figure 5.2.4-3 Device Placement

5.2.5 Bacterial Endotoxin Testing

The bacterial endotoxin test (BET) described in compendial test chapters is an enzymatic assay that employs the reagent *limulus amebocyte lysate* (LAL) along with a vial of controlled standard endotoxin (CSE). The CSE serves as an artificial, laboratory-derived source of bacterial endotoxin that can be used to perform the suitability test (inhibition/enhancement test); it is also employed as a positive control to ensure that incubation conditions during product testing have not been compromised. The BET can also be conducted using a gel clot procedure or with the use of a spectrophotometer, employing a modified version of the LAL reagent ***(34).*** Each of these reagents requires careful handling and storage, the directions for which are clearly stated in the product's package instructions.

To minimize potential data integrity problems with the final laboratory test results, when performing the BET method for finished product testing of pharmaceutical drugs or medical devices, there are a few critical parameters that need to be understood, satisfied, and documented:

- During product container storage (refrigerated or at room temperature), when vial or ampoule samples containing aqueous solutions are delivered to the laboratory, the indigenous bacterial endotoxin may form micelles or attach to the glass or rubber stopper surfaces and move out of the solution. Unless the laboratory SOP for performing the BET on aqueous products includes a mixing step prior to removing the test aliquot, the detectable level of endotoxin determined by the assay will be underestimated and may inaccurately portray the product's endotoxin unit value within specifications. Consequently, the final analytical results could be impacted, even when using a validated and properly controlled assay, depending on the outcome of a formal investigation ***(35).***
- An allowable amount of bacterial endotoxin (as defined in the pharmacopeial product monographs) may be present in a drug product based on its dosage, route of administration, and total amount of endotoxin delivered, e.g., within a one-hour dosing for an injectable product. A well-designed BET method requires that the maximum valid dilution (MVD) be calculated before the assay is performed. If it is not calculated precisely, with the formula variables and the units used in the MVD formula, an incorrect value may result. The data integrity problem may occur if the calculated MVD value is higher than the true number. That would make it possible to run the assay at a higher product dilution, creating a testing situation where unacceptable levels of endotoxin may be present in the product but released without detection. Since endotoxin contamination can have dire patient consequences, this is a crucial data integrity matter.
- In a U.S. Department of Justice criminal prosecution brought by the FDA involving a fraudulent and contaminated hormone product, the drug manufacturer submitted the bacterial endotoxin analytical data as part of the laboratory evidence. The FDA laboratory detected levels of bacterial endotoxin in the vials used for product rehydration above USP specifications. The drug manufacturer employed a private laboratory to test the same suspect lot for bacterial endotoxin and reported the levels of bacterial endotoxin detected as below the compendial specification. Laboratory records showed that the analyst for the private lab manipulated the product dilution to avoid detecting the actual level of endotoxin in the product. The analytical report had been tailored to give a finished result with an endotoxin level below the USP allowable limit. The FDA laboratory, however, performed the full range of product dilutions to avoid missing the actual endotoxin contamination level. The FDA's test data proved the contract laboratory had manipulated the dilution to produce false results for their client. This example illustrates the need to both understand the analysis procedure and recognize how it can be manipulated.

6.0 Data Integrity in the Analytical Quality Control Laboratory

6.1 General Considerations and Risks

Manual and electronic data generated within the analytical quality control laboratory (chemical and physical testing) should be maintained and reported in a manner that ensures compliance with CGMP, as well as with the FDA's measure of being attributable, legible, contemporaneous, original, and accurate (ALCOA) ***(2).***

This compliance is accomplished through the implementation of robust controls, beginning with the establishment of policies and procedures aligned with regulatory requirements, and a data governance process that ensures the data for health products are reliable enough to make a case in court ***(36).*** Factors affecting data integrity include risk-based governance of laboratory data processes; appropriate validation of test methods; controls on the computerized system; and training and education of analysts, reviewers, and individuals involved in the testing or review of laboratory testing operations.

Some firms have implemented a laboratory data governance manual as one way of addressing the complexities within an analytical QC laboratory. A document of this type can be used as a roadmap, guiding the user through the manual and electronic data governance processes in place from the point of sample receipt to the time of data reporting. Associated equipment, logbooks, and procedural controls can be referenced and the overall laboratory flow for samples and data can be outlined. Flowcharts of various analytical equipment data handling and/or processes can be presented for quick reference and verification to evaluate the quality and data integrity risks. Flow charts are also useful in applying principles of quality risk management as noted in ICH Q9 ***(37).***

In order to understand data integrity risks within the laboratory, it is important to understand the types of data being generated and the systems in place that impact and control data integrity. The associated data acquisition processes may range from simple systems to complex: simple systems, where data is recorded manually; hybrid systems, where the equipment or instruments generate both source electronic data and a paper printout of the data; and complex systems, where all the data is generated, processed, recorded and maintained electronically. Original records include source data and all metadata and must be recorded contemporaneous with the GXP step or event, whether the process and data are manual/paper or automated/electronic. When source data is generated electronically via an analog signal and then converted to a digital signal and/or transferred from a source system with limited storage capabilities, such as a mobile device, or to a storage database, such as an electronic data capture, then end-to-end data process governance and verification controls must ensure that what is stored in the database is a complete and accurate copy of the source data and all metadata and allows for full reconstruction of the data process. Specific attention should be given to establishing controls that prevent and detect the alteration, corruption, or deletion of the data in temporary memory or transient locations, including proper security and verification of the complete data flow ***(27).***

6.2 Hybrid Systems

A hybrid system refers to analytical equipment for which both electronic and paper documentation combine to build the record. Analytical balances, autotitrators, polarimeters, dissolution apparatus, and pH meters, for example, are instruments managed by firmware that provide paper records. Per MHRA, balances and pH meters without software are considered simple systems ***(5).*** To comply with regulatory requirements, a firm must ensure that the original data generated is retained and/or that the record archived represents a true copy of the data ***(2).***

Several models of the above-listed equipment (balance, auto titrator, polarimeter, dissolution apparatus, and pH meter) with various functionalities are available in the market. Equipment with features including software, audit trail functionality, and storage capacity along with equipment with firmware, without electronic audit trail storage capacity, are considered analytical laboratory computerized systems (ALCS). For example, if a laboratory uses a balance connected to a computer or with integrated software, this balance qualifies as ALCS (discussed further in **Section 6.3)** and is not in the scope of hybrid systems. As shown in **Figure 6.2-1,** simple systems with or without analytical data storage capability are both considered to be hybrid systems.

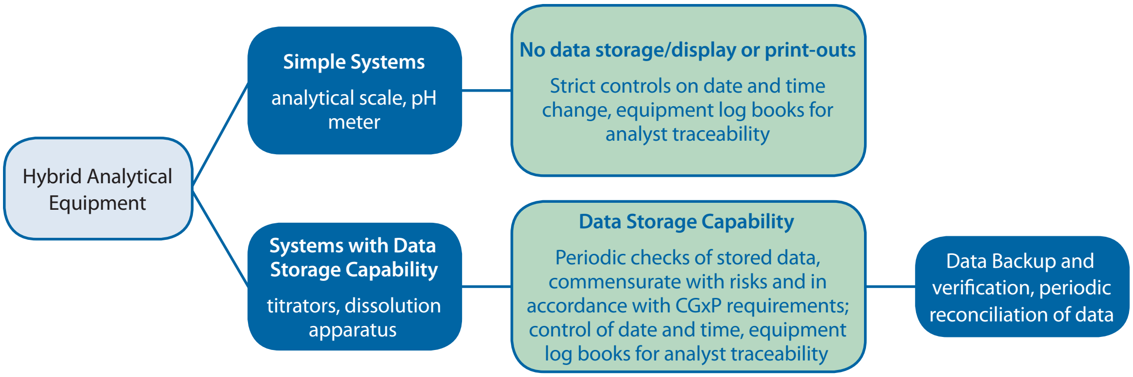

Hybrid Analytical Equipment
Simple Systems
analytical scale, pH meter
No data storage/display or print-outs
Strict controls on date and time change, equipment log books for analyst traceability
Systems with Data Storage Capability
titrators, dissolution apparatus
Data Storage Capability
Periodic checks of stored data, commensurate with risks and in accordance with CGxP requirements; control of date and time, equipment log books for analyst traceability
Data Backup and verification, periodic reconciliation of data

Figure 6.2-1 Data Flow in Hybrid Analytical Systems

6.2.1 Hybrid Systems—Associated Risks

The major risks associated with data integrity in the data governance of laboratory hybrid systems should be monitored by quality personnel on a regular basis and include, but are not limited to, the following:

- Lack of traceability for all the data generated (lack of password control, lack of audit trail capability and/or intentional inactivation of audit trail, and vulnerability of date and time to manual change)
- Lack of understanding of the functionality and available features
- Lack of second-person review
- Testing into compliance or duplicate prints of the same record
- Poor restoration, backup, or single-point failure (hard drive)
- Lack of controls to retain source electronic data and data that is "complete" and includes all metadata, which may be due to access to the computer clock, recycle bin, and data files in operating system files
- Lack of adequate second-person verification that printed data is a true copy of original data or a representative summary of the source electronic data, including all metadata and results

Many of these risks also occur in full electronic systems if adequate controls are not in place.

6.2.2 Hybrid Systems—Qualification

Most vendors provide a standard validation protocol defining the functional criteria and controls of the hybrid system. The firm's Quality Unit is responsible for ensuring that these controls, validation criteria, and instrument operational qualifications are properly understood and implemented. If required, the Quality Unit should implement company-designed controls to govern the intended use of the system. Please note that all types of data have the potential for manipulation, particularly in CSV text or PDF format. Some additional examples of limitations that should be checked are:

- **Data format and storage capacity.** The data storage format, limits, and storage capacity should be known to identify possible risks, e.g., data that is not stored in its original format, or can be formatted in "CSV," "Unix code formatter," or saved as a spreadsheet or PDF. Systems with insufficient data storage capacity may result in data being overwritten or not saved.
- **Data backup and archival capabilities.** The process of data backup, archival, and retrieval of data should be controlled and tested. Ideally, backups will be automated to eliminate errors and/or incomplete data transfer.
- **Cross-platform data capabilities.** The requirements for viewing, printing, or analyzing data on a computer should be known and tested, e.g., if the data is stored in CSV text or PDF format, it may be viewed directly. Most data (such as Karl Fischer equipment for measuring moisture) may require installation of a specific software program to store and interpret this data; in that case, software validation may be required, and the software should be checked for additional features, such as data compatibility with commonly used software (e.g., PDF generators and spreadsheets).

- **Data integrity when copied to computer.** If data or results are being copied to a computer, the possibility of data manipulation must be tested to define the controls and limitations for data copying and printing; for example, if the data is stored in spreadsheet format, the date and time of acquisition, identity, result, etc., might be open to manipulation.
- **Data handling.** If an analytical instrument (e.g., balance) does not have the functional capability to store and manage the data or the critical metadata, the printed data may be considered as the original record, only when that record is a complete and accurate copy of the complete data and metadata generated by the instrument. Firms engaged in the manufacture and testing of pharmaceutical products who process information electronically should have laboratory equipment that meets CGMP standards for the processing and maintenance of electronic data. The entire end-to-end data handling process, from the point of generation of the electronic signal in the source system through to final decision-making based upon this source data, needs to be assessed for data integrity risks and designed to reduce these risks through a combination of appropriate technical and procedural controls. The Quality Unit is ultimately responsible for ensuring that appropriate procedures are in place for storing and protecting electronic records and restricting access to those files. One best practice is to identify an independent system administrator with specialized expertise to be responsible for storing and protecting electronic records.
- **Results output.** The results from hybrid systems (pH meters, balances, and titrators) should be printed with date-and-time stamp, raw data, metadata, measurement values, sample identity, batch number, file names, and calculated values.
- **Backup and data review.** For hybrid systems that are not connected to computers, ideally a report (event log) can be printed (meaning published in PDF) with every analysis or, at least, printed periodically. Publishing or viewing event logs may not always be possible on hybrid analytical equipment; therefore, data integrity should be ensured by periodic Quality Unit checks for date and time breaches, data breaches, weights-on-results calculations vs. analytical scale printouts, checks against the timing of other instruments, and periodic data reconciliation (results stored on the instrument vs. recorded in an equipment logbook). Any breach in data or of established laboratory criteria should be investigated according to laboratory SOPs and applicable regulatory guidance.
- **Data lifecycle management.** Periodic data backups, if applicable, should be implemented and archived. Archived data should be stored according to Quality Unit procedures. Archived data is generally stored off-site and should be checked for ease of data retrieval. Backup data should be more readily accessible.

Deficiencies that have been cited in FDA Warning Letters include:

- Investigators found that laboratory analysts did not document the balance weights at the time of sample weighing. Specifically, sample weights used in calculations were created after the chromatographic runs ***(38).***
- A review of the Karl Fischer electronic records revealed an OOS result that was not reported. The passing results reported on the data sheets were generated from another sample tested an hour after the initial OOS results were obtained on the same day ***(39).***

6.3 Analytical Laboratory Computerized Systems (ALCS)

This section describes instruments that are connected to computers for data acquisition, analysis, and storage. Typical examples are HPLC, GC, particle-size distribution analyzers (PSD), ultraviolet spectrophotometry (UV-Vis), infrared spectrophotometry (IR), and X-ray diffraction instrumentation (XRD). The system includes the hardware, software, and operating platform as well as manuals, SOPs, and trained analysts.

Although some laboratories currently maintain data generated from ALCS on the validated computer connected to the instrument, best practice is to maintain such data on a qualified server for increased security. Procedures should be established for the following:

- Lifecycle management of the data collected, detailing the roles and responsibilities of the personnel operating these systems
- Definition of quality oversight for the system administrator role, including access levels, roles, and periodic review of actions. To avoid any real or perceived conflict of interest, administrator privileges best be assigned to an individual who is not involved in laboratory activities. Also, any changes to administrator roles or privileges should be documented with Quality Unit oversight and approval.
- Controls to prevent raw data from being overwritten, manipulated, or deleted without detection by enabling audit trails
- Controls to verify detection (i.e., audit trail functionality) and accurate documentation to support any investigations (e.g., if a system audit trail has been turned off for any reason, it should be associated with proper justification)
- Verification of the original, approved, validated state of the system
- Systems to recover and review data in-progress when an automated process has been interrupted (either manually or automatically)
- Consistent names for files, file folders, and file paths of storage locations of electronic data
- Demonstration that each step or event, such as processing of data to generate a result, is recorded at the time of the step or event and before the next step or event, such as reprocessing data

Suggested controls to prevent and detect possible data integrity breaches include:

- SOPs that require unique user identification and password; user types and permissions; registration and configuration of new systems; creation of folders to manage the hierarchies of data; and designation of who will perform backups/restores and how often, who can create and adjust methods, who can optimize methods that can be changed, who can create data, who can approve and review data, who can determine what should be reviewed, and who can archive data when it is "completed"
- Protocol that restricts users from changing the system date and time
- Protocol that restricts permission to delete any kind of data to the responsible users who need it, e.g., restricting part of data archival procedures to only the independent administrator
- Procedure that allows only authorized personnel to access the application/operating system or install software updates and only under the appropriate change control by an authorized person independently approved by the Quality Unit to ensure system validation is preserved
- Security policies that configure and restrict access to data via the operating system to ensure maintenance of data integrity, including internet access
- Dedicated network or server for analytical systems (recommended)
- Automatic operating system updates must be disabled; only scheduled updates by IT personnel should be enabled
- When an analytical test run has been interrupted for any reason (e.g., power outage or equipment malfunction), appropriate documentation and a record of the event up to the point of interruption should be maintained, along with an assessment of the possible impact
- Mapping of end-to-end data process for the ALCS to identify and mitigate data integrity risks and identify opportunities for future improvements
- Procedure requiring periodic data and audit trail reviews

In addition, any computer system attached to analytical equipment should not be accessible for general purposes, such as generating SOPs or checking email. Personal mobile devices also should not be permitted to be connected to analytical equipment to avoid infecting the computer with a virus and causing it to crash. **Figure 6.3-1** illustrates one example of a typical data flow and configuration which includes a remote data center. In a smaller laboratory setting, the configuration could be much simpler with a desktop connected directly to the chromatography instruments. Some configurations do not use temporary storage but send raw data directly to the data center/file server. The system configuration will determine how audit trails are established and reviewed, which is discussed in greater detail in **Section 6.3.9.**

6.3.1 Qualification of Computer Server and/or Virtual System

Software verification provides objective evidence that the design output of a specific phase of a software development lifecycle will meet all the requirements for that phase of the application's development. Software verification looks for consistency, completeness, and correctness of the software and its supporting documentation.

Typically, an ALCS is designed to run on a local computer or, often, several ALCS could be connected to a centralized server. That server could be hosted from another building, from a remote site, or from a third-party hosting site, often referred to as a virtual system or "Cloud" system. Whether the server is housed locally or in the Cloud, the requirement exists that the server must be qualified to demonstrate that it is fit for use and able to support the software in a compliant environment related to all applicable regulations. Testing this premise of control is an expectation from all major health authorities.

