Mitigating Data Integrity Risk in Analytical Methods and Stability Testing

Chris Wubbolt

Laboratory Data Integrity

December 4, 2017

Training Objectives

- **Quick Review of Data Integrity Basics**
- **Discuss Laboratory Data Integrity Issues Found in Audits and Inspections**
- **Implement Electronic Controls around Data Integrity**
- **Exercise**

Data Integrity

Data Integrity

- Completeness, consistency, and accuracy of data.

- Attributable
- Legible
- Contemporaneous
- Original (or true copy)
- Accurate

ALCOA +

- Enduring
- Complete
- Consistent
- Available

Current Regulatory Requirements and Guidance

March 2015	September 2015	April 2016
• MHRA - GMP Data Integrity Definitions and Guidance for Industry	• WHO - Guidance on Good Data and Record Management Practices	• FDA – Data Integrity Guidance and Compliance with CGMP

July 2016	August 2016	August 2016
• MHRA - GxP Data Integrity Definitions and Guidance for Industry	• PIC/S - Good Practices for Data Management and Integrity	• EMA – Data Integrity Guidance Q&A

Data Integrity Requirements

21 CFR 211.180 (d)	Records required under this part may be retained either as **original records** or as **true copies** such as photocopies, microfilm, microfiche, or other accurate reproductions of the original records.
21 CFR 211.194 (a)	Laboratory records shall include **complete data derived from all tests** necessary to assure compliance with established specifications and standards, including examinations and assays, including

- (4) A **complete record** of all data secured in the course of each test.
- (7) The initials or signature of the person who performs each test and the date(s) the tests were performed.
- (8) The initials or signature of a second person showing that the original records have been reviewed for accuracy, completeness, and compliance with established standards.

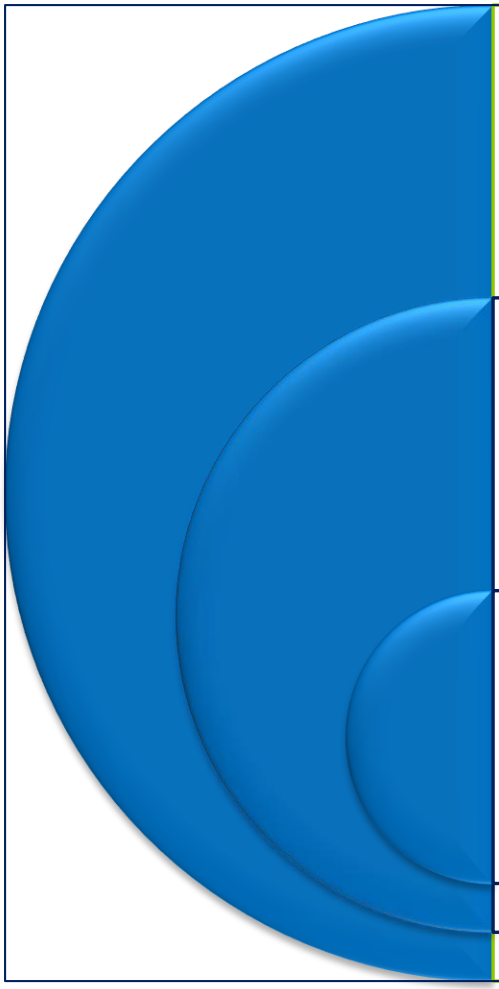
Q&A on CGMP, Good Guidance Practices, Level 2 Guidance - Records and Reports (August 2010)*

How do the Part 11 regulations and "predicate rule requirements" (in 21 CFR Part 211) apply to the electronic records created by computerized laboratory systems and the associated printed chromatograms that are used in drug manufacturing and testing?

- The printed paper copy of the chromatogram would not be considered a “true copy” of the entire electronic raw data used to create that chromatogram, as required by 21 CFR 211.180(d).
- The printed chromatogram would also not be considered an “exact and complete” copy of the electronic raw data used to create the chromatogram.
- The chromatogram does not generally include, for example, the injection sequence, instrument method, integration method, or the audit trail, of which all were used to create the chromatogram or are associated with its validity.
- Therefore, the printed chromatograms used in drug manufacturing and testing do not satisfy the predicate rule requirements in 21 CFR Part 211.