The intended functionality of the server must be qualified to ensure data transmitted, processed, and maintained is as accurate as the originally generated data, and that the audit trail capabilities remain enabled to ensure authenticity and integrity of the electronic data. Network mapping, fitness for intended use, and functional testing are basic criteria for any server qualification. The levels of control

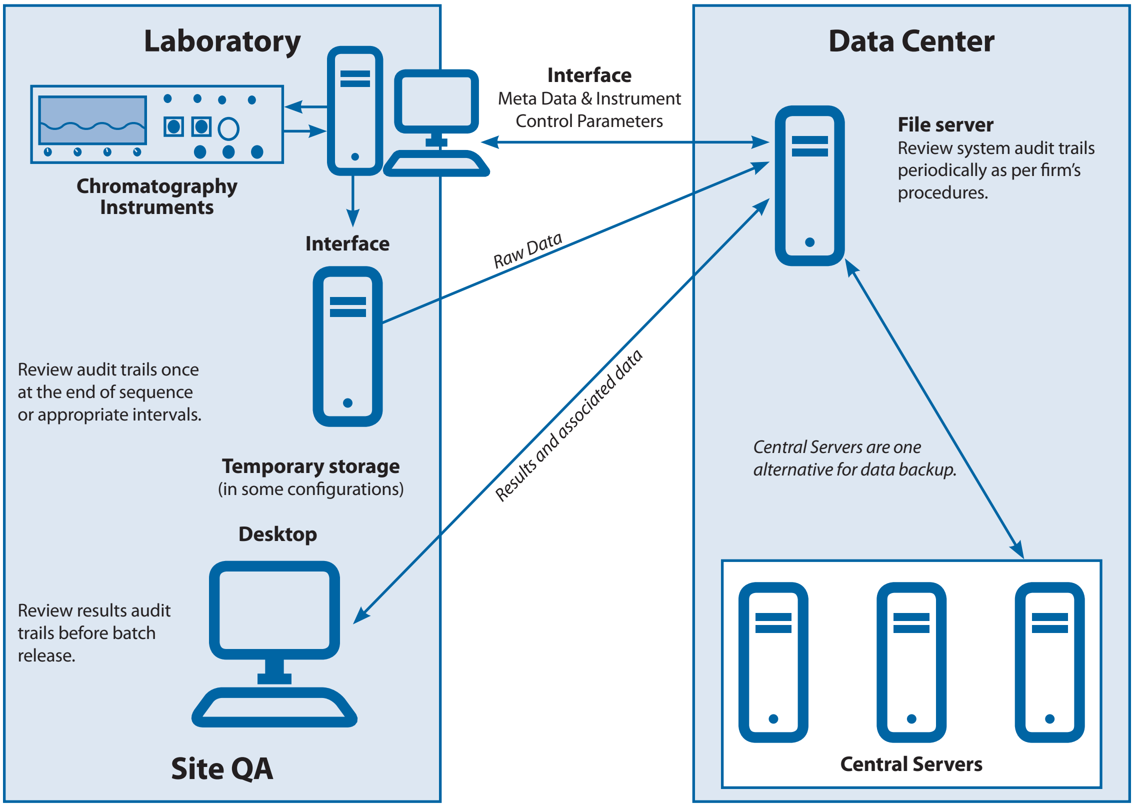

Laboratory
Chromatography Instruments
Interface
Interface
Meta Data & Instrument Control Parameters
Review audit trails once at the end of sequence or appropriate intervals.
Temporary storage
(in some configurations)
Desktop
Review results audit trails before batch release.
Site QA
Raw Data
Results and associated data
Data Center
File server
Review system audit trails periodically as per firm's procedures.
Central Servers are one alternative for data backup.
Central Servers

Figure 6.3-1 Sample Data Flow and Audit Trail Points in an ALCS

should be the same as those for computer system qualification. The following are recommended components of server qualification:

- Assign the system a unique identification number
- Locate the server in a secured environment
- Restrict access to the physical location of server
- Document the operating system details and version number
- Qualify the server for its intended use and controls that prevent misuse
- Map the network and perform functional testing
- Define the periods to update applications, operating system, and antivirus software
- Control remote access appropriately (e.g., maintenance or system upgrades)

As a result of Cloud technology, software-as-a-service (SaaS) is becoming a common offering by software vendors. An SaaS environment offers pharmaceutical companies many benefits; however, they must understand that, ultimately, as the end user, the pharmaceutical company is responsible for the appropriate use and the control of this technology. Consequently, a detailed service level agreement (SLA) between the SaaS hosting company and the end user is needed to clearly define the roles and responsibilities of each party particularly to satisfy each regulatory requirement. Such an agreement details information about the vendor, the physical and logistical security of the facility, and the security of the firewall and firewall monitoring for possible cyberattack. It should also include any other elements to ensure the environment is well controlled for the application's use, including data backups, application response times, and support response times. Appropriate metrics that can be used to monitor the SaaS hosting company's ability to meet the established expectations of the SLA should be maintained. Both companies should devise a contingency plan to ensure against loss of data in the event of network outage, hardware failure, or a cyber event and conduct a routine and detailed audit of the SaaS application and the hosting environment at a frequency determined based on risk. The ultimate responsibility remains with the pharmaceutical laboratory, including the review of audit trails, backup logs, change controls, and system administration controls to assure that only appropriate users are accessing the system.

A clear advantage for the use of SaaS applications is that, typically, the buyer can use much of the vendor's documentation for installation qualification (IQ) and operational qualification (OQ) and the vendor provides test scripts for the standard out-of-the-box functionality. This may reduce the documentation required by the company buying the services to test unique features or user-defined configurations. When the application is ready for use, the end-user company performs the user acceptance testing that certifies the system meets the agreed-upon requirements and is fit for use in the company environment. It is important to note that this approach does not alleviate the regulatory requirement for the end user to assure a compliant use of the system.

Pharma companies (end users) can also host the company-owned regulated systems in a third party's Cloud environment. This scenario allows a third party to run a company's application in a virtualized server in the third party's data center. The regulated company must still assure compliance in the third party's environment, but this allows the regulated company to focus more on its own core business rather than staffing the complex environment of a regulated data center.

As with an SaaS system, a detailed SLA must be established with the third party's data center detailing information about the vendor, the physical and logistical security of the facility, and the security of the firewall and firewall monitoring for possible cyberattack. The agreement should include any other elements that ensure the environment is well controlled for the application's use. The end-user company should devise a contingency plan to ensure against loss of data in the event of network outage or hardware failure and conduct a detailed audit of a Cloud system and application vendor at least once a year. As with SaaS, the end-user company should perform user acceptance testing of the vendor's application hosted in the vendor's Cloud to certify that the application is fit for use in the company's environment ***(7)***.

Additional information on Cloud and SaaS qualification can be found in the Control Objectives for Information and Related Technologies (COBIT) framework created by the international professional association ISACA as a good practice for information technology (IT) management and IT governance ***(40)*** and in ITIL® (Information Technology Infrastructure Library) books, a set of widely accepted best practices for IT service management for business ***(41).***

Several different health authorities have published guidances and regulations that set out their expectations for system qualification and software validation. Consensus standards are also available in some areas. **Table 6.3.1-1** provides a cross-reference of key terms related to automated systems and the regulations, guidances, or standards that specify the expectations.

Table 6.3.1-1 Key Terms and References for Automated Systems Requirements

Reference Term	FDA Part 11 *(6)*	FDA Part 820 (42)	EU Annex 11 *(7)*	ICH Q7 (43)	WHO DI (Draft) *(3)*	ISO 13485:2016 *(44)*	GAMP 5 *(45)*	GAMP 5 and IT Infrastructure and Control *(45)*	COBIT 5 Reference *(40)*	MHRA 'GXP' Data Integrity Guidance and Definitions *(5)*
Audit Trail	Part 11.10(e)		Section No. 9	5.43	5.4; 13.7; 6.6				BAI07	6.13
Change and Configuration Management	Part 11.10(k)	820.70(i)	Section No. 10	5.43; 5.47	8.6; 13.6	4.1.6	Appendix M8 and O6	6.1	BAI06	6.16; 6.17.2; 6.19
Data Backup	Part 11.10(c)	820.180	Section No. 7.2	5.48	5.4; 11.2; 13.3; 13.7		Appendix O9		DSS04	6.17; 6.17.2
Data Encryption									DSS05	
Data Exchange	Part 11.10(h) Device checks		Section No. 4.8				Appendix D7		BAI07	
Disaster Recovery					3.2; 13.11		Appendix O10		BAI07 DSS04	
Electronic Media Management					14.2				DSS06	
Incident and Problem Management				5.46	11.2; 13.12		Appendix O4		DSS02, DSS03	
Infrastructure Monitoring						6.3		6.11 Appendix10	DSS01	
Network Connectivity									DSS01	
Periodic Review	Part 11.300(b) & (c); Part 11.10(k)		Section No. 11	12.60	13.12	7.2.2	Appendix O8	Appendix 4	MEA01	6.2; 6.15; 6.17.1

6.3.2 Commercial Off-the-Shelf Software Validation for HPLC, GC, and other Instrument Operations

Most commercial off-the-shelf (COTS) software includes formal, structural testing and a compliance certificate from the vendor, who has the proprietary source code. Once the system is installed, the purchasing laboratory must configure the equipment, define roles and responsibilities, and confirm operation in its environment. Validation must be completed on-site for the intended use. Part of the validation may include verification and/or audits that the vendor has performed adequate testing prior to shipping the software.

Software validation is often referred to by regulators as "confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses, and that the particular requirements implemented through software can be consistently fulfilled" ***(46).*** In practice, software validation activities may occur both during and at the end of the software development lifecycle to ensure that all requirements have been fulfilled. A conclusion that software is validated is highly dependent upon comprehensive software testing, inspections, analyses, and other verification tasks performed at each stage of the software development lifecycle.

Validation documentation should include evidence of verification by the system owner, or Quality Unit, of the following:

- Vendor has performed adequate testing prior to shipping the software
- Intended functionality of software in terms of analysis, data acquisition, processing, reporting, tracking, and security
- Software name, configuration, and version number
- Compliance of audit trail(s) that meets 21 CFR Part 11 requirements
- Logic/basis for the algorithms used in calculations (e.g., USP tailing, ASTM peak integration)
- Common statistical calculations used by the software (such as mean, standard deviation, and % relative standard deviation), as well as complex statistics (such as residual error, regression, and slope) calculated manually and compared with software values
- Data transmission checks of the computer, the server, and the interfaces between the two (to verify what happens with the server, network unavailability, and local PC unavailability) are essential to ensure data transmitted has not been manipulated, altered, or corrupted during the transmission phase. The compatibility of COTS software with the laboratory data management software being used, such as laboratory information management system (LIMS), electronic laboratory notebooks (ELN), and enterprise resource planning (ERP), is also important to ensure the integrity of the electronic data.

Additional details on validation planning and lifecycle management can be found in *Validation of Chromatography Data Systems* by Robert McDowall ***(47).***

6.3.2.1 Controls for COTS Software for HPLC, GC, and Other Instrument Operations

The following are the minimal controls needed to safeguard COTS software and secure its use:

- Identifying the person(s) responsible for installing updates
- Addressing any changes to software through change control procedure with risk assessment
- Setting up secure individual user log-ins and periodic change of passwords
- Disabling data modification, deletion, or copying by anyone other than the administrator
- Restricting data deletion to only the authorized system administrator following established procedures, with oversight by the Quality Unit
- Maintaining a detailed, QA-approved list of roles and responsibilities and copies of previous versions of software when updating to allow reviewing, processing, audit trail review, backup/restore testing, and reporting of older reports in case of regulatory requirements and investigations (recommended)
- Establishing periodic review of control effectiveness based on the risk posed, paying attention to software upgrades and patches, and taking appropriate remediation and/or mitigation actions
- Maintaining a detailed list of roles, responsibilities, and access privileges for all the software in the laboratory

6.3.3 Laboratory Instrument Functionality and Qualification

Risk assessments to be executed during the initial qualification of laboratory instruments should identify various controls to manage risks, including data risks, at an acceptable level and should be challenged upfront. Necessary periodic checks and/or system controls would be identified at the same time.

Qualification of laboratory instruments and any features or functionality that may compromise data should be verified, for example:

- Date and time stamp function should be enabled either in the instrument or on the computer attached to the instrument, but analysts should not have the option of modifying the date and time stamp functionality
- Analysts should not have the authority or capability to disable the audit trail feature
- Some instruments are manufactured with built-in memory and a computer that can also be connected to an external computer; the system owner should clearly define the role of such computers without compromising the data generated on those instruments

6.3.4 Data Governance — Generating, Processing, Reporting, and Archiving

Any features or functionalities that will enable data generation should be checked for how they function without connecting to computer (e.g., samples injected prior to the official test). Analysts should not have the authority to conduct independent trial or pre-sample injections, and system suitability/equilibration procedures should be defined in method validation/procedures. FDA Warning Letters have cited companies for performing these types of testing prior to the official test. As per USP <621>, no sample analysis is acceptable unless the suitability of the system has been demonstrated ***(48).*** If the system suitability test fails, the results should be documented and handled according to the firm's SOPs; in this case, adjustments can be made, and a system suitability test can be repeated. Procedures should be designed, however, to prevent trial injections in quality control analysis. FDA has found trial injections of official samples included in a few company SOPs and has determined that the practice is not acceptable. Regulators have also found trial injections conducted with samples masked or identified as standards, that when reexamined, were found to be samples and not standards.

Regulatory authorities prohibit pre-testing samples with the goal of obtaining a favorable or specific result prior to testing the official or reportable sample, or to overcome an unexpected/unacceptable result (e.g., testing different samples until the desired passing result is obtained). This practice, also referred to as "testing into compliance," is not consistent with CGMP. In some situations, actual samples have been used to perform system suitability testing as a means of testing into compliance. Regulatory authorities consider the practice of using an actual sample in test, prep, or equilibration runs as a means of disguising testing into compliance and deem it a violation ***(47).***

Modern chromatographic software has the capability of acquiring data until the point a chromatographic run is intentionally or unintentionally interrupted. Any such instances that are cited as "system crash/equipment unplugged" or "miscommunication" without documented justification may not be accepted by regulatory agencies. These instances should be properly investigated and documented. Companies should evaluate this software capability as a part of qualification of new equipment. It is also recommended to evaluate this for existing analytical equipment where available.

6.3.5 Data Generation

The Quality Unit should have clear procedures and qualified personnel to meticulously define data governance in the organization. Appropriate written procedures should be in place and should be followed to ensure all data generated by the laboratory is reliable and accurate. The moment an injection is made, or signal processing starts, the data file is deemed to be generated. The following are the criteria or characteristics that define a data file:

- Analyst's name
- Name of product
- Description of sample
- Date and time stamp
- Method parameters (wave length, flow, injection volume, and run time, at a minimum)

Figure 6.3.5-1 depicts the typical data flow in chromatographic analysis. The following conditions should be defined in the laboratory procedures and any deviations investigated:

- When the data file can be treated as raw data
- What to do if a run aborts before completion
- How to handle transmission loss from analytical equipment to connected computer
- What to do if power is lost between chromatographic runs
- Protocol for renaming of data file after signal acquisition
- How to identify willful acts to compromise data using any of the above methods

6.3.6 Injection Sequences

Analyzing several samples at one time is a common practice in analytical laboratories, where samples are queued by a set of commands or "sequences." The Quality Unit should approve the software system architecture and the defined rules for creating and executing sequences; controls and permissions for renaming files after acquisition; controls on modifying method parameters during sample execution; and copying or moving data files. Where possible, these rules should be incorporated into the system architecture. Renaming a file to mask or hide the identity of a trial or pre-sample injection is not an acceptable practice.

In addition, the following controls are recommended to capture such events in an audit trail:

- Name/number of sequence
- Analyst's name
- Name of the product
- Reason for modification
- Description of the method for each sample
- Review or clearance by a second analyst before execution of sequence (suggested)

The following conditions also should be listed in the functional requirements and defined in laboratory procedures and any deviations should be investigated:

- Modification or execution of partial sequences
- Acceptable situations to abort a sequence and to maintain a track of aborted sequences
- Modification of the method parameters after initiating the sequence
- Criteria for adding a sample to a sequence after initiation
- Handling transmission loss from analytical equipment to the connected computer
- Managing power loss between chromatographic runs
- Controls on sample trial injections, system check injections, or single injections
- Controls to identify willful acts to compromise data using any of the above situations

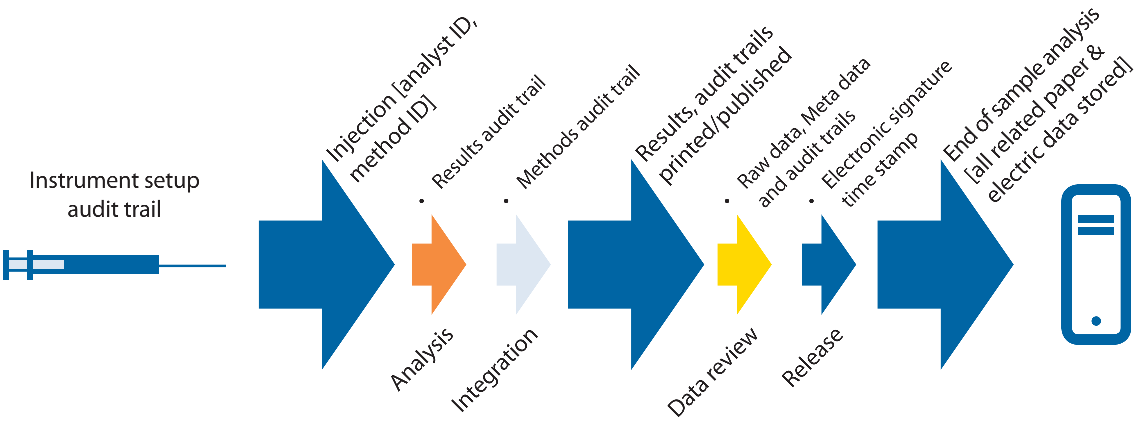

Instrument setup audit trail
Injection [analyst ID, method ID]
Analysis
Results audit trail
Integration
Methods audit trail
Results, audit trails printed/published
Data review
Raw data, Meta data and audit trails
Release
Electronic signature time stamp
End of sample analysis [all related paper & electric data stored]

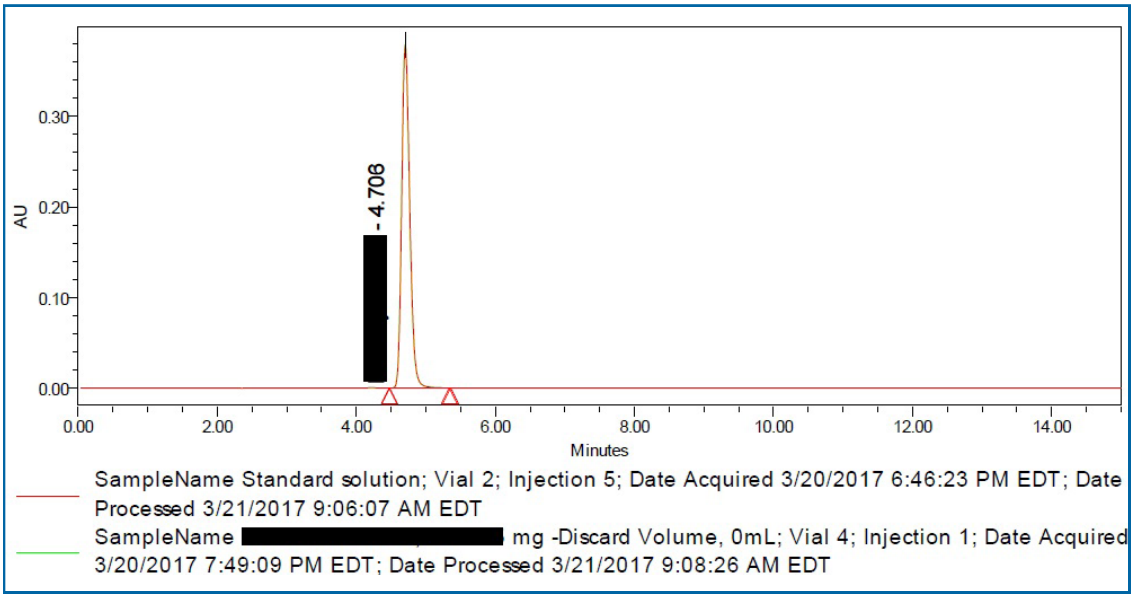
Figure 6.3.5-1 Typical Data Flow in Chromatographic Analysis

6.3.7 Data Processing and Peak Integration

Chromatographic software uses dynamic peak detection algorithms and automatic peak detection algorithms. Integrating the chromatograms using software to apply the integration events, such as peak width, threshold, height, and area, etc., and then visually observing the peak integration for its correctness is generally recommended. The inherent or analytical variations and combination of various factors can result in non-Gaussian peaks and drifting baselines in which the auto-integration will either underreport or overintegrate the peak areas.