* https://www.fda.gov/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/ucm124787.htm

FDA Guidance

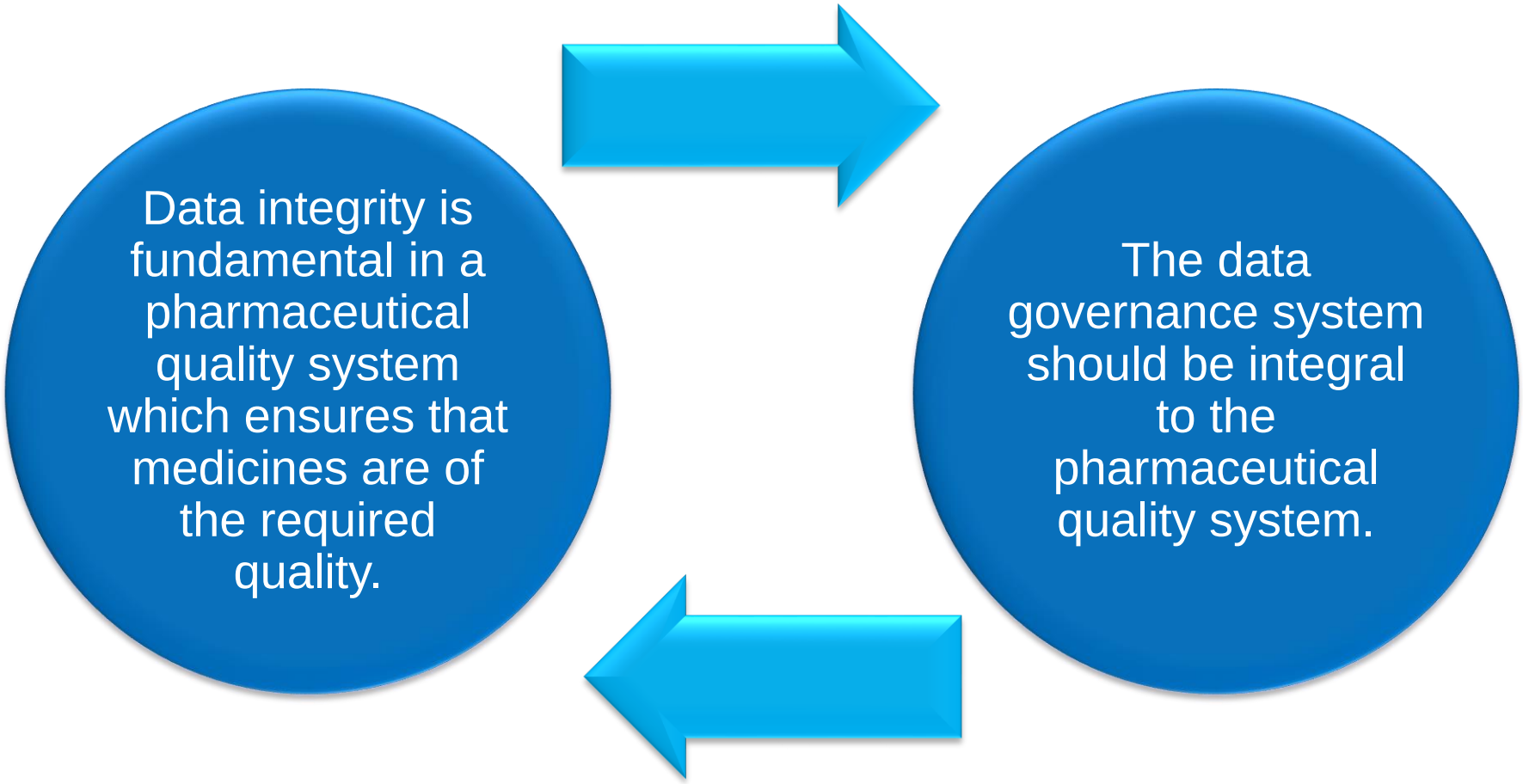


FDA expects data to be accurate and reliable.

Flexible and risk-based strategies to prevent and detect data integrity issues.

Ensuring data integrity is an important component of industry's responsibility to ensure the safety, efficacy, and quality of drugs, and of FDA's ability to protect the public health.