Once acquired, the electronic raw data of the measurements (measured values and metadata) are stored and available for processing. Some acquired electronic raw data already represent usable results (e.g., weight, temperature, and humidity). Other acquired electronic raw data, such as intensity values correlated with time or wavelength and generated by chromatography or spectroscopy, require further processing to obtain usable results (e.g., retention times, peak areas, and amounts). These processes, such as integration and calibration, are defined by processing parameters or calibration factors and affect only the resultant data after processing, but not the acquired electronic raw data. In contrast to the acquired electronic raw data, the processing parameters, such as integration events and calibration curves, may be changed during data evaluation. The changed processing parameters, methods, and processed data should be identified by versioning (i.e., number of times reprocessed) either on the results or from the audit trail data ***(25).***

Integration events should be defined through standard algorithms, and metadata and should be associated with respective raw data files. In such cases, the analyst adjusts the integration events to obtain proper peak integration. As chromatography is a comparative technique, the consistent integration events should be applied for the entire set of chromatograms, as much as possible, or published along with the chromatograms. **Figure 6.3.7-1** represents an overlaid chromatogram of the standard and a sample (of the same concentration) integrated with the same integration events. Integrating small peaks, closer peaks, negative peaks, drifting peaks, and peak-to-valley requires time and skill. Integrating peaks manually is not recommended and should be avoided to the extent possible.



SampleName Standard solution; Vial 2; Injection 5; Date Acquired 3/20/2017 6:46:23 PM EDT; Date Processed 3/21/2017 9:06:07 AM EDT

SampleName [redacted] mg -Discard Volume, 0mL; Vial 4; Injection 1; Date Acquired 3/20/2017 7:49:09 PM EDT; Date Processed 3/21/2017 9:08:26 AM EDT

Figure 6.3.7-1 Typical Overlaid Chromatogram of Two Injections (Standard and Sample) Integrated with Same Integration Events

QC laboratories should have procedures in place that require authorization to perform manual integration and for procedures to track such events to avoid unnoticed or unevaluated cases that may affect the accuracy of the results. PDA defines manual integration as a process used by a person to manually integrate the peak height or area by modifying the baseline of the chromatogram with use of chromatographic software. The conditions and circumstances when manual integration would be allowed should be predefined (e.g., complexity of the sample matrix). Generally, a good chromatographic data system would be able to render consistent and reliable baselines for an overwhelming majority of injections within a chromatographic run. When consistently bad chromatographic peaks and baseline issues are encountered, having good documentation should not be the only way to address the issue. In this circumstance, the goal should be to improve the system and ensure that the data generated is reliable and consistent.

The Quality Unit should define standard protocols for processing data to include the following, which may be instrument- or application-specific:

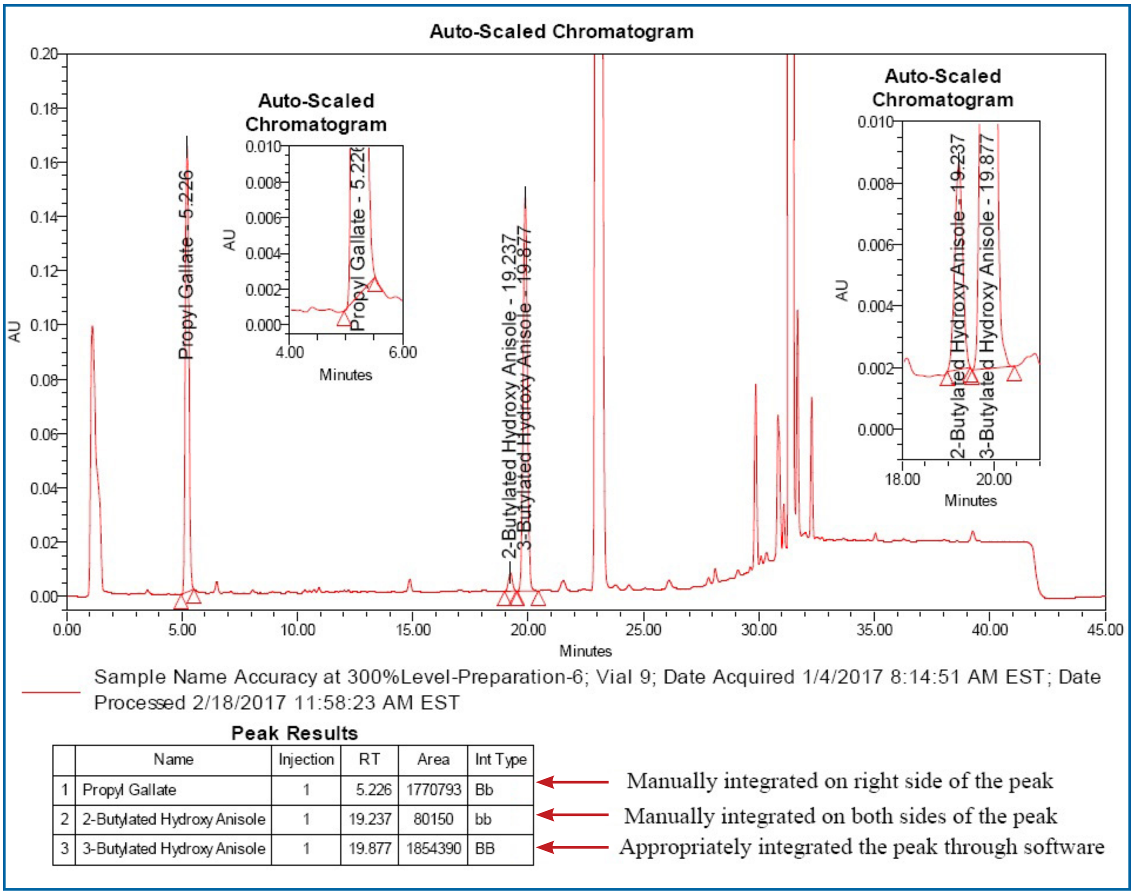
- Reprocessing peaks
- Applying instrument/application-specific integration events/algorithms
- Fully integrating peaks
- Inhibiting or disregarding any peaks in the test chromatogram (e.g., blank peaks, placebo peaks, solvent peaks) without scientific justification; examples where justification is needed include counter ion and reagent interactions with a sample
- Applying the same integration events for all samples in the sample set or sequence and justifying any change in integration events

Peak integration is the process used by a chromatographic system to determine the peak height and width and obtain the quantitation of the peak of interest. Certain USP monograph methods specify inhibiting integration at specified zones in the chromatographic run. USP <621> states that peaks can be disregarded by setting the thresholds in the integration to at least half of those below reporting threshold ***(32).*** Therefore, utilizing the built-in capability of the chromatographic data acquisition software to inhibit integration of peaks from solvent, mobile phase, placebo, and counter ions in impurity analysis is a common industry practice. Firms should scientifically evaluate and judiciously determine whether to use the inhibit integration functionality. Peaks in the chromatographic analysis may be excluded in the event of a known abnormality. Unknown peaks should be integrated and investigated according to the firm's quality procedures.

Manual integration is the process used by the analyst to integrate the peak height or area by modifying the baseline of the chromatograph using software ***(49).*** Manual integrations may be required for R&D and biological labs. Though in QC labs, manual integration may be necessary or acceptable only under special circumstances (e.g., complex chromatography due to sample matrix interferences, poor resolution, co-elution of peak of interest, problem with the baseline, or software with limited capabilities); however, manual integration is not generally acceptable for assay. Manual integration should not be left to an analyst's discretion; it should be performed only according to an approved procedure, with documented approval from a supervisor and results appropriately documented. A mature quality system will review these instances as part of continual improvement of methods and equipment. Modern chromatographic software identifies and displays manually integrated peaks. **Figure 6.3.7-2** represents a model chromatogram with manually integrated peaks and software integrated peaks.

Printed chromatograms should be presented in visible scale as per the respective analysis (peak top visible for assay or single analysis, peak base clearly visible for purity analysis). After integration, results may be published or electronically stored. If results are reprocessed, permission from a supervisor is required. Those types of events may be noted in a log (paper or electronic) for quick reference.

Figure 6.3.7-3 illustrates a chromatogram in proper scale and visibility to determine the proper integration. Common practice across the industry is to present a visible and clear baseline for multicomponent analysis and the entire peak for single-peak analysis.



Sample Name Accuracy at 300%Level-Preparation-6; Vial 9; Date Acquired 1/4/2017 8:14:51 AM EST; Date Processed 2/18/2017 11:58:23 AM EST

Peak Results

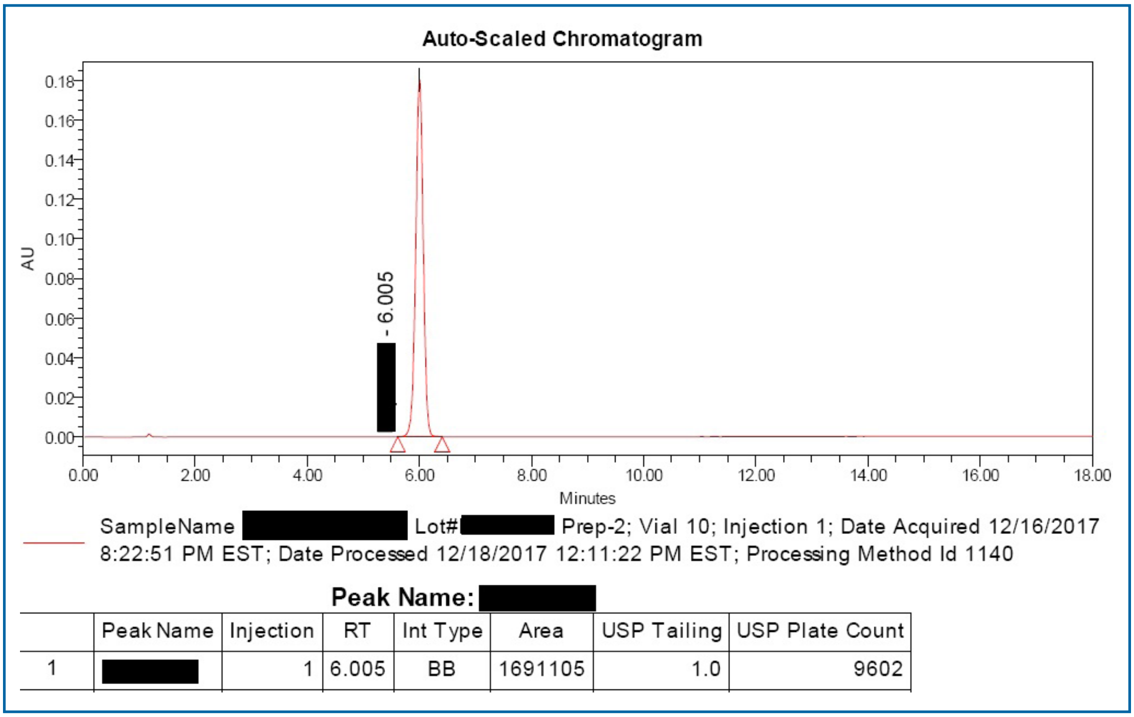
	Name	Injection	RT	Area	Int Type
1	Propyl Gallate	1	5.226	1770793	Bb
2	2-Butylated Hydroxy Anisole	1	19.237	80150	bb
3	3-Butylated Hydroxy Anisole	1	19.877	1854390	BB

Manually integrated on right side of the peak

Manually integrated on both sides of the peak

Appropriately integrated the peak through software

Figure 6.3.7-2 Typical Chromatogram with Integration Type (Manual/Chromatographic Software)



SampleName [redacted] Lot# [redacted] Prep-2; Vial 10; Injection 1; Date Acquired 12/16/2017 8:22:51 PM EST; Date Processed 12/18/2017 12:11:22 PM EST; Processing Method Id 1140

Peak Name: [redacted]

	Peak Name	Injection	RT	Int Type	Area	USP Tailing	USP Plate Count
1	[redacted]	1	6.005	BB	1691105	1.0	9602

Figure 6.3.7-3 Chromatogram with Appropriate Integration Events

Figure 6.3.7-4a represents the chromatogram printed in large scale, where peak integration is not visible. **Figure 6.3.7-4b** represents the same chromatogram with printed proper scaling, where peak trimming and missing peak integrations are visible, revealing possible intentional data manipulation.

Assay analysis, dissolution, and content uniformity involve a single analyte/peak analysis where the content will be calculated against a known standard. Gaussian peaks, with allowed system suitability characteristics of accuracy and precision, are expected in these types of analysis. Normal Gaussian peaks should be integrated exactly where the peak starts and finishes. The peak integration represented in these types of analysis is illustrated in **Figures 6.3.7-5a-f.**

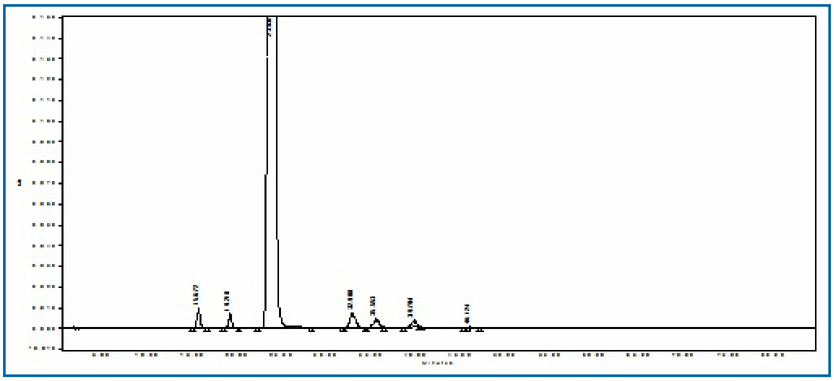


Figure 6.3.7-4a Chromatogram of Related Substances Analysis Presented with an Improper Scale

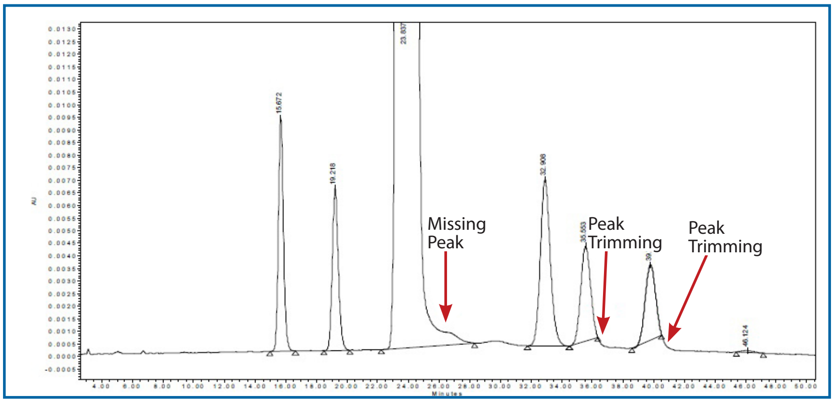


Figure 6.3.7-4b Chromatogram of Related Substances Analysis Presented with Appropriate Scale

Improper Integration

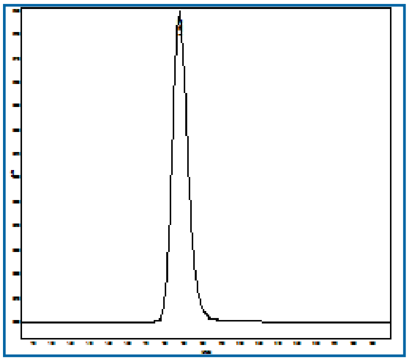


Figure 6.3.7-5a Raw Data of a Single Component Analysis before Integrating

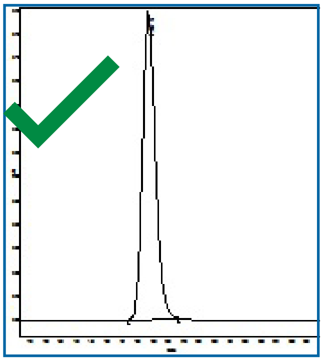


Figure 6.3.7-5b Raw Data Integrated with Proper Peak Width and Threshold

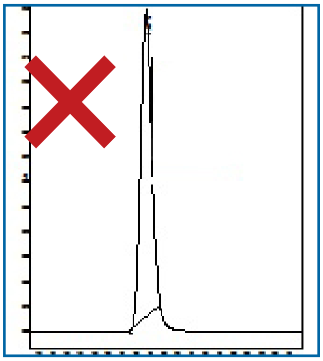


Figure 6.3.7-5c Raw Data Integrated with Improper Integration Events Leading to Peak Trimming

Figure 6.3.7-5a is the unprocessed signal of a single component analysis. **Figure 6.3.7-5b** represents raw data integrated with proper integration events and displayed in visible scaling. **Figure 6.3.7-5c** represents the peak integrated by trimming to yield low area. (Associated risk: Reporting fewer peak areas leads to less assay or dissolution or lower content values.) **Figures 6.3.7-5d–f** represent the raw data integrated with improper integration events, which presents more area. (Associated risk: Reporting more peak areas leads to more assay or dissolution or higher content values.)

Data manipulation of chromatograms by manually manipulating the integrated peaks is one factor the FDA has cited in Warning Letters ***(50–53).*** In these illustrations, all the integrations presented are made through chromatographic software by adjusting integration events. Chromatographic software will indicate which peaks are manually integrated. Laboratory management should have appropriate controls in place for detecting the data compromises made by applying the wrong integration events.

Figures 6.3.7-6a–c and Figures 6.3.7-7a–c show integration errors that occur for multicomponent analysis (peak groups), such as related substances analysis/chromatographic purity analysis. In both cases, fewer peak areas will be reported.