MHRA Guidance

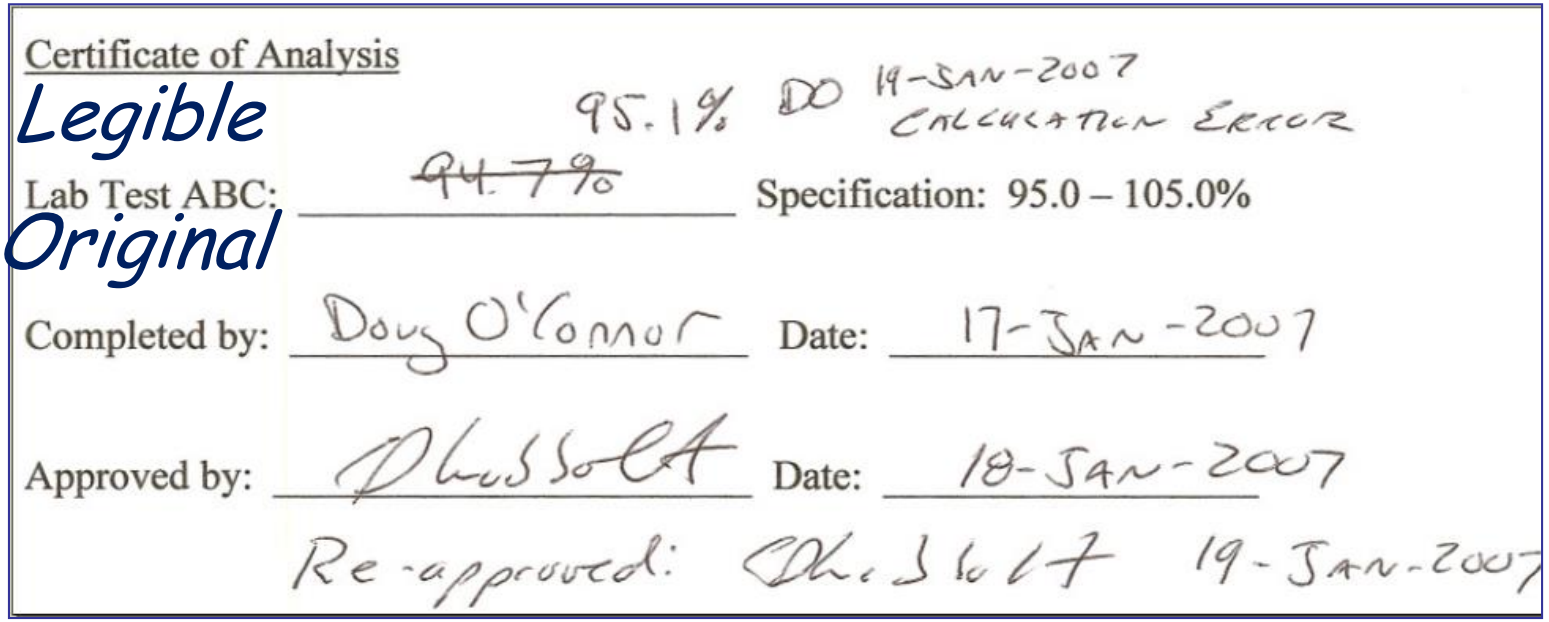


MHRA Guidance

▪Data Governance System	• Policies and procedures • Training
Data Lifecycle	• Initial generation to archival / destruction
Risk	• Degree of effort should be commensurate with data criticality.

Data Integrity - Paper

Accurate and Complete



Certificate of Analysis

95.1% DO 19-JAN-2007 CALCULATION ERROR

Lab Test ABC: ~~94.7%~~ Specification: 95.0 – 105.0%

Completed by: Doug O'Connor Date: 17-JAN-2007

Approved by: [signature] Date: 18-JAN-2007

Re-approved: [signature] 19-JAN-2007

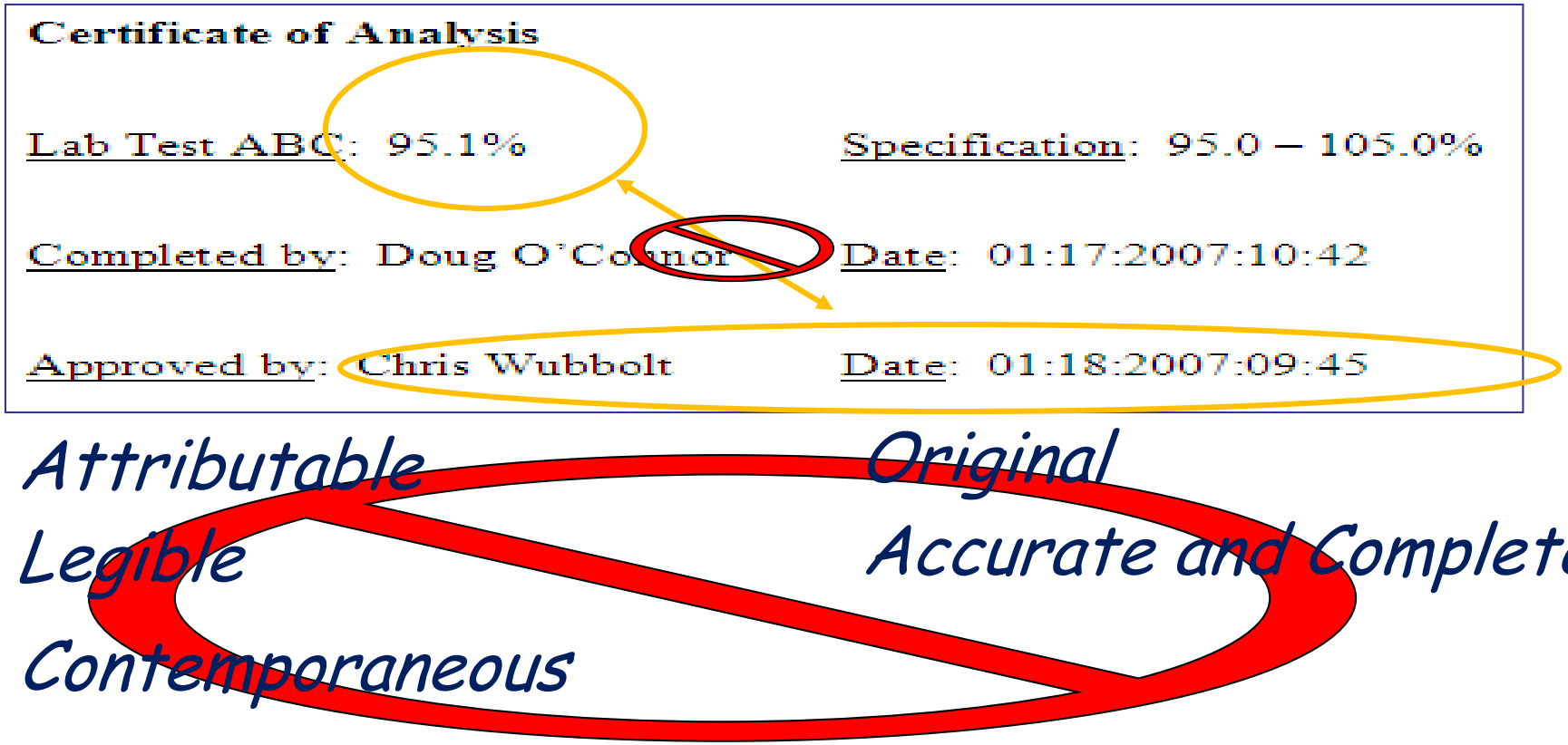
Legible

Original

Attributable

Contemporaneous

Data Integrity - Electronic



Data Integrity - Electronic

Certificate of Analysis

Legible

Lab Test ABC: 95.1%

Specification: 95.0 – 105.0%

Completed by: Doug O'Connor

Date: 01:19:2007:08:45

Attributable

Contemporaneous

Approved by: Chris Wubbolt

Date: 01:19:2007:09:33

Original

Event	User ID	Previous Value	New Value	Date	Time	Reason
Data Entry	DOCon	NA	94.7	1/17/2007	10:42 EST	NA
Approval	Cwubb	NA	NA	1/18/2007	09:45 EST	NA
Data Change	DOCon	94.7	95.1	1/19/2007	8:45 EST	Calculation Error
Approval	Cwubb	NA	NA	1/19/2007	9:33 EST	NA

Accurate and Complete

FDA Guidance

Key Points

- Key Terms
- Define “data” and how it is used
  - Original and True Copy
  - Static vs Dynamic
  - Metadata and audit trails
  - Review of electronic data
- Validation
- Operation and use of systems
- Reporting and Retention
- Handling of Data Integrity Issues

MHRA Guidance - Data

Original record

- Data as the file or format in which it was originally generated, preserving the integrity (accuracy, completeness, content and meaning) of the record, e.g. original paper record of manual observation, or electronic raw data file from a computerised system

True Copy

- A copy of original information that been verified as an exact (accurate and complete) copy having all of the same attributes and information as the original. A true copy may be retained in a different electronic file format to the original record, if required, but must retain the equivalent static/dynamic nature of the original record.