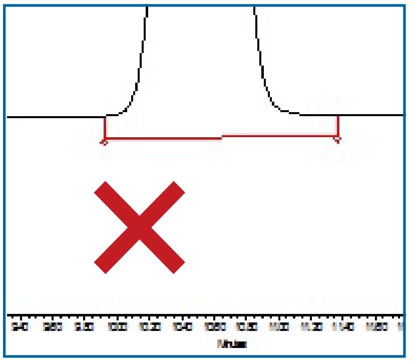


Figure 6.3.7-5d Raw Data Not Integrated Base to Base

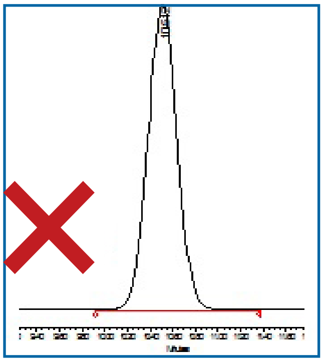


Figure 6.3.7-5e Raw Data Integrated with Peak Tailing

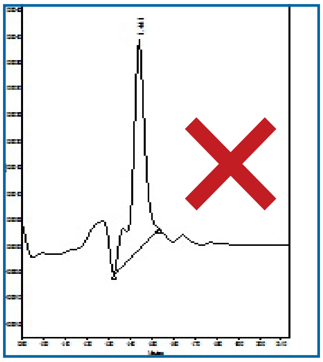


Figure 6.3.7-5f Raw Data Integrated Peak Followed by a Negative Peak or Drift

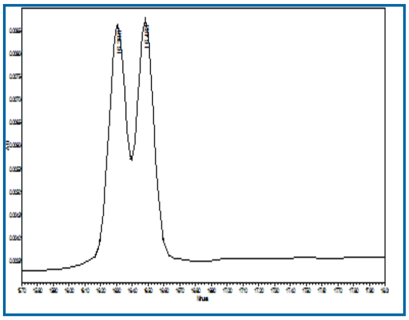


Figure 6.3.7-6a Raw Data of Co-eluting Peaks of Related Substance Analysis

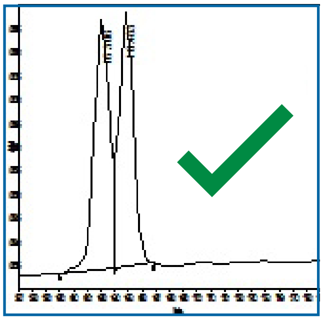


Figure 6.3.7-6b Co-eluting Peaks Integrated with Suitable Peak Width and Threshold

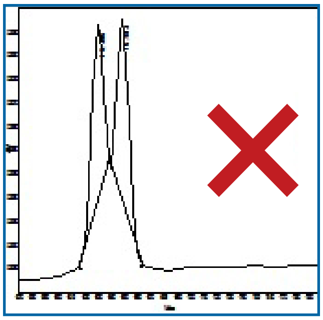


Figure 6.3.7-6c Co-eluting Peaks Integrated with Improper Integration Events, Presents Less Response

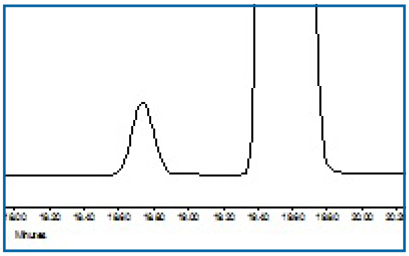


Figure 6.3.7-7a Raw Data of Multicomponent Analysis

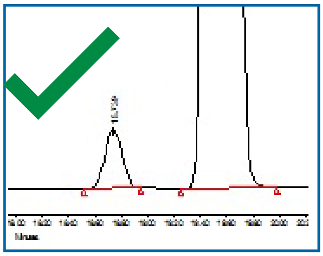


Figure 6.3.7-7b Multicomponent Peaks Integrated with Suitable Peak Width and Threshold

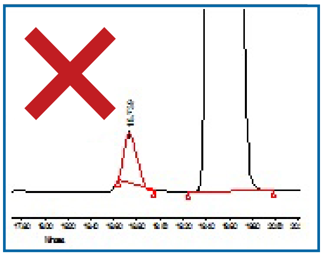


Figure 6.3.7-7c One Peak Integrated with Peak Trimming and another Peak by Integrating Tailing, Fronting

6.3.8 Results Printing or Publishing

Some software packages use the term "printing" to generate a final result; in this case, printing does not mean output to paper form. Printing, or "publishing," refers to the next step in generating output once testing is complete. In a well-configured system, the results after this step are final and may not be changed without reprocessing. Reprocessing must be governed by procedures and software that is correctly configured and should require a comment or justification. Before publishing, the supervisor or Quality Unit should review the results, according to established laboratory procedures. Though printing results on paper is not an ideal practice, some firms still use this approach, often due to limited software functionality or limited resources. The following items or reports should be generated, through publishing or software functionality, after each analysis and made available in the system for review:

- Sample sequence
- Instrument method
- Integration events/processing method
- Results (chromatograms)
- Results audit trail (if available)
- Sequence audit trail (if available)
- Method audit trail (if available)

The results should include the following criteria:

- Analyst's name and signature
- Date and time results were processed
- Results audit trail, method audit trail, and sequence audit trail
- Chromatograms presented in visible scale per respective analysis (peak top for assay or single-analyte analysis, peak base for purity analysis)

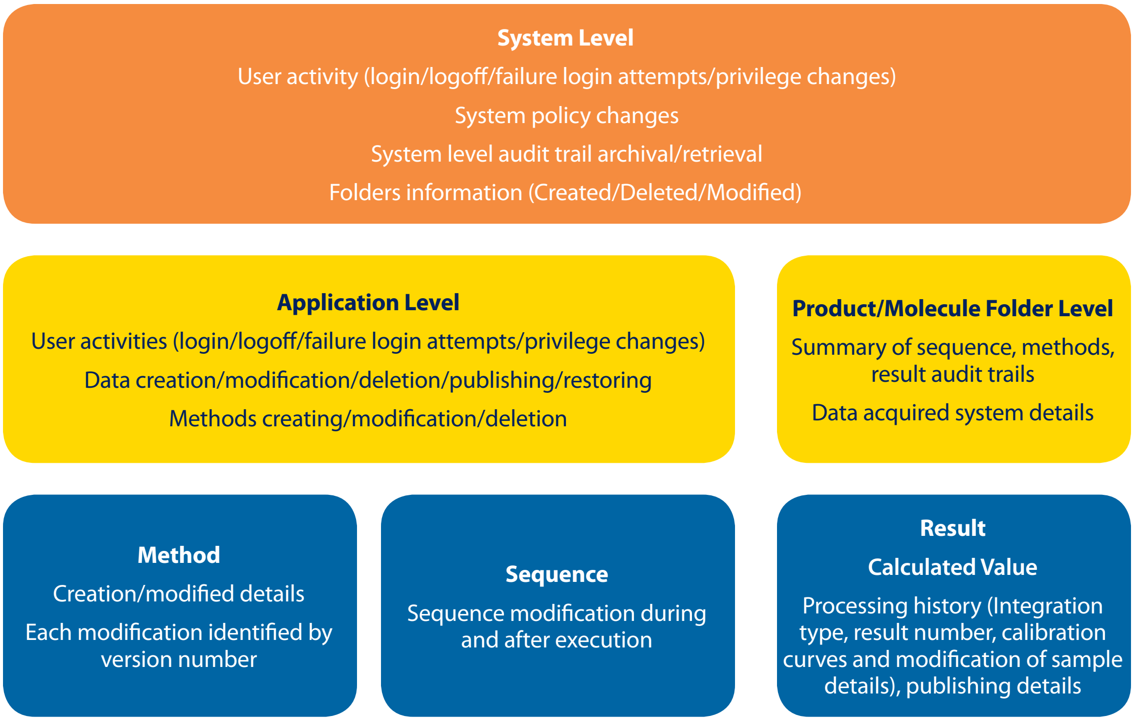
6.3.9 Audit Trails

An audit trail is a chronology of the "who, what, when, and why" of a record. It ensures a secure, computer-generated, time-stamped electronic record is available that allows for reconstruction of the course of events relating to the creation, modification, or deletion of an electronic record. For example, the audit trail for an HPLC run could include the user name, date and time of the run, integration parameters used, and details of reprocessing, if any, including the change justification. In addition, as part of reconciliation, the injection log can be included, but this injection log does not include audit trail injection information (blank/system suitability/Lot#) ***(2).***

The audit trail feature (or function) should be enabled at all times, with strict access controls in place; equipment with data processing capability but lacking audit trail capability should be upgraded to CGMP standards. In those instances where the equipment lacks such capability, appropriate controls (e.g., paper-based) should be implemented to ensure all data and information generated, along with the history of all activities performed, is available for review.

The audit trail should include all possible data changes; then, the reviewer can decide whether any data change represents a compromised or regulated event.

Different types of audit trails supply data on different functions; each should be assessed individually and, then, all audit trails should be assessed collectively to determine the integrity of the data. Instrument-specific software provides several fields for configuring audit trails, and templates from which to choose for presentation. **Figure 6.3.9-1** illustrates one approach to audit trail classification.



System Level
User activity (login/logoff/failure login attempts/privilege changes)
System policy changes
System level audit trail archival/retrieval
Folders information (Created/Deleted/Modified)

Application Level
User activities (login/logoff/failure login attempts/privilege changes)
Data creation/modification/deletion/publishing/restoring
Methods creating/modification/deletion

Product/Molecule Folder Level
Summary of sequence, methods, result audit trails
Data acquired system details

Method
Creation/modified details
Each modification identified by version number

Sequence
Sequence modification during and after execution

Result
Calculated Value
Processing history (Integration type, result number, calibration curves and modification of sample details), publishing details

Figure 6.3.9-1 Example of an Audit Trail Summary

The Quality Unit is responsible for enabling fully functional audit trails, assessing the different kinds of metadata captured, and choosing which fields are required to verify and ensure data reliability and compliance. This approach should be carefully selected with a view to design the most appropriate procedures for batch release as well as a sound periodic review. The following list reflects one recommended approach to the various classifications of audits, each of which are discussed in the sections below:

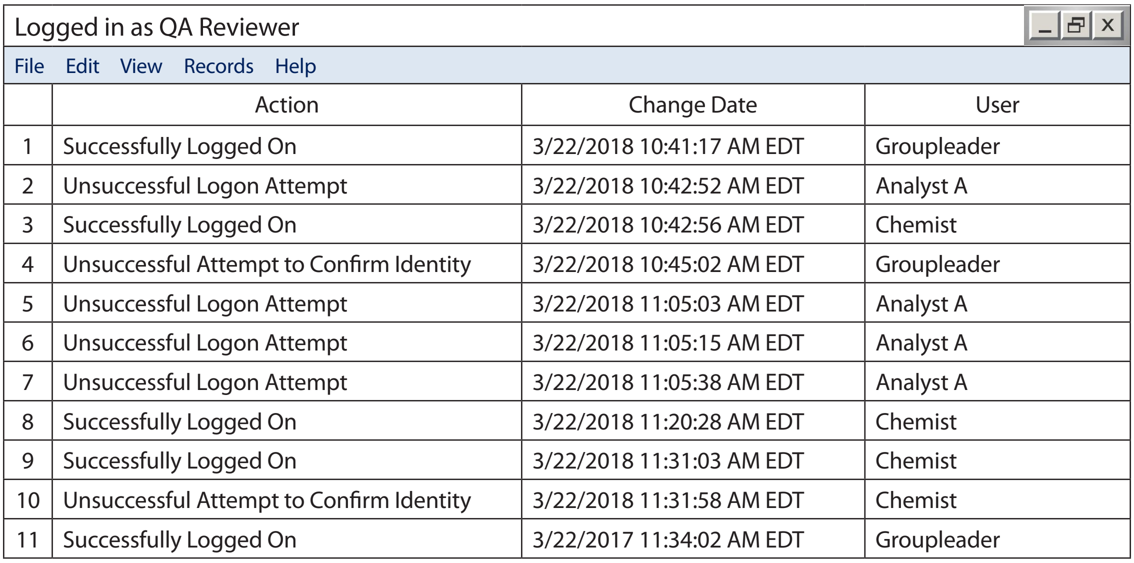
- System-level audit trail
- Application-level audit trail
- Method audit trail
- Results audit trail (or injection audit trail)
- Sequence audit trail
- Transaction log/system error log

6.3.9.1 System-Level Audit Trail

If a system-level audit capability exists, the audit trail should capture, at a minimum: any attempt to log in, successful or unsuccessful; ID, date, and time of each login attempt; date and time of each logoff; device used; and function(s) performed while logged in, i.e., applications that the user attempted, successfully or unsuccessfully, to perform, as shown in **Figure 6.3.9.1-1** ***(2).***

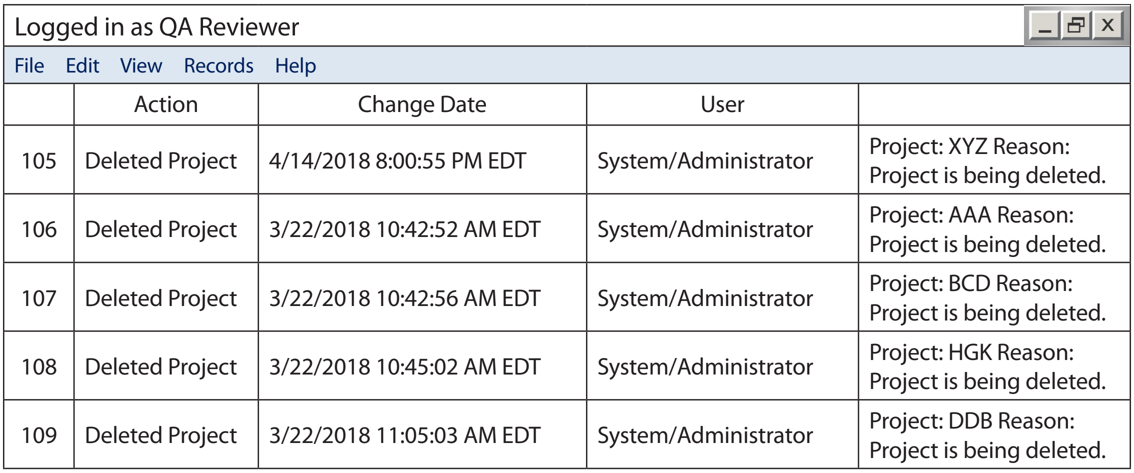
System audit trails cover the activities related to system policy changes, user activities (login, logoff, unauthorized logins and user privileges changes), changes to projects (creating, deleting, modifying and restoring), verification of project integrity and changes to systems. The Quality Unit should review system audit trails on a periodic basis established by the firm for any type of deletions.

Figure 6.3.9.1-2 displays a typical system audit trail for project deletion**.** System audit trails are reviewed in investigations to check the login and logoff times as well as any system-based information that is not captured on application-level audit trails ***(2).***



	Action	Change Date	User
1	Successfully Logged On	3/22/2018 10:41:17 AM EDT	Groupleader
2	Unsuccessful Logon Attempt	3/22/2018 10:42:52 AM EDT	Analyst A
3	Successfully Logged On	3/22/2018 10:42:56 AM EDT	Chemist
4	Unsuccessful Attempt to Confirm Identity	3/22/2018 10:45:02 AM EDT	Groupleader
5	Unsuccessful Logon Attempt	3/22/2018 11:05:03 AM EDT	Analyst A
6	Unsuccessful Logon Attempt	3/22/2018 11:05:15 AM EDT	Analyst A
7	Unsuccessful Logon Attempt	3/22/2018 11:05:38 AM EDT	Analyst A
8	Successfully Logged On	3/22/2018 11:20:28 AM EDT	Chemist
9	Successfully Logged On	3/22/2018 11:31:03 AM EDT	Chemist
10	Unsuccessful Attempt to Confirm Identity	3/22/2018 11:31:58 AM EDT	Chemist
11	Successfully Logged On	3/22/2017 11:34:02 AM EDT	Groupleader

Figure 6.3.9.1-1 System Audit Trail (Default)



	Action	Change Date	User	
105	Deleted Project	4/14/2018 8:00:55 PM EDT	System/Administrator	Project: XYZ Reason: Project is being deleted.
106	Deleted Project	3/22/2018 10:42:52 AM EDT	System/Administrator	Project: AAA Reason: Project is being deleted.
107	Deleted Project	3/22/2018 10:42:56 AM EDT	System/Administrator	Project: BCD Reason: Project is being deleted.
108	Deleted Project	3/22/2018 10:45:02 AM EDT	System/Administrator	Project: HGK Reason: Project is being deleted.
109	Deleted Project	3/22/2018 11:05:03 AM EDT	System/Administrator	Project: DDB Reason: Project is being deleted.

Figure 6.3.9.1-2 System Audit Trail for Project Deletion

6.3.9.2 Application-Level Audit Trail

Application-level audit trails monitor and log user activities, including which data files were opened and closed, and what specific actions have been taken, such as reading, editing, processing, and deleting records or fields, and publishing reports. This could also be called a project-level audit trail. Some applications may be sensitive enough to create an audit trail that captures "before" and "after" information for each modified record or the data changed within a record ***(54).***

6.3.9.3 Method Audit Trail

Method audit trails track the changes made to the method and typically contain the following information:

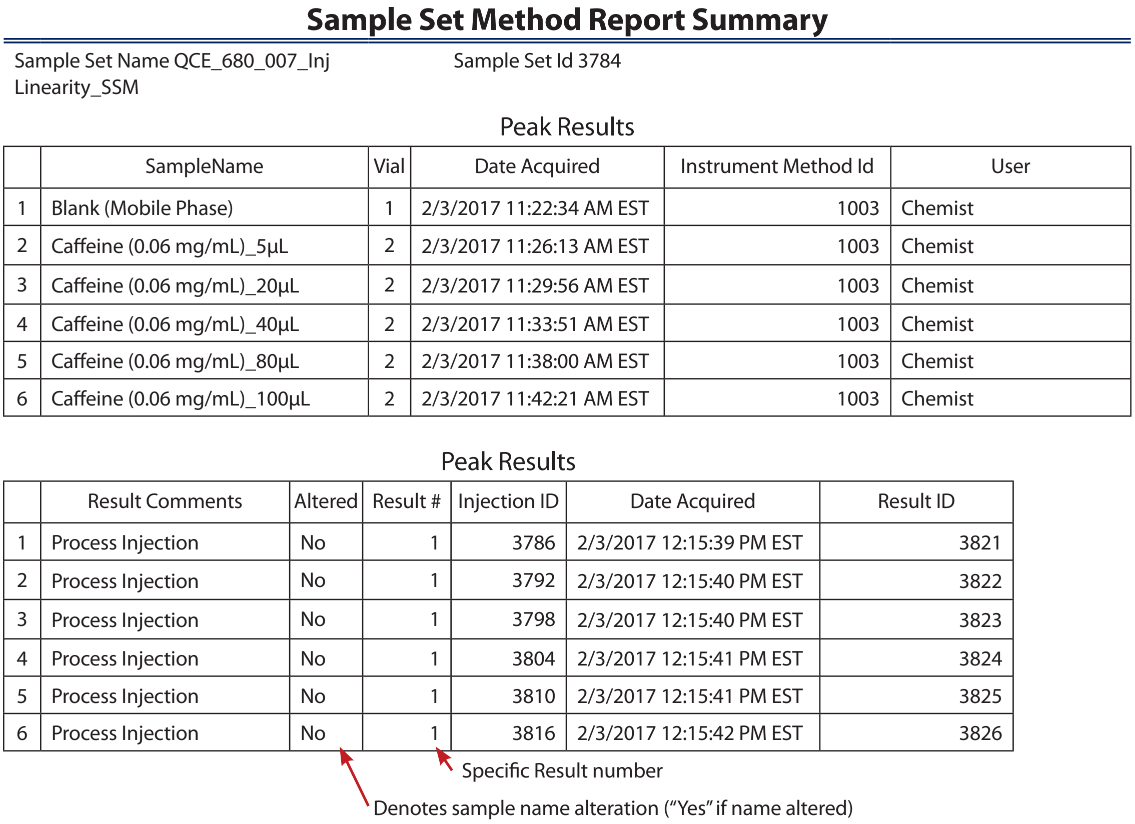
- Method modification history
- Method used for all injections
- Method modified between the sequences

6.3.9.4 Results Audit Trail

Chromatograms or reports can serve as a results audit trail. **Figure 6.3.9.4-1** is a model results audit trail report that presents integration type, date acquired, date processed and by whom, and if the chromatogram was altered after generating data. Typically, chromatograms should contain:

- Sample description
- Date and time of sample acquisition
- Date and time of results processed, if possible
- Minimum method parameters, i.e., wave length, injection volume, and method name/ID
- Integration type
- Retention time (any other system suit parameters)
- Time printed, published, or saved
- Integration events
- Sample name change after execution

Filters can also be used to search the requirement from huge amounts of data. **Figure 6.3.9.4-2** represents a filter to search whether the sample has been injected in multiple projects. For older systems with limited functionality, the reviewer should sign and stamp results printed on paper and review the electronic data according to the Quality Unit policy. If the results are published electronically, the reviewer should e-sign the results after reviewing and lock the signed file. If it will be used for any investigational purpose, the Quality Unit must review the electronic data per the firm's policy, as electronic data is deemed to be final. Once the printed data is audited, original electronic data should be available for reference and should not be altered. Any modification to the approved data needs to be justified.



Sample Set Method Report Summary

Sample Set Name QCE_680_007_Inj Linearity_SSM

Sample Set Id 3784

Peak Results

	SampleName	Vial	Date Acquired	Instrument Method Id	User
1	Blank (Mobile Phase)	1	2/3/2017 11:22:34 AM EST	1003	Chemist
2	Caffeine (0.06 mg/mL)_5µL	2	2/3/2017 11:26:13 AM EST	1003	Chemist
3	Caffeine (0.06 mg/mL)_20µL	2	2/3/2017 11:29:56 AM EST	1003	Chemist
4	Caffeine (0.06 mg/mL)_40µL	2	2/3/2017 11:33:51 AM EST	1003	Chemist
5	Caffeine (0.06 mg/mL)_80µL	2	2/3/2017 11:38:00 AM EST	1003	Chemist
6	Caffeine (0.06 mg/mL)_100µL	2	2/3/2017 11:42:21 AM EST	1003	Chemist

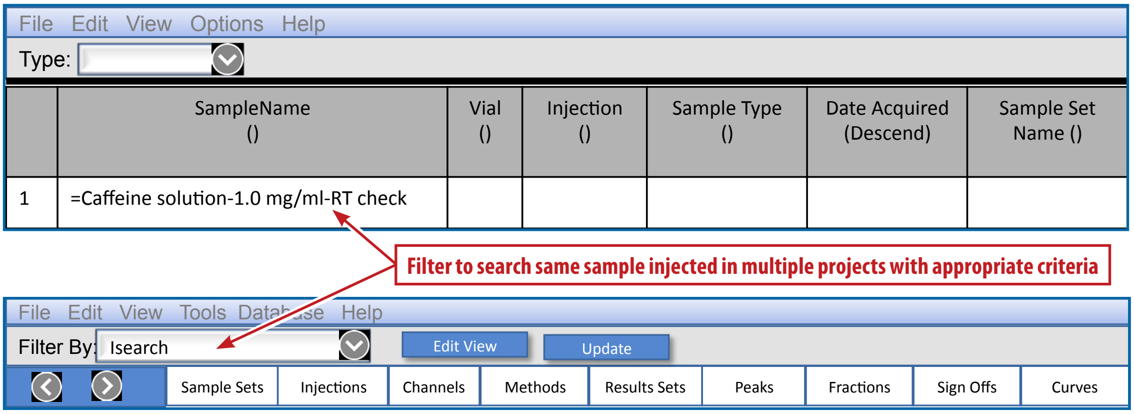
Peak Results

	Result Comments	Altered	Result #	Injection ID	Date Acquired	Result ID
1	Process Injection	No	1	3786	2/3/2017 12:15:39 PM EST	3821
2	Process Injection	No	1	3792	2/3/2017 12:15:40 PM EST	3822
3	Process Injection	No	1	3798	2/3/2017 12:15:40 PM EST	3823
4	Process Injection	No	1	3804	2/3/2017 12:15:41 PM EST	3824
5	Process Injection	No	1	3810	2/3/2017 12:15:41 PM EST	3825
6	Process Injection	No	1	3816	2/3/2017 12:15:42 PM EST	3826

Specific Result number

Denotes sample name alteration ("Yes" if name altered)

Figure 6.3.9.4-1 Results Audit Trail Report



	SampleName ()	Vial ()	Injection ()	Sample Type ()	Date Acquired (Descend)	Sample Set Name ()
1	=Caffeine solution-1.0 mg/ml-RT check					

Filter By: Isearch

Filter to search same sample injected in multiple projects with appropriate criteria

Figure 6.3.9.4-2 Filter to Search Sample in Multiple Projects

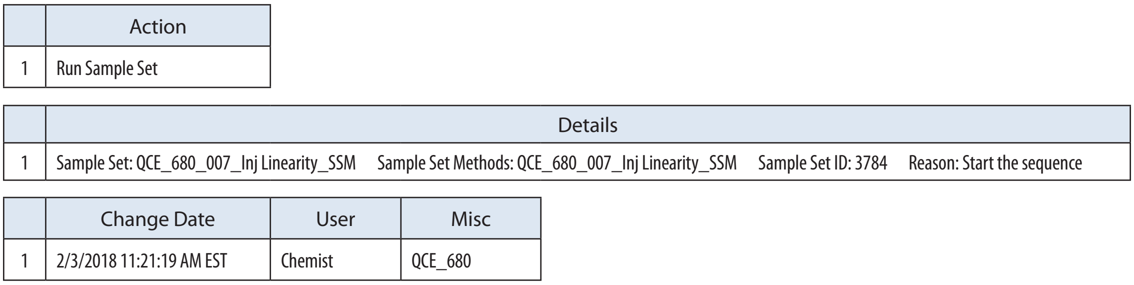
6.3.9.5 Sequence Audit Trail

Sequence audit trails, or sample set audit trails, track the changes made to the sample sequence or batch. **Figure 6.3.9.5-1** represents a typical sequence audit trail report, which generally contains the following information:

- Name correction for sample set or injections after injection acquisition
- Sample set alteration
- Sample name alteration during sequence execution
- Method used for all injections
- Aborted sequences

6.3.9.6 Project-Level Audit Trail

By enabling the audit trails option while creating it, a project will capture all the activities performed with respect to sample set, injections, channels, results, calibration curves, and peaks. **Figure 6.3.9.6-1** represents a project audit trail record for deleted injection as a poor example to show fraudulent data.

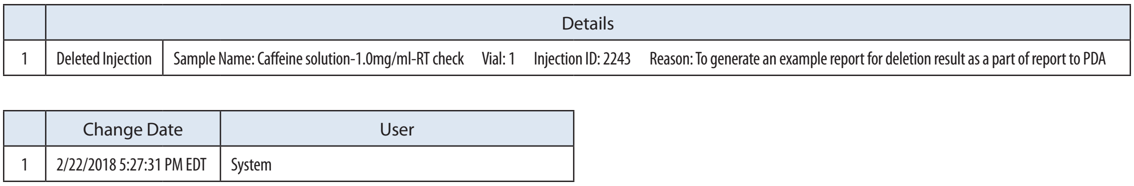


	Action
1	Run Sample Set

	Details
1	Sample Set: QCE_680_007_Inj Linearity_SSM Sample Set Methods: QCE_680_007_Inj Linearity_SSM Sample Set ID: 3784 Reason: Start the sequence

	Change Date	User	Misc
1	2/3/2018 11:21:19 AM EST	Chemist	QCE_680

Figure 6.3.9.5-1 Sample Set Audit Trail Report



	Details	
1	Deleted Injection	Sample Name: Caffeine solution-1.0mg/ml-RT check Vial: 1 Injection ID: 2243 Reason: To generate an example report for deletion result as a part of report to PDA

	Change Date	User
1	2/22/2018 5:27:31 PM EDT	System

Figure 6.3.9.6-1 Project Audit Trail – Deleted Injection

6.3.9.7 Injection Log

Chromatographic data acquisition software typically has the ability to maintain a log of injections. In addition to the date and time, the software may include additional information associated with the injection such as lot number, blank or system suitability, reference, or sample. An audit trail ensures the integrity of the data and, if the audit trail is enabled, review of the injection log is not necessary. Injection log reports are typically built in by the software developer, though with limited ability to customize without expert programming capability. The type, ease of log retrieval, and ease of printing/publishing are also built-in functionalities of the software; however, their inclusion will vary among software suppliers. An injection log is separate and distinct from an audit trail; while it is a good tool to have, it is not essential to ensuring data integrity ***(2).***

6.3.10 Transactional Log/System Errors

6.3.10.1 Chromatography

The transactional log (which may be referred to by other terms depending on the equipment vendor) and system error logs are online, instantaneous features that display pop-up messages about system functionality, user activity, and hardware-related issues or errors. **Figure 6.3.10.1-1** shows the types of errors generated by the software or transactional log and a typical representation of a software transactional log. **Figure 6.3.10.1-2** represents a typical transactional error log.

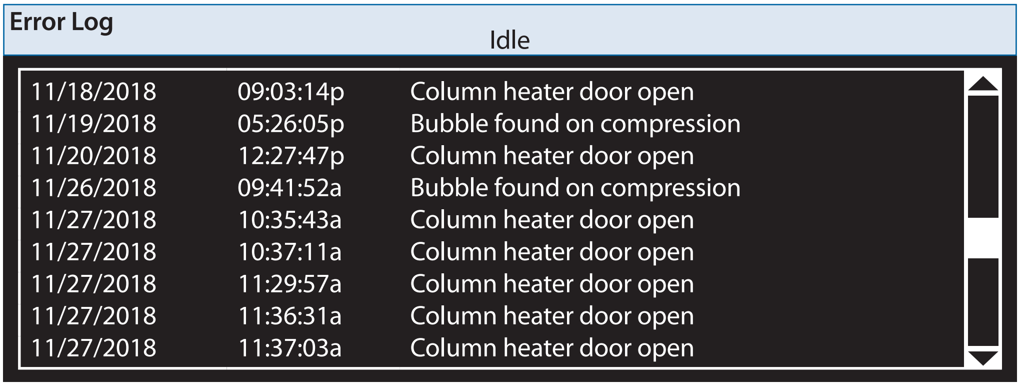
The transactional log is neither an audit trail nor is it intended to be a replacement for or component of other audit trails. A transactional log generally provides some additional information related to software (e.g., missing vial, lost prime) or hardware malfunctions (e.g., HSS fault, lost connection) and can help in interpreting the audit trail.

No one should have access or authority to manually change this log; however, the system can be configured to automatically purge the messages on a periodic basis to ensure efficient operation of the system processing memory. If the audit trail is never turned off, any deletion, modification, or copying of messages performed by the administrator will be recorded in validated audit trails (e.g., system audit trail). The Quality Unit should verify when a system or run has been interrupted due to a disconnection or power loss.

Type	Category	Time	Application	User	Project
Error	*Instrument*	*1/19/2017 4:22:32 AM EST*	*QCE_568*	*Groupleader*	*HPLC Calibration_2017*
Error	*Instrument*	*1/19/2017 4:22:32 AM EST*	*QCE_568*	*Groupleader*	*HPLC Calibration_2017*

Message
Lost prime
Instrument Failure W2690/5#D11SM7731A

Figure 6.3.10.1-1 Example of a Transactional Log



Error Log
Idle

```
11/18/2018    09:03:14p    Column heater door open
11/19/2018    05:26:05p    Bubble found on compression
11/20/2018    12:27:47p    Column heater door open
11/26/2018    09:41:52a    Bubble found on compression
11/27/2018    10:35:43a    Column heater door open
11/27/2018    10:37:11a    Column heater door open
11/27/2018    11:29:57a    Column heater door open
11/27/2018    11:36:31a    Column heater door open
11/27/2018    11:37:03a    Column heater door open
```

Figure 6.3.10.1-2 Example of a System Error Log

The messages appearing in the log may come from the application software, third-party software, (e.g., Oracle database supporting system for chromatographic software) or other connected instruments (e.g., balance connected to HPLC) or equipment. Some chromatographic software packages offer this functionality. The transactional logs are system-level messages, temporarily stored and often automatically purged by the system at time-based defined intervals; their utility is therefore time-sensitive. These transactional logs may prove beneficial for trending (e.g., trending of most frequent instrument or processing errors that require attention helps in troubleshooting) or investigational purposes (e.g., describing the cause of the failure) and companies may utilize this information accordingly. During software validation, messages will present as information, warning, or error according to listed categories (e.g., general, security). Critical messages and actions regarding data manipulation or data deletion that may appear in the transactional log must be captured in validated audit trails (e.g., system, result, sequence or sample, or method audit trails).

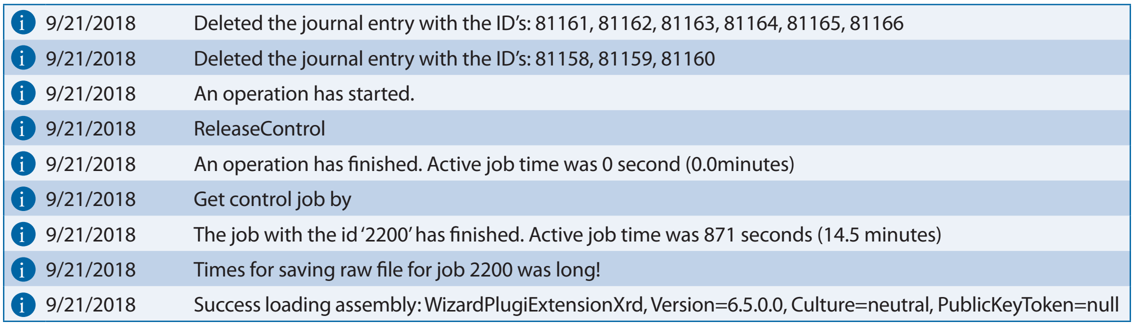
Categorization of error messages having an impact on the software and product ideally would be incorporated during software development and validation by the vendor. Some errors with titles that sound critical (e.g., cable disconnected, connection lost, communication failure) may not be captured in a validated audit trail but recorded in a transactional log. It may be difficult to confirm that these types of messages are all caused by intentional interruptions or have any impact on product quality data. It is therefore important to have appropriate controls and procedures in place to ensure that true power outages be recorded, especially if a chromatographic run is affected.

The Quality Unit for the lab must establish and validate error messages during equipment installation and qualification. Some error messages are specific to the operating system of the software and are not directly related to data or equipment operation. It is important to work with the software supplier to understand the description of messages that are recorded in the transactional log as they may be subject to evaluation during inspection. Further, it is important to identify those messages that are critical, i.e., related to data and instrument operations. For existing or previously installed equipment (e.g., legacy systems), during installation and qualification, the Quality Unit should assure that all transactional log messages are reviewed and understood, and that critical messages are identified and included in validated audit trails. Transactional log messages that have no impact on analyses or quality attributes of a product and messages that are also recorded in validated audit trails need not be retained.

For example, if a cable is disconnected from an HPLC to a LAC/E box, then the data will not be captured, and the transactional log will show a message as system interruption due to cable disconnection. Further dialogue between industry, health authorities, and vendors is needed to resolve how to address this evolving topic.

6.3.10.2 Other Types of Equipment

Transactional logs are also available from other types of automated analytical equipment such as X-ray diffraction(XRD) or Karl Fisher(KF). Examples are shown in **Figure 6.3.10.2-1** and **Figure 6.3.10.2-2** below. **Figure 6.3.10.2-2** also provides an example of how the log entries can be misleading if an auditor is not fully trained on the system. For example, although one entry reads “Deleted the journal entry” in the XRD log, the actual reason for displaying the message is a job interruption. The Quality Unit should recognize critical messages recorded in transactional logs and ensure they are recorded in validated audit trails.



```
ⓘ 9/21/2018    Deleted the journal entry with the ID's: 81161, 81162, 81163, 81164, 81165, 81166
ⓘ 9/21/2018    Deleted the journal entry with the ID's: 81158, 81159, 81160
ⓘ 9/21/2018    An operation has started.
ⓘ 9/21/2018    ReleaseControl
ⓘ 9/21/2018    An operation has finished. Active job time was 0 second (0.0minutes)
ⓘ 9/21/2018    Get control job by
ⓘ 9/21/2018    The job with the id '2200' has finished. Active job time was 871 seconds (14.5 minutes)
ⓘ 9/21/2018    Times for saving raw file for job 2200 was long!
ⓘ 9/21/2018    Success loading assembly: WizardPlugiExtensionXrd, Version=6.5.0.0, Culture=neutral, PublicKeyToken=null
```

Figure 6.3.10.2-1 Example of a Transactional Log for XRD

Warning	2017-09-22 13:04:10 UTC-4	KF2	Conditioning stopped
Information	2017-09-22 13:03:51 UTC-4	KF2	Determination finished
Warning	2017-09-22 13:03:17 UTC-4	KF1	Conditioning stopped
Information	2017-09-22 13:03:10 UTC-4	KF1	Determination finished
Warning	2017-09-22 13:02:57 UTC-4	KF2	Sample data live modified
Information	2017-09-22 13:01:35 UTC-4	KF2	Determination started
Warning	2017-09-22 13:00:37 UTC-4	KF1	Sample data live modified
Information	2017-09-22 12:59:21 UTC-4	KF1	Determination started

Figure 6.3.10.2-2 Example of a Transactional Log for KF

6.3.11 Common Deficiencies

The following problems, listed with the respective ALCS components, are often encountered and commonly found in audits or cited in FDA Warning Letters: ***(55)***

- Computers
  - Shared passwords
  - No control over data generated
  - Data acquisition date-and-time-stamp changes to alter actual date and time of results
  - No control of automatic software updates
  - Computer systems/software validation errors
  - Time synchronization across all equipment and computers in the laboratory
  - Inappropriate database protection in computerized systems
  - Unauthorized changes made by analysts
  - Altering or setting back the computer's clock or date and time of the chromatographic injection
- Server
  - Lack of oversight by Quality Unit
  - Validation errors
  - Improper network mapping that leads to data transmission losses
  - Cloud systems not verified for data transmission and data losses
- Equipment
  - Single injections or sample trial injections of test samples made directly on instrument
  - Stand-alone equipment connected to computer without server lacks controls, routine audit trail reviews, and full data retention capabilities that prevent analysts or other personnel from deleting data
  - Features not appropriately selected or engaged, e.g., provision for trial injections without being captured in audit trails (implies lack of understanding or verification by lab personnel)
  - Improper configuration of computers or storage devices that can lead to duplication or falsification of data (implies lack of training for IT personnel)
  - Data losses due to power outage without investigation
  - Altering system suitability to make it appear as if the sample failure was caused by an equipment malfunction
- Off-the-Shelf Software
  - Data processing scenarios not validated
  - Data calculations not validated
  - Part 11 compliance assumed or not verified
  - Software version changes incompatible with older files
- Data Handling
  - Trial injections of test samples
  - Data integration problems and compromises
  - Not reviewing/publishing/enabling audit trails
  - Not reporting incidents

- Retesting samples, deleting OOS results, and reporting passing results during stability or to release batches
- Data deletions
- Data manipulations, such as changing integration, date and time, or method parameters
- Data not archived
- Data archived on unreadable discs
- Reviewers unable to detect the problems due to lack of understanding fields
- Aborted sequences
- Inhibition of peaks/disregarding peaks without proper scientific justification

6.4 Other Laboratory Equipment

Due to the increasing number of citations about HPLC and GC instruments that have led to FDA Warning Letters, laboratory management may underestimate the importance of other equipment (e.g., UV, FTIR) being in compliance with 21 CFR Part 11. Because not all laboratory equipment is available in both a hybrid-system and a computer operated system (e.g., UV spectrophotometer, Fourier transform infrared spectrometer (FTIR), atomic absorption spectrometer, X-ray spectrometer, or titrator), there could be a mix of formats in the laboratory. As a result, some laboratories have adopted "scientific data management systems," which can capture data from all instruments that generate signals and are equipped with RS 232 or local area network ports. If used, this scientific data management system needs to be qualified as laboratory data management software and should be compliant with 21 CFR Part 11 requirements.