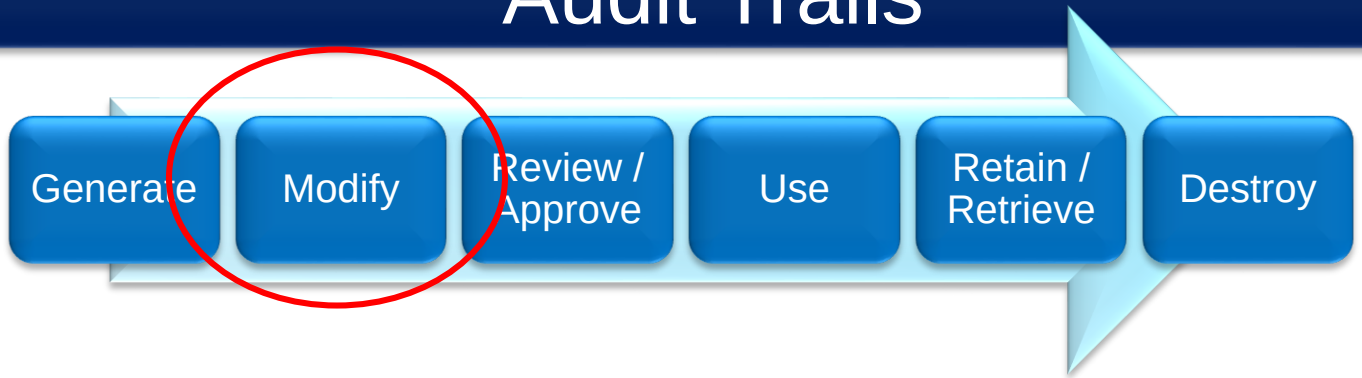
MHRA Guidance
Terms and Definitions

Metadata

- Data that describes attributes of other data, and provide context and meaning.
- Without metadata, data has no meaning.
  - Example

3.5 *sodium chloride batch 1234,* ***3.5*** *mg.*
J Smith 01/07/14

FDA Guidance
Audit Trails



- Audit trails that capture changes to critical data be reviewed with each record and before final approval of the record.

FDA recommends routine scheduled audit trail review based on the complexity of the system and its intended use.

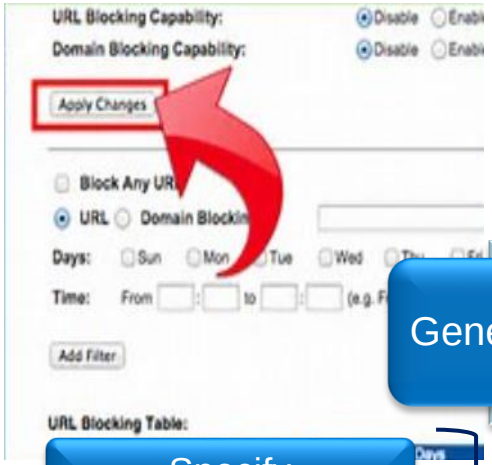
Audit Trails

- Upon review of the audit trail configuration within LIMS, audit trails were turned off for many of the tables within the XXX Module.

Documentation was not available to justify why the audit trails for these tables was turned off. For example,

- The audit trail was not turned on for the XXX table, which is used when jobs, such as stability time pulls, are cancelled or suspended.
- This was observed by reviewing the audit trail configuration within the system.
- Audit trail configuration is documented within Design specification, XXX, YYY, version 2.0, approval date 11-Mar-2016.