Although the software supplied for UV and FTIR instruments may not have the same applications as HPLC or GC software, similar observations have been listed as deficiencies in audits and FDA Warning Letters, for example: ***(55)***

- Lack of audit trails
- No unique user IDs and passwords
- Data can be deleted
- Data files can be saved as new data files using "save as" function
- Not all changes to data captured in audit trails
- Processing parameters not saved or not captured as metadata
- Not enabling, reviewing, or printing/publishing audit trails
- All user IDs and passwords treated as "administrator" for the majority of stand-alone systems
- Failure to establish and exercise adequate controls over computers to prevent unauthorized access, changes to, or omission of electronic data
- Failure to maintain complete electronic raw data for instruments, Malvern particle-size analyzer, and UV spectrophotometer, e.g., instruments were connected to stand-alone computers that stored the data, which could be deleted at any time

Laboratory management should ensure that the following procedures and system design, where possible, are put in place for UV and FTIR instruments:

- Audit trail feature enabled at all times
- System audit trails review, including scope and how to conduct
- Data protection and archival
- Individual user logins
- Qualification of software

6.5 Laboratory Data Management Software

Some analytical laboratories manage laboratory data using commercial software like LIMS or scientific data management systems. Whether the software is validated at the site, either by the vendor or by the user, the user is responsible for assuring its compliance with 21 CFR Part 11. The Quality Unit should understand completely the functionality, features, and capability of the software. All automatic equipment used in pharmaceutical manufacturing environment, including computers used to test drug products, must also comply with 21 CFR Part 211.68. Regulatory expectations for computerized systems used in the manufacture of API are found in the ICH Q7 Guidance for Industry ***(6,8,43).***

Browser-enabled user logins from multiple computers pose a potential risk. Login functionality is recommended to be properly challenged, mitigated, and verified. An additional layer of security should be embedded in the software that allows only user logins that have been verified by specific, permitted IP addresses as filter logins.

Laboratory data management software typically is validated using the following steps (not necessarily in this order):

- Document the software name and version number
- Define the period for software updates
- Check and validate e-signatures
- Validate the software for its intended use
- Determine capability of meeting 21 CFR Part 11 requirements in terms of audit trail and controls
- Test the software on the network for data transmission
- Set up controls and traceability of printouts and define number of printouts allowed
- Check data and security of offshore and Cloud data
- Validate Cloud-based data management system for security and possibility of compromise
- Establish quality service agreement and contingency plan for Cloud-based systems and determine exact physical location of servers
- Verify record and logic behind the algorithms used in calculations
- Calculate manually the common statistical computations used by software (such as mean, standard deviation, percentage of relative standard deviation to complex math like potency content, similarity factor (F2) values for dissolution analysis, and coefficient of variation for uniformity of dosage) and compare with software values
- Check data transmission and losses from instruments to attached computer
- Check data transmission to computer, server, and interfaces in between, and validate for intended functionality of analysis, data acquisition, processing, reporting, tracking, and security
- Ensure PDFs of any converted data files are not editable and bear a date-and-time stamp
- Confirm that intended software is compatible with COTS software for any laboratory instrument (e.g., HPLC, GC, and PSD).

6.5.1 Controls

The following are the minimum controls needed to validate laboratory data management software:

- Identify the person responsible for updates and maximum possible software updates to be performed by the software vendor and in-house IT personnel
- Address any changes to software through change history
- Establish secure unique user login identifications and periodic change of passwords
- Restrict permission to delete data to administrator or IT personnel

- Maintain copies of older versions of software whenever version is updated (recommended) and ensure that backed-up data from previous versions can still be accessed
- Check software integrity on a periodic basis
- Maintain detailed list of roles, responsibilities, and privileges for all staff who use the laboratory data management software

6.5.2 Common Deficiencies that May Lead to Data Compromise

- Browser-based interface enabling simultaneous logins with the same IDs without sufficient controls to prevent redundant data activity
- Not investigating qualification errors or shortfalls according to nonconformance procedure
- Not enabling, reviewing, or publishing audit trails
- Installing features without complete understanding, leading to data compromise
- Lapses in training, e.g., lack of training or inadequate training for tasks being performed

6.5.3 Spreadsheet Validation

Many laboratories use customized spreadsheets for calculations. To avoid possible data breaches, the Quality Unit should validate the customized spreadsheet template for its intended use and protect it by restricting permissions to alter the template or delete data.

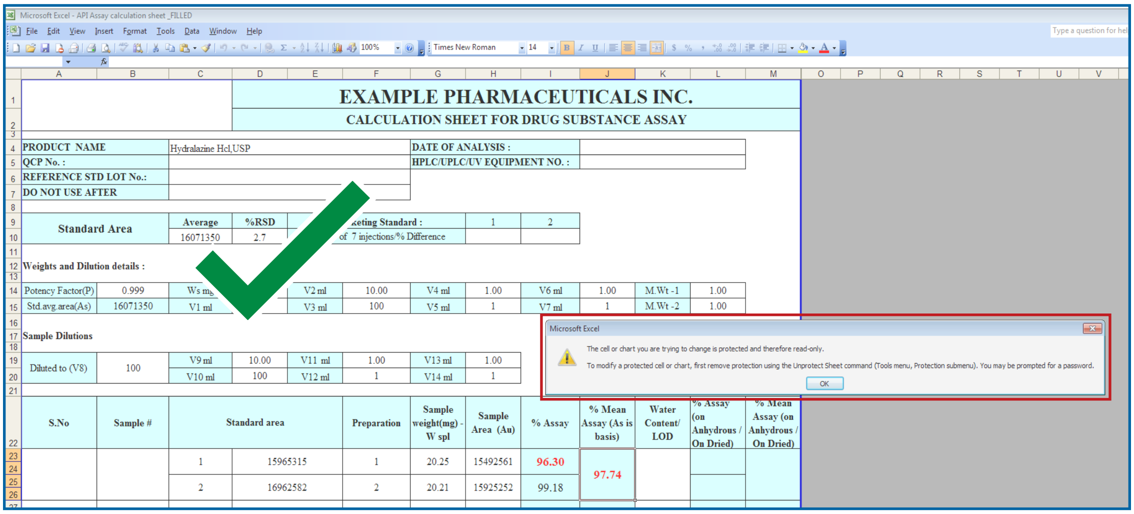
Typically, customized spreadsheets are validated by customizing them to the intended use with a standardized formula in the USP or another valid source, comparing the manual calculations against the spreadsheet calculations, and testing boundaries and functions.

6.5.3.1 Spreadsheet Controls

The following are the minimum controls to be put in place for customized spreadsheets, which are recommended to be captured in the SOPs:

- Encrypt with password protection
- Restrict editing (set to "Read only") so previous data is not retained in the template
- Save spreadsheets to a designated location on the server and capture the file location on each spreadsheet
- Change passwords and revalidate customized spreadsheets periodically per established SOPs

Figure 6.5.3.1-1 represents a typical template for a validated, protected, tamper-resistant spreadsheet.


Microsoft Excel - API Assay calculation sheet _FILLED
File Edit View Insert Format Tools Data Window Help
100%
Times New Roman
14
Type a question for hel
A B C D E F G H I J K L M N O P Q R S T U V

EXAMPLE PHARMACEUTICALS INC.

CALCULATION SHEET FOR DRUG SUBSTANCE ASSAY

PRODUCT NAME	Hydralazine Hcl,USP	DATE OF ANALYSIS :	
QCP No. :		HPLC/UPLC/UV EQUIPMENT NO. :	
REFERENCE STD LOT No.:			
DO NOT USE AFTER			

Standard Area	Average	%RSD		keting Standard :	1	2
	16071350	2.7		of 7 injections/% Difference		

Weights and Dilution details :

Potency Factor(P)	0.999	Ws mg		V2 ml	10.00	V4 ml	1.00	V6 ml	1.00	M.Wt -1	1.00
Std.avg.area(As)	16071350	V1 ml		V3 ml	100	V5 ml	1	V7 ml	1	M.Wt -2	1.00

Sample Dilutions

Diluted to (V8)	100	V9 ml	10.00	V11 ml	1.00	V13 ml	1.00
		V10 ml	100	V12 ml	1	V14 ml	1

S.No	Sample #	Standard area		Preparation	Sample weight(mg) - W spl	Sample Area (Au)	% Assay	% Mean Assay (As is basis)	Water Content/ LOD	% Assay (on Anhydrous / On Dried)	% Mean Assay (on Anhydrous / On Dried)
		1	15965315	1	20.25	15492561	96.30	97.74			
		2	16962582	2	20.21	15925252	99.18				

Microsoft Excel

The cell or chart you are trying to change is protected and therefore read-only.

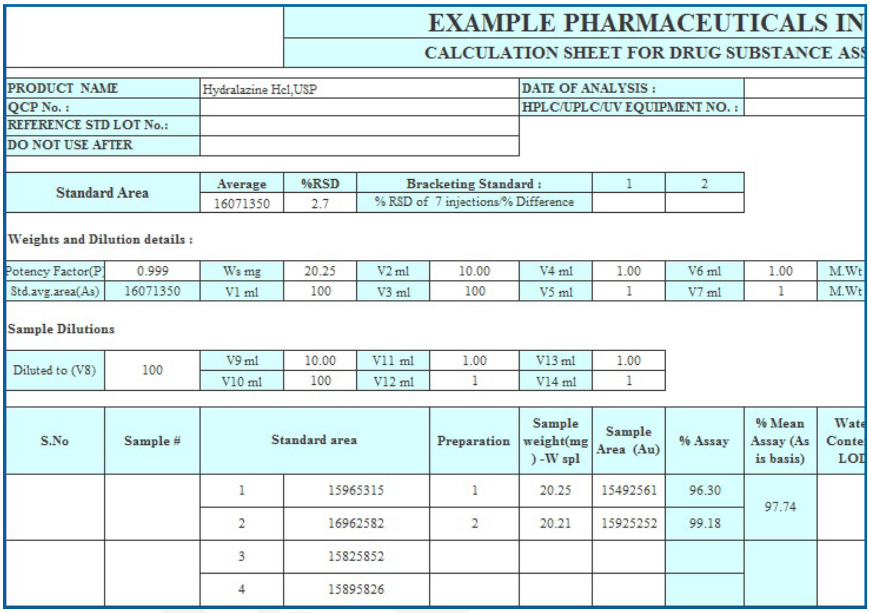
To modify a protected cell or chart, first remove protection using the Unprotect Sheet command (Tools menu, Protection submenu). You may be prompted for a password.

Figure 6.5.3.1-1 Example of Validated, Protected Spreadsheet

6.5.3.2 Common Deficiencies in Spreadsheets

The following are commonly seen deficiencies in spreadsheets that may lead to data compromise and risk of data integrity problems:

- Spreadsheets not validated
- Accidental or deliberate formula changes made in unprotected spreadsheets (e.g., in **Figure 6.5.3.2-1,** data was manipulated; the failing value of 96.30 was replaced with a passing value of 98.23, which was entered manually on the unprotected sheet)
- Entering passing results in unprotected spreadsheets (**Figure 6.5.3.2-2**)
- Lack of controls on spreadsheet access and lack of training of staff to respect password control



EXAMPLE PHARMACEUTICALS IN

CALCULATION SHEET FOR DRUG SUBSTANCE ASS

PRODUCT NAME	Hydralazine Hcl,USP	DATE OF ANALYSIS :	
QCP No. :		HPLC/UPLC/UV EQUIPMENT NO. :	
REFERENCE STD LOT No.:			
DO NOT USE AFTER			

Standard Area	Average	%RSD	Bracketing Standard :	1	2
	16071350	2.7	% RSD of 7 injections/% Difference		

Weights and Dilution details :

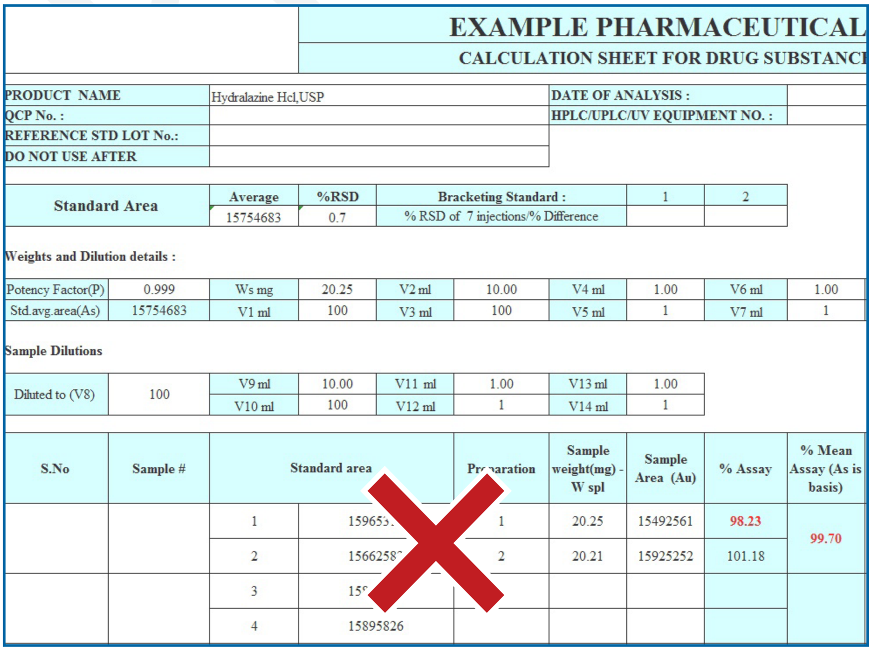
Potency Factor(P	0.999	Ws mg	20.25	V2 ml	10.00	V4 ml	1.00	V6 ml	1.00	M.Wt
Std.avg.area(As)	16071350	V1 ml	100	V3 ml	100	V5 ml	1	V7 ml	1	M.Wt

Sample Dilutions

Diluted to (V8)	100	V9 ml	10.00	V11 ml	1.00	V13 ml	1.00
		V10 ml	100	V12 ml	1	V14 ml	1

S.No	Sample #	Standard area		Preparation	Sample weight(mg) -W spl	Sample Area (Au)	% Assay	% Mean Assay (As is basis)	Wate Conte LOD
		1	15965315	1	20.25	15492561	96.30	97.74	
		2	16962582	2	20.21	15925252	99.18		
		3	15825852						
		4	15895826						

Figure 6.5.3.2-1 Validated Spreadsheet: API Assay Failure (Failure Result is 96.30)



EXAMPLE PHARMACEUTICAL

CALCULATION SHEET FOR DRUG SUBSTANCI

PRODUCT NAME	Hydralazine Hcl,USP	DATE OF ANALYSIS :	
QCP No. :		HPLC/UPLC/UV EQUIPMENT NO. :	
REFERENCE STD LOT No.:			
DO NOT USE AFTER			

Standard Area	Average	%RSD	Bracketing Standard :	1	2
	15754683	0.7	% RSD of 7 injections/% Difference		

Weights and Dilution details :

Potency Factor(P)	0.999	Ws mg	20.25	V2 ml	10.00	V4 ml	1.00	V6 ml	1.00
Std.avg.area(As)	15754683	V1 ml	100	V3 ml	100	V5 ml	1	V7 ml	1

Sample Dilutions

Diluted to (V8)	100	V9 ml	10.00	V11 ml	1.00	V13 ml	1.00
		V10 ml	100	V12 ml	1	V14 ml	1

S.No	Sample #	Standard area		Pr[illegible]paration	Sample weight(mg) - W spl	Sample Area (Au)	% Assay	% Mean Assay (As is basis)
		1	15965[illegible]	1	20.25	15492561	98.23	99.70
		2	1566258[illegible]	2	20.21	15925252	101.18	
		3	15[illegible]					
		4	15895826					

Figure 6.5.3.2-2 Modified Standard Average Change Value in Spreadsheet for Assay Preparation 1

6.6 Electronic Data Governance

In the current analytical laboratory environment, the key factors, discussed in this section, need to be considered for data governance. Analytical equipment controlled by firmware may not be able to publish audit trails. If not, the Quality Unit should implement a procedure to check for data compromises on any equipment for which this is the case. Controls should be similar for all equipment and data integrity should be ensured on all equipment. A logbook for data backup and deletion should also be maintained.

A high-level diagram of electronic data governance in an analytical laboratory is presented in **Figure 6.6-1.**

6.6.1 Data Backup and Storage

The Quality Unit should develop a procedure for data backup and determine at what intervals it will be performed. Hybrid systems have temporary electronic storage that is overwritten (e.g., calibration curves on pH meters); this printed/published record is the primary data source. This electronic information is not intended for backup or long-term retention. Analytical equipment on which electronic data is generated should be included in the data backup. Copying data onto discs as a backup is recommended to protect against the potential failure of the server or Cloud. The data copied onto the discs should be checked for completeness and accuracy. To ensure the safety of the data, common industry practice is to maintain two copies of the data at different locations. Any Cloud-based storage service should be GXP-compliant ***(5).*** Wherever possible, a risk-based cold backup (a scheduled backup without any manual intervention) should be planned to avoid surprises and regulatory complications.

It is strongly recommended that electronic signatures, if adopted, comply with 21 CFR Part 11 requirements and include date and time stamps.

The laboratory data governance manual is useful for consolidating current information about laboratory equipment and data procedures and may contain sections such as those listed below. **Table 6.6.1-1** represents a model table from a laboratory data governance manual. Preparing this manual and keeping it current is a good practice, one that makes a laboratory audit more efficient.

- Details of all laboratory equipment
- Details of all equipment software, including version information
- Laboratory equipment procedure numbers

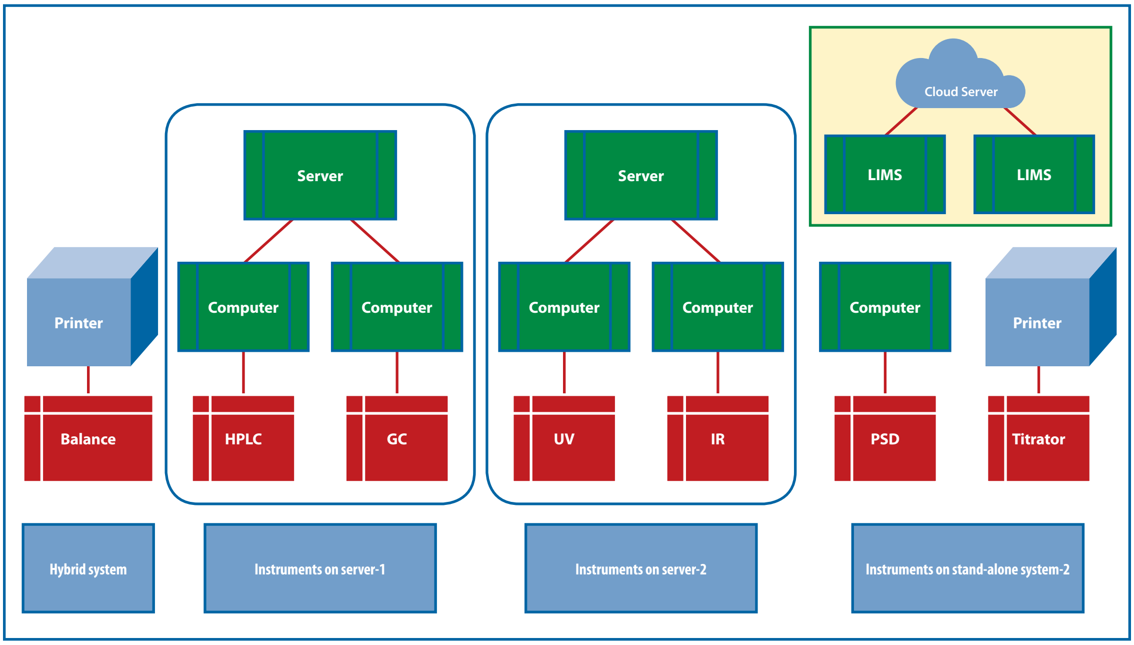


Figure 6.6-1 Typical Analytical Laboratory Data Mapping

- Data handling procedures, list of audit trails published or reviewed, each analysis, and typical information captured
- List of all users of all software and their roles
- Server(s) details
- Data backup frequency
- Risk analysis and mitigation plan
- Names and contact information of key personnel and vendors

Table 6.6.1-1 Example of a Table in a Laboratory Manual

Instrument	Software	Version	Procedure Reference	Part 11 Compliant	Audit Trails Reviewed	Data Frequency	
						Backup	Reconciliation
HPLC	Important	R 1	SOP 34, 36, 45	Yes	Yes	3 M	30 days
GC	Important	R 1	SOP 34, 39, 45	Yes	Yes	3 M	30 days
PSD	Super	V 5	SOP 34, 48, 56	Yes	Yes	3 M	60 days
Balance	N/A	N/A	SOP 15	N/A	N/A	N/A	N/A
LIMS	Excel	V 4.2	SOP 98, 89, 105	Yes	Yes	1 M	N/A

6.6.2 Routine Checks of Data and Multiple Equipment in the Laboratory

The Quality Unit should schedule regular data reconciliation to detect data compromises early. Creating a data flow of the entire laboratory from the top down will provide an excellent overview of where mistakes or breaches might occur. Random checks of employee shifts or timing logs against equipment use should be performed to check data integrity. Synchronization of raw data across the instruments can be verified to expose data manipulation by random checks, such as checking the injection time and balance printout/PDF time for sample weighing and reconciling data periodically on instruments, as represented in **Figure 6.6.2-1.**

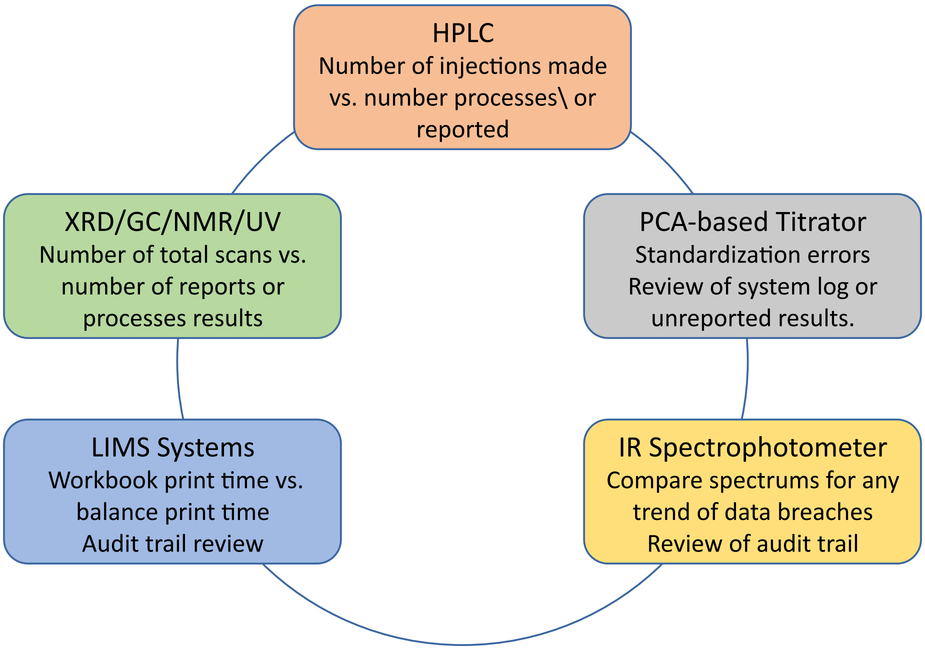

HPLC
Number of injections made vs. number processes\ or reported
PCA-based Titrator
Standardization errors
Review of system log or unreported results.
IR Spectrophotometer
Compare spectrums for any trend of data breaches
Review of audit trail
LIMS Systems
Workbook print time vs. balance print time
Audit trail review
XRD/GC/NMR/UV
Number of total scans vs. number of reports or processes results

Figure 6.6.2-1 Typical Data Reconciliation Exercise

Examples of what to look for on some instruments are:

- **Titrator:** Data stored on the internal memory vs. number of records in the instrument logbook
- **HPLC:** Number of injections vs. number of logbook entries or number of results
- **UV, IR:** Number of data files vs. number of logbook entries.

6.6.3 Communications with Chromatographic Software Vendors

Since instrumental software may have some exceptional behavior, firms should document the communications with software vendors regarding clarification/remediation of error messages, warning messages, software bugs, and other issues that may be identified in audit trails, or other operations that need support from the vendor. These issues, communicated over the phone or via email, should be documented and will serve as a basis for change of procedures or initiation of new controls. Often vendor call centers or tech support groups allot a ticket number or tag number that can be referenced. In addition, there may be issues or restrictions in the software that a vendor would identify and communicate to all users through website notification or email communication. Firms should assess and document how those communications will be evaluated and how a determination is made regarding the effect on GMP operations. Recordings of audit trails and other critical data are recommended to be checked on a periodic basis to have better control and understanding of software issues. If any anomalies are observed they should be investigated immediately, and if they are suspected as software issues they should be communicated to the vendor for next steps of investigation.

6.6.4 Presenting Data on Request in Electronic Format for Audits and Inspections

Auditors and health authority inspectors may request that electronic data be copied onto portable media (such as a USB or portable hard drive) or in a readable format (such as PDF, Microsoft Excel, or text) for their review evidence. Copying data from a validated system compliant with 21 CFR Part 11 or EU GMP Annex 11 onto media or into a readable format that does not maintain the original metadata should be avoided if possible. If data is transferred onto media or into a readable format, verification that the data and metadata are a true copy is recommended. Uncontrolled use of the copy-and-paste function can be prone to error and give the impression that original data has been altered or falsified. Establishing an SOP that governs how to copy and save data from laboratory systems is highly recommended. The SOP should describe the standard queries and reports that can be generated for audit and inspection purposes and the controls in place to ensure the accuracy of non-routine reports. Printing or exporting injection logs with all the details, such as injection time and sample name, may not be readily possible on some chromatographic software.

7.0 Risk Management of Data Governance Systems

Data integrity controls should be based on quality risk management principles such as ICH Q9 ***(37),*** that is, the level of controls, verification, and oversight should be commensurate with the criticality of the data to patient safety and with the risk to data accuracy, completeness, fabrication, or falsification.

7.1 Risk Assessment

Conducting a risk assessment is a recommended method to assess and challenge processes, systems, controls, and practices in place for the generation, review, and archival of paper and electronic data.

Risk assessments may be performed as part of the selection, commissioning, and validation of computerized systems. Testing of system functions and user privileges should be performed to ensure appropriate controls are in place that prevent or track changes to data, including any mechanism or role that allows data to be altered, overwritten, not saved, or deleted.

Risk assessments for paper data should be performed to assess controls in place that provide for traceability and reconciliation of the records. Mechanisms should also be in place to ensure that original records can be authenticated.

7.2 Risk-Based Mitigation

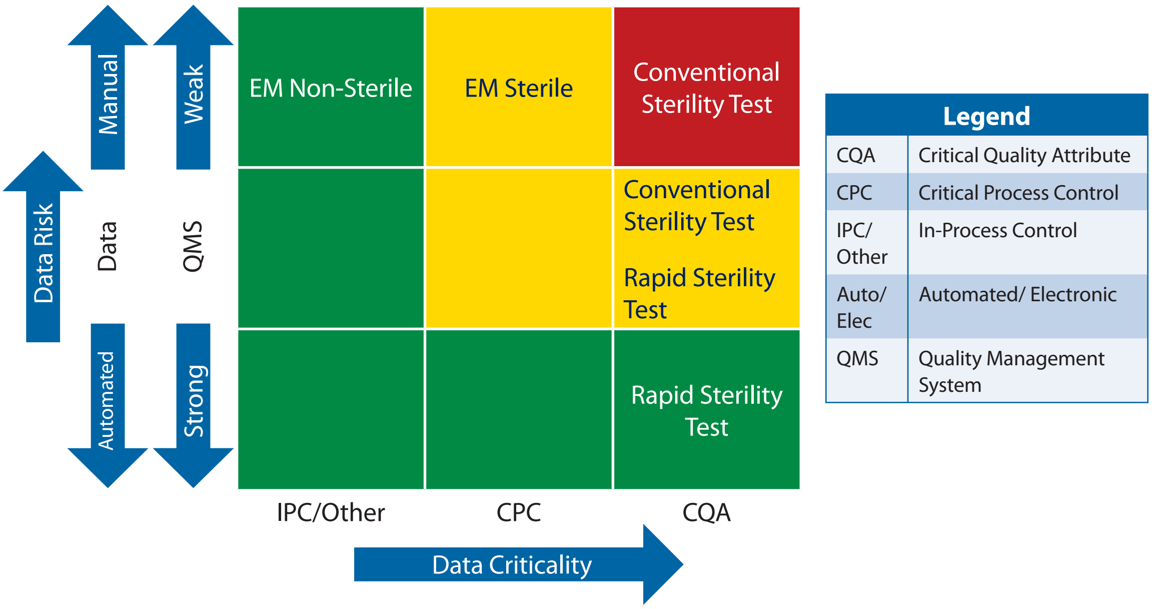
As discussed earlier in this paper, risks to ensuring data integrity might include computerized systems with lack of audit trails or appropriate security controls to prevent unauthorized changes as well as observational test methodologies. A systematic approach to risk mitigation is the use of a risk matrix.

A risk matrix can be established using criticality of the test and maturity of the quality system and use of risk-reducing technology. Data criticality can be established based on whether the test is for a critical quality attribute (CQA), such as a sterility test; a critical process control (CPC), such as an environmental monitoring test; or an in-process control or other test, such as environmental monitoring for nonsterile products. **Figure 7.2-1** shows a risk matrix applied to data integrity. In this example, the matrix is used to establish which microbiological tests require second-person verification prior to approving test results.

Currently, a high percentage of the tests conducted in microbiology laboratories are observational, that is, the results (such as a colony count) are viewed and manually recorded on a paper document or in a computer record. Absent an easy, reliable method to verify the recorded data, some laboratories require microbiologists to use second-person verification (e.g., supervisor) by physical examination of the test plates. Further, the second-person verification could be performed as a discreet step prior to approval of the data or combined with the data-approval step.

Risk factors for the collection, control, and verification of microbiology data are reduced with computer interface technology, such as automated plate readers or rapid methods that produce an electronic record that is retrievable and relatively tamper-proof or digitally time-and-date-stamped photography equipment. This can include automation and the use of advanced methods with a validated data recording (for example, ATP bioluminescence platform) system and audit trail capabilities. Even when a technological solution is not available, a strong pharmaceutical quality system (PQS), including an effective site audit program, supervisory and Quality Unit presence in the laboratory, and a robust periodic review of the documentation system, will reduce data integrity risk. On the other hand, a weak PQS increases the data integrity risk.

Potential Data Integrity Risk Matrix for Microbiological Testing



	IPC/Other	CPC	CQA
	🟩 EM Non-Sterile	🟨 EM Sterile	🟥 Conventional Sterility Test
	🟩	🟨	🟨 Conventional Sterility Test Rapid Sterility Test
	🟩	🟩	🟩 Rapid Sterility Test

Legend	
CQA	Critical Quality Attribute
CPC	Critical Process Control
IPC/ Other	In-Process Control
Auto/ Elec	Automated/ Electronic
QMS	Quality Management System

Figure 7.2-1 Risk Matrix Example for Microbiological Testing

8.0 How to Remediate Breaches in Data Integrity

8.1 Discovery of Data Integrity Issues in Pharmaceutical Laboratories

Data integrity issues may be discovered by various means, including self-reporting, data review, and internal audits, as well as during regulatory inspections. Any deviations from the established procedures that affect data integrity should be reported through the quality system; the Quality Unit should then investigate those situations to assess their impact and scope, determine the root cause, and define corrective and preventative actions.

Deviations affecting data integrity may be a single event or the result of ongoing practices. Regardless, each instance must be investigated to ensure data reliability. Any data breach or compromise that takes place due to ignorance or to a willful act may lead to a quality- or public safety-related event. Upon discovery of a data integrity breach, the actions taken should be proportional to the circumstances. Key considerations are to contain the event, to gather the data necessary to confirm event details, and to determine the scope.

Employee interviews play a key role in data integrity investigations and should be conducted as soon after an event as possible. To prevent a conflict of interest, interviewers selected to conduct the investigations should be independent from the unit under investigation and should conduct interviews away from the unit under investigation. While data integrity investigations should be documented within the quality system (as are all types of investigations), portions of these investigations may need to be kept "confidential" within the quality management system while the investigation is underway to protect the anonymity of the individuals involved. This is necessary to protect against retaliation, to promote open communication, and to avoid possible roadblocks during the course of the investigation.

Factors that may contribute to data integrity breaches include:

- Inadequate resources, training, or necessary expertise
- Time constraints
- Poor test methods, validation gaps, or product issues
- Processes, procedures, or systems that do not fundamentally support data integrity.

Data integrity failures may be unintentional errors or may be attributed to sloppiness. They may also be a deliberate attempt to mislead, misrepresent, alter, or falsify the original data. While corporate officers, management, and personnel often dismiss the willingness of their colleagues to breach data integrity principles, its occurrence has been evidenced by multiple incidents of regulatory correspondence and in industry discussions. Leadership may be culpable, intentionally or not, of creating an environment where values and/or performance expectations hinder compliance, or where individuals may act in their own interests. Acknowledging these risks is crucial to developing a data governance system that can detect and remediate data integrity failures of this nature.

8.2 Investigation Considerations

An investigation must evaluate both the impact of the data integrity breach on the data generated and the decisions made based on that data. Companies might want to use the services of an independent laboratory to conduct a retrospective review of data and/or perform additional testing.

Remediation of data integrity "risks," as opposed to an identified data integrity breach, may follow a similar pattern of investigation to determine the possible impact on data generated; however, the approach and level of effort invested in a retrospective review will differ. For example, if a system gap is identified and process improvements are made to address the gap, a retrospective review of data generated prior to the process improvement may not be necessary. Factors to consider in this decision may include the overall site compliance profile; complexity of the risk (level of effort to exploit the risk); associate knowledge (well-known gap or initial discovery); or type of risk, as well as measures in place and/or other testing that detects a product failure. It may not be possible to confirm with absolute certainty that a gap has not been exploited; however, when identified, immediate actions should be taken to protect against that risk being exploited and to correct the system or process for the future.

As an example, if administrator access was given to a laboratory supervisor or analyst and audit trails were not in place or turned on, a retrospective data review and associate interviews may provide some evidence of actions taken. Yet, most likely, that review will not provide 100% certainty that the data generated, while those risks were in place, were not compromised. Taking immediate action to address those gaps will contribute greatly to ensuring data integrity in the future. Added controls can demonstrate gaps related to test methods or product issues that may not have been detectable prior to system upgrades. In that event, a full investigation would be required, including a retrospective review of previously tested and/or released batches as well as test results for pending and approved applications that might have been affected.

8.3 Comprehensive Assessment of Systems

For a remediation plan to be effective, a comprehensive assessment (CA) of the potentially affected system(s) and extent of the inaccuracies must be performed including identification of root cause. Depending on the severity and complexity of the issue, a competent independent party might best be utilized to perform the CA under a protocol that specifies how the data or information will be assessed, along with the scope of the evaluation. The approach selected should be justified. The following points in the scope of a CA for laboratory data integrity breaches should be considered:

- Time period and product(s) to be covered
- Details specifying data types to be examined (estimated number of HPLC-processed injections, type of microbial identification platform)
- Equipment to be evaluated (HPLC, GC, NIR, FTIR, automated microbial air sampler, stand-alone equipment)
- Departments included in the assessment (R&D, stability, microbiology laboratory)

Systems other than the laboratory may need to be included.

The CA should focus on the process gaps that permitted the data integrity breach to occur without detection. Depending on these gaps, the CA would be designed to identify other possible data integrity breaches that may have occurred. In most cases, the CA and retrospective review should include an assessment of testing data for incoming materials, in-process testing, stability and finished testing, and data used to support pending and approved applications to determine if any wrongful acts might have adversely impacted the application. This should include impact on the development/scale-up/validation of products distributed. This data review is critical because the findings may need to be reported to the regional regulatory agency and can be used to inform decisions to initiate corrective actions against marketed products or the withdrawal of pending or approved applications.

For the remediation to be effective, the scope of the CA must be appropriate. For example, if one or two employees were engaged in deliberate practices that compromised data integrity, the CA should require evaluation of all test results generated by those employees. Whether or not lab managers were aware of the wrongdoing should also be considered in the scope of the CA.

The following are recommendations on how to implement a CA:

- Consider using independent interviews of staff, without fear of reprisal, to ensure the causes of data integrity issues and scope of the problematic practices are fully understood.
- Develop a detailed protocol and methodology, a summary of all laboratories, manufacturing operations, and systems to be covered, and a justification for excluding any relevant operation.
- Identify the omissions, alterations, deletions, records destroyed, nonconcurrent records completed, etc.

- When appropriate, conduct a retrospective evaluation of the nature of the deficiencies in testing data integrity. A risk-based decision should be made in determining the scope of such reviews considering the data integrity gap, whether there is evidence that the gap has been exploited, and the potential impact on product quality.
- Assess the associated risk and potential effects of failures on drug products released and on patients.
- Third-party product testing may be considered as part of additional verification.

8.4 Corrective and Preventive Action Plans

A risk-based approach is necessary for establishing corrective and preventive actions for data integrity breaches uncovered. Actions taken may include establishing additional controls, providing training or resources to prevent recurrence, or implementing measures to promote transparency and detection.

Any permanent changes implemented should be based upon the results of the investigation and comprehensive assessment, the resulting root cause determination, and the gap analysis. The following steps are commonly taken to prevent recurrence:

- Product impact assessment (e.g., evaluation of risk to patient safety and potential market actions)
- Creation of a mechanism for anonymous reports to surface data integrity issues early, before they become systemic
- Changes to SOPs
- Changes in personnel
- Changes in access to computerized systems
- Capital investment in upgrading to equipment with more compliant features
- Changes to the quality oversight function (reassessment of roles and responsibilities, QA review process, how corporate quality/compliance will oversee)
- Improvement in systems that allows employees to report suspected noncompliant practices without fear of retaliation
- Gap analysis providing clear understanding of deficiencies that lead to questionable practices so to prevent recurrence
- Evaluation of potential market actions
- Assessment of similar practices affecting other markets (products intended for international markets)
- Engagement with other regulatory authorities and reporting findings
- Comprehensive continuous training program in place and training effectiveness assessment
- Changes to the internal audit program
- Assurance that incidents of missing data, deletion of data, and changes to time-and-date stamps has stopped and actions have been taken to prevent recurrence
- Verifiable changes to software to ensure inability to manipulate electronic data
- Management strategy, including global corrective action plan that could identify if problems were limited to a specific site or generalized throughout corporation and how problems will be prevented
- Create a detailed plan on how a firm will ensure reliability, accuracy, and completeness of data generated and/or submitted to the regulating agency in applications or DMF submissions
- A mechanism to provide regulators and sponsors notifications and updates regarding the assessment of each application should also be considered

9.0 Conclusion

Data integrity is a key element of ensuring robust operations in laboratories. It signifies the level of completeness, consistency, and accuracy of testing processes and results. The current focus on data integrity by health authorities requires companies to remain alert to changing regulations and to instigate internal strategies to detect and correct gaps in data integrity. Therefore, this report identified the global guidances applicable to the data integrity of analytical and microbiological laboratories and described recent regulatory actions against pharmaceutical manufacturers who have major breaches.

Frequent internal auditing, continual training of analysts on regulatory expectations for data generation and management, and assessment of various types of data generated by simple, hybrid, and complex systems are essential. Advancements in automated systems are improving electronic data generation and storage, even as many tests are still performed manually, particularly in micro labs. Thus, computer server qualification, software validation, laboratory equipment qualifications, and data retrieval for inspection or review are the key elements of data integrity.

Risk assessment of data governance and control of systems in the pharmaceutical industry should be conducted to remove or mitigate the potential for a breach in data integrity and to avoid enforcement actions (warning letters, import alerts, notices of concern, and refusal to accept or approve applications).

10.0 References

1. U.S. Food and Drug Administration. *Guide to Inspections of Pharmaceutical Quality Control Laboratories;* Silver Spring, Md., July 1993.

2. U.S. Food and Drug Administration. *Data Integrity and Compliance with cGMP Guidance for Industry: Draft Guidance for Comment;* Office of Pharmaceutical Quality and Office of Compliance: Silver Spring, Md., April 2016.

3. World Health Organization. *Annex 5: Guidance on Good Data and Record Management Practices; WHO Technical Report Series, No. 996.* Geneva, 2016.

4. Pharmaceutical Inspection Convention/Pharmaceutical Inspection Co-operation Scheme. Draft PIC/S Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments, 2016. PIC/S Publications–Guidance documents. (accessed Mar 1, 2017).

5. Medicines and Healthcare products Regulatory Agency. *MHRA 'GXP' Data Integrity Definitions and Guidance for Industry;* MHRA: London, March 2018.

6. U.S. Food and Drug Administration. *Guidance for Industry, Part 11, Electronic Records; Electronic Signatures—Scope and Application;* Office of Compliance in the Center for Drug Evaluation and Research : Silver Spring, Md., August 2003.

7. European Commission. *EudraLex, Volume 4: Good Manufacturing Practice, Annex 11: Computerised Systems;* Brussels, Jun 2011.

8. U.S. Food and Drug Administration. *Questions and Answers on Current Good Manufacturing Practices, Good Guidance Practices, Level 2 Guidance – Records and Reports,* July 19, 2011. https://www.fda.gov/drugs/guidancecomplianceregulatoryinformation/guidances/ucm124787.htm (accessed Jul 17, 2018).

9. European Medicines Agency. Questions and answers: Good manufacturing practice -- Data Integrity. http://www.ema.europa.eu/ema/index.jsp?curl=pages/regulation/q_and_a/q_and_a_detail_000027.jsp (accessed Sep 29, 2017).

10. Federal Financial Institutions Examination Council (US Government). IT Booklets – Information Security, 2016. FFIEC IT Examination Handbook Infobase. Washington, D.C. https://ithandbook.ffiec.gov/it-booklets/information-security/appendix-b-glossary.aspx#D (accessed Mar 16, 2018).

11. Parenteral Drug Association. *Technical Report No. 62: Recommended Practices for Manual Aseptic Processes;* Bethesda, Md., 2013.

12. Watson, D. D. The What, When, and How of Pek Integration: Part 1. What. https://www.chromacademy.com/chromatography-Integration-Parameters-1.html (accessed April 12, 2018).

13. U.S. Food and Drug Administration. *21 CFR Part 58 – Good Laboratory Practice for Nonclinical Laboratory Studies;* U.S. Department of Health and Human Services: Silver Spring, Md., April 2017.

14. American National Standards Institute. *American National Standard for Information Systems—Dictionary for Information Systems;* ANSI/Secretariat: Computer and Business Equipment Manufacturers Association: New York, 1991.

15. U.S. Food and Drug Administration. Part 211–Current Good Manufacturing Practice for Finished Pharmaceuticals, Subpart C–Buildings and Facilities, 1995. Electronic Code of Federal Regulations. http://www.ecfr.gov/cgi-bin/text-idx?SID=9dcac232c962080c0e560c774ccdd429&mc=true&node=pt21.4.211&rgn=div5#se21.4.211_142 (accessed October 7, 2016).

16. World Health Organization. *Annex 2: Good Manufacturing Practices for Pharmaceutical Products: Main Principles. WHO Technical Report Series, No. 986;* Geneva, 2014.

17. European Commission. *Eudralex Volume 2A, Chapter 5. Guidelines on the Details on Various Categories of Variations.* 2013. https://ec.europa.eu/health/sites/health/files/files/eudralex/vol-4/annex11_01-2011_en.pdf (accessed June 1, 2011).

18. U.S. Food and Drug Administration. *21 CFR 211.25 Organization and Personnel; Personnel qualifications;* Department of Health and Human Services: Silver Spring, Md., 2017.

19. U.S. Food and Drug Administration. Warning Letter No. 320-17-17 to FACTA Farmaceutici S.p.A., dated 1/13/17, from the Office of Compliance, Center for Drug Evaluation and Research. FDA's Electronic Reading Room - Warning Letters. https://www.fda.gov:80/FDAgov/ICECI/EnforcementActions/WarningLetters/2017/ucm538068.htm (accessed Feb 27, 2017).

20. U.S. Food and Drug Administration. Warning Letter No. 320-17-13 to Wockhardt, Ltd., dated 12/23/16 from Office of Compliance, Center for Drug Evaluation and Research. FDA's Electronic Reading Room – Warning Letters. https://www.fda.gov/iceci/enforcementactions/warningletters/2016/ucm534983.htm (accessed Feb 27, 2017).

21. U.S. Food and Drug Administration. Warning Letter No. 320-17-05 to Srikem Laboratories Pvt. Ltd., dated 11/8/16, from Office of Compliance, Center for Drug Evaluation and Research. FDA's Electronic Reading Room – Warning Letters. https://www.fda.gov/iceci/enforcementactions/warningletters/2016/ucm529237.htm (accessed Feb 27, 2017).

22. U.S. Food and Drug Administration. Warning Letter No. 320-17-02 to Interpharm Praha A.S., dated 10/18/16, from Office of Compliance, Center for Drug Evaluation and Research. FDA's Electronic Reading Room – Warning Letters. (accessed Feb 28, 2016).

23. U.S. Food and Drug Administration. Warning Letter No. 320-17-04 to Sekisui Medical Co., Ltd., dated 11/8/16, from the Office of Compliance, Center for Drug Evaluation and Research. FDA's Electronic Reading Room – Warning Letters. https://www.fda.gov/iceci/enforcementactions/warningletters/2016/ucm528590.htm (accessed Feb 28, 2017).

24. U.S. Food and Drug Administration. Warning Letter No. 320-17-03 to Beijing Taiyang Pharmaceutical Industry Co., Ltd., dated 10/19/16, from Office of Compliance, Center for Drug Evaluation and Research. FDA's Electronic Reading Room - Warning Letters. https://www.fda.gov/iceci/enforcementactions/warningletters/2016/ucm527005.htm (accessed Feb 28, 2016).

25. U.S. Food and Drug Administration., 2015. Regulatory Action Against Ranbaxy. https://www.fda.gov/Drugs/GuidanceComplianceRegulatoryInformation/EnforcementActivitiesbyFDA/ucm118411.htm (accessed Mar 7, 2017).

26. U.S. Department of Justice. Consent Decree of Permanant Injunction Case 1:12-cv-00250-JFM, 2012. Casewatch.net. http://www.casewatch.net/doj/ranbaxy/consent_decree.pdf (accessed Jun 12, 2018).

27. Cahilly, M. Data Integrity Training Lessons Learned and Case Studies. Washington D.C., 2015.

28. Stramler, J. H. Jr. The Dictionary for Human Factors Ergonomics: A Significant Reference Work in Human Factors. *Human Factors and Ergonomics Society Annual Meeting Proceedings*, 1992; pp 544-547.

29. Siegfried Schmitt, E. *Assuring Data Integrity for Life Sciences;* PDA DHI, Bethesda, Md., March 2016.

30. U.S. Pharmacopeia. General Chapter <71> Sterility Tests. In *USP41–NF36;* Rockville, Md., 2017.

31. Platco, C.; Cundell, A. Data Integrity Issues in Microbial Testing. *Microbiology* **2017**.

32. U.S. Pharmacopeia. General Chapter <61> Microbiological Examination of Nonsterile Products: Microbial Enumeration Tests. In *USP41–NF36;* Rockville, Md., 2017.

33. U.S. Pharmacopeia. General Chapter <62> Microbiological Examination of Nonsterile Products: Tests for Specified Microorganisms. In *USP41–NF36;* Rockville, Md., 2017.

34. U.S. Pharmacopeia. General Chapter <85> Bacterial Endotoxins Test. In *USP41–NF36;* Rockville, Md., 2017.

35. Guilfoyle, D.; Yager, J.; Carito, S. Effect of Refrigeration and Mising on Detection of Endotoxin in Parenteral Drugs Using the Limulus Amebocyte Lysate (LAL) Test. **1989,** *43* (4), 183-187.

36. Lopienski, K. *How Paper and Electronic Source Data Meet ALCOA Elements;* Forte Research Systems: Madison, Wisc., 2014.

37. International Conference on Harmonisation. Quality Guideline Q9: Quality Risk Management, 2006. ICH Guidelines. http://www.ich.org/products/guidelines/quality/article/quality-guidelines.html (accessed August 2016).

38. U.S. Food and Drug Administration. Warning Letter No. 320-14-03 to Usv Limited dated 2/6/14. FDA's Electronic Reading Room - Warning Letters. http://www.fda.gov/iceci/enforcementactions/warningletters/2014/ucm386678.htm. (accessed Feb 28, 2017).

39. U.S. Food and Drug Administration. Warning Letter No. 320-14-11 to Apotex Pharmachem India Pvt Ltd. dated 6/16/14. FDA's Electronic Reading Room – Warning Letters. http://www.fda.gov/iceci/enforcementactions/warningletters/2014/ucm401451.htm (accessed Feb 28, 2017).

40. Haes, S. D.; Grembergen, W. V. Chapter 5: COBIT as a Framework for Enterprise Governance of IT. In *Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5, 2nd Ed.;* Springer, 2015; pp 103-128.

41. International Organization for Standardization. *ISO/IEC 20000-1:2011 Information technology - Service management - Part 11: Guidance on the relationship between ISO/IEC 20000-1:2011 and service management frameworks: ITIL®;* ISO/IEC: Geneva, 2011.

42. U.S. Food and Drug Administration. *U.S. Code of Federal Regulations Title 21 Part 820.30: Design Controls.* Silver Spring, Md., 2014.

43. International Conference on Harmonisation. *Quality Guideline Q7: Good Manufacturing Practice Guide for Active Pharmaceutical Ingredients.* Geneva, 2000.

44. International Organization for Standardization. *ISO 13485:2016. Medical Devices--Quality Management Systems--Requirements for Regulatory Purposes.* Geneva, 2016.

45. International Society of Pharmaceutical Engineers. *GAMP 5 Guide: Compliant GxP Computerized Systems.* Bethesda, Md., 2008.

46. U.S. Food and Drug Administration. *General Principles of Software Validation; Final Guidance for Industry and FDA Staff;* U.S. Department Of Health and Human Services: Rockville, Md., Jan 2002.

47. McDowall, R. *Validation of Chromatography Data Systems: Meeting Business and Regulatory Requirements: Edition 2;* Royal Society of Chemistry: Cambridge, 2017.

48. U.S. Pharmacopeial Convention. General Chapter <621> Chromatography. In *USP41–NF36;* Rockville, Md., 2017.

49. Dyson, N. *Chromatographic Integration Methods: Edition 2 (RSC Chromatography Monographs),* 2nd ed.; The Royal Society of Chemistry: Cambridge UK, 1998.

50. U.S. Food and Drug Administration. Warning Letter No. 320-15-01 to Sharp Global Limited dated 10/15/14 from Office of Compliance, Center for Drug Evaluation and Research. FDA's Electronic Reading Room - Warning Letters. https://www.fda.gov/iceci/enforcementactions/warningletters/2014/ucm421988.htm (accessed Feb 28, 2017).

51. U.S. Food and Drug Administration. Warning Letter No. 320-16-07 to Ipca Laboratories Ltd. dated 1/29/16. FDA's Electronic Reading Room - Warning Letters. https://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2016/ucm484910.htm (accessed Feb 28, 2017).

52. U.S. Food and Drug Administration. Warning Letter No. 320-15-17 to Unimark Remedies Ltd. dated 9/28/15 from Office of Compliance, Center for Drug Evaluation and Research. FDA's Electronic Reading Room - Warning Letters. https://www.fda.gov/iceci/enforcementactions/warningletters/2015/ucm465626.htm (accessed Feb 28, 2017).

53. U.S. Food and Drug Administration. Warning Letter No. 320-15-05 to Micro Labs Limited dated 1/9/15 from Office of Compliance, Center for Drug Evaluation and Research. FDA's Electronic Reading Room - Warning Letters. https://www.fda.gov/iceci/enforcementactions/warningletters/2015/ucm431456.htm (accessed Feb 28, 2017).

54. Guttman, B.; Roback, E. Chapter 18: Audit Trails. In *Introduction to Computer Security: The NIST Handbook, NIST Special Publication 800-12;* Government Printing Office: Washington, D.C., Oct 1995; pp 211-222.

55. U.S. Food and Drug Administration. Warning Letters by year, 1998–current. Warning Letters and Notice of Violation Letters to Pharmaceutical Companies. https://www.fda.gov/Drugs/GuidanceComplianceRegulatoryInformation/EnforcementActivitiesbyFDA/WarningLettersandNoticeofViolationLetterstoPharmaceuticalCompanies/default.htm (accessed March 1, 2017).

Terms of Usage for PDA Electronic Publications (Technical Reports, Books, etc.)
An **Authorized User** of this electronic publication is the purchaser.

Authorized Users are permitted to do the following:

- Search and view the content of the PDA Electronic Publication
- Download the PDA Electronic Publication for the individual use of an Authorized User
- Print the PDA Electronic Publication for the individual use of an Authorized User
- Make a reasonable number of photocopies of a printed PDA Electronic Publication for the individual use of an Authorized User

Authorized Users are not permitted to do the following:

- Allow anyone other than an Authorized User to use or access the PDA Electronic Publication
- Display or otherwise make any information from the PDA Electronic Publication available to anyone other than an Authorized User
- Post the PDA Electronic Publication or portions of the PDA Electronic Publication on websites, either available on the Internet or an Intranet, or in any form of online publications without a license from PDA, Inc.
- Transmit electronically, via e-mail or any other file transfer protocols, any portion of the PDA Electronic Publication
- Create a searchable archive of any portion of the PDA Electronic Publication
- Use robots or intelligent agents to access, search and/or systematically download any portion of the PDA Electronic Publication
- Sell, re-sell, rent, lease, license, sublicense, assign or otherwise transfer the use of the PDA Electronic Publication or its content
- Use or copy the PDA Electronic Publication for document delivery, fee-for-service use, or bulk reproduction or distribution of materials in any form, or any substantially similar commercial purpose
- Alter, modify, repackage or adapt any portion of the PDA Electronic Publication
- Make any edits or derivative works with respect to any portion of the PDA Electronic Publication including any text or graphics
- Delete or remove in any form or format, including on a printed article or photocopy, any copyright information or notice contained in the PDA Electronic Publication
- Combine any portion of the PDA Electronic Publication with any other material

To License or purchase Reprints

- **Licensing:** Site licenses and licenses to distribute PDA Electronic Publication can be obtained for a fee.
  To learn more about licensing options and rates, please contact:
  Janny Chua, Publications Manager, +1 (301) 656-5900,
  ext. 133. Written correspondence can be sent to: PDA, Inc. Attn: Janny Chua, 4350 East West Highway,
  Suite 150, Bethesda, MD 20814.
- **Reprints:** Reprints of PDA Electronic Publication can be purchased for a fee.
  To order reprints, please contact:
  Janny Chua, Publications Manager, +1 (301) 656-5900, ext. 133.

Written correspondence can be sent to: PDA, Inc. Attn: Janny Chua, 4350 East West Highway, Suite 150, Bethesda, MD 20814.

Technical Report No. 80

About PDA Technical Reports

PDA Technical Reports are global consensus documents, prepared by member-driven Task Forces (listed on inside front cover) comprised of content experts, including scientists and engineers working in the pharmaceutical/biopharmaceutical industry, regulatory authorities and academia. While in development, PDA Technical Reports are subjected to a global review of PDA members and other topic-specific experts, often including regulatory officials. Comments from the global review are then considered by the authoring Task Force during the preparation of the final working draft. The level of expertise of the Task Force and those participating in the global review ensure a broad perspective reflecting best thinking and practices currently available.

The final working draft is next reviewed by the PDA Advisory Board or Boards that sanctioned the project. PDA's Advisory Boards are: Science Advisory Board, Biotechnology Advisory Board, and Regulatory Affairs and Quality Committee. Following this stage of review, the PDA Board of Directors conducts the final review and determines whether to publish or not publish the document as an official PDA Technical Report.

While PDA goes to great lengths to ensure each Technical Report is of the highest quality, all readers are encouraged to contact PDA about any scientific, technical, or regulatory inaccuracies, discrepancies, or mistakes that might be found in any of the documents. Readers can email PDA at: TRfeedback@pda.org.

PDA Publication Production and Editing

Denyse Baker, *Director, Scientific & Regulatory Affairs*
Tina Morris, *VP, Scientific & Regulatory Affairs*
Walter Morris, *Director of Publishing*
Katja Yount, *Publication Designer*
Marilyn Foster, *Technical Editor/Writer*

PDA®
Parenteral Drug Association

Bethesda Towers
4350 East West Highway
Suite 600
Bethesda, MD 20814 USA
Tel: +1 (301) 656-5900
Fax: +1 (301) 986-0296
E-mail: info@pda.org
Web site: www.pda.org