Data Lifecycle

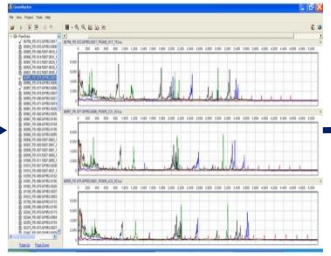


Generate → Modify → Review / Approve → Use → Retain / Retrieve → Destroy

Validation:
- Specify
- Design
- Configure
- Verify

Understanding the Data Flow

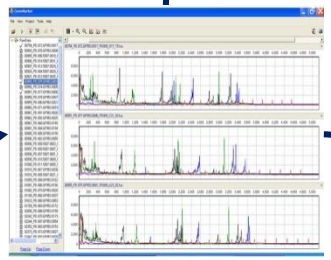
LIMS



… throughout the record lifecycle

Backup

LIMS



Retention

Destruction

FDA Guidance
Static & Dynamic Records

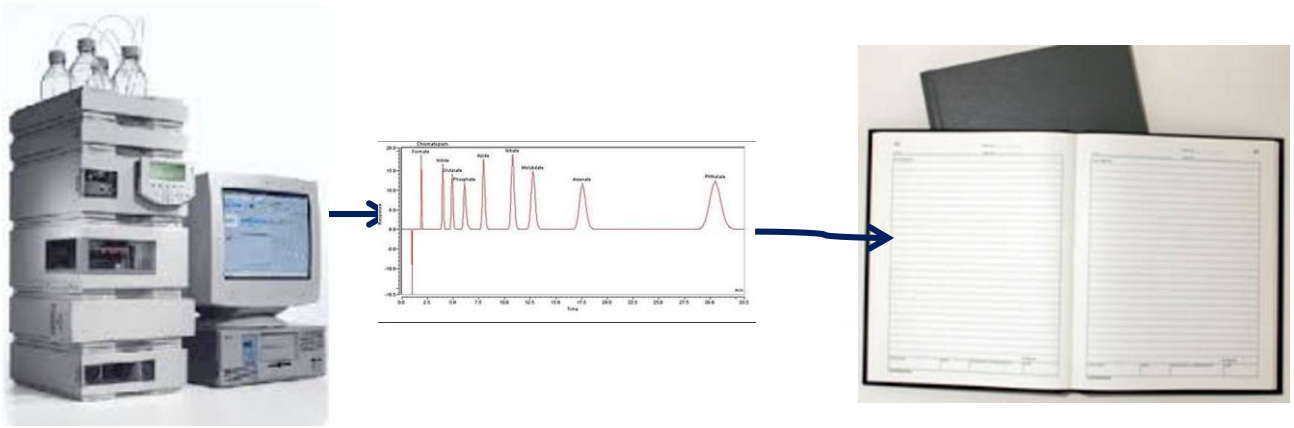
Static

- Fixed-data document such as a paper record or an electronic image.

Dynamic

- Format that allows interaction between the user and the record content.
- Chromatographic Record
  - Allows user to change the baseline.
  - Reprocess chromatographic data.
  - Resulting peaks may appear smaller or larger.
- Spreadsheet
  - User modification of formulas or entries used to compute test results.

Static / Dynamic Data



Static / Dynamic Data

Project Name: Redacted

Reported by User: Redacted

System Suitability Report

Sample Set Name Redacted

System Name SYSTEM 15

Processed By Redacted/Analyst

Sample Set Start Date 9/15/2015 9:37:45 AM EDT

Run Time 8.00 Minutes
Injection Volume 10.00 ul

WriteUp_Page_Num Redacted

Result Set Id Redacted

Peak Results
Name: Redacted

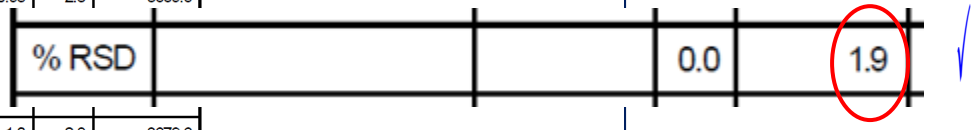
	SampleName	Name	RT	Area	USP Tailing	K Prime	USP Plate Count
1	SYSSUIT-1		4.8	222567.99	0.95	2.8	3654.4
2	SYSSUIT-2		4.8	221851.61	0.95	2.8	3666.7
3	SYSSUIT-3		4.8	221019.54			6
4	SYSSUIT-4		4.8	291670.44			0
5	SYSSUIT-5		4.8	222059.11	0.95	2.8	3669.6
Mean			4.8	221833.74			
% RSD			0.0	1.9			
Min							
Max					1.0	2.8	3679.6

291670.44

System Suitability: %RSD < 2.0%

%RSD 3.9%

X



MHRA Guidance
Terms and Definitions

Validation

- Comply with EU GMP Annex 11.
- Requires an understanding of the computerised system's function within a process.
- **The acceptance of vendor-supplied validation data in isolation of system configuration and intended use is not acceptable**.
- In isolation from the intended process, vendor testing is likely to be limited to functional verification only, and may not fulfil the requirements for performance qualification.

The assessment – Intended Use / Documentation Review

Approval of Records

- Internal assessment of Stability LIMS
- Vendor Supplied Documentation Provided
  - User Requirements Specification
  - User Acceptance Test
- URS – Included statement “the system has a ‘configurable option’ for ….. electronic signatures”.
- Requested configuration specification – none available
- Reviewed configuration within system – esigs turned off
- Requested system demonstration – approval by pressing approve button
- Reviewed UAT documentation – esigs functionality passed
  - First step of test – turn on esig functionality
  - Last step of test – turn off esig functionality
- Record integrity issue – lack of approved stability protocols and results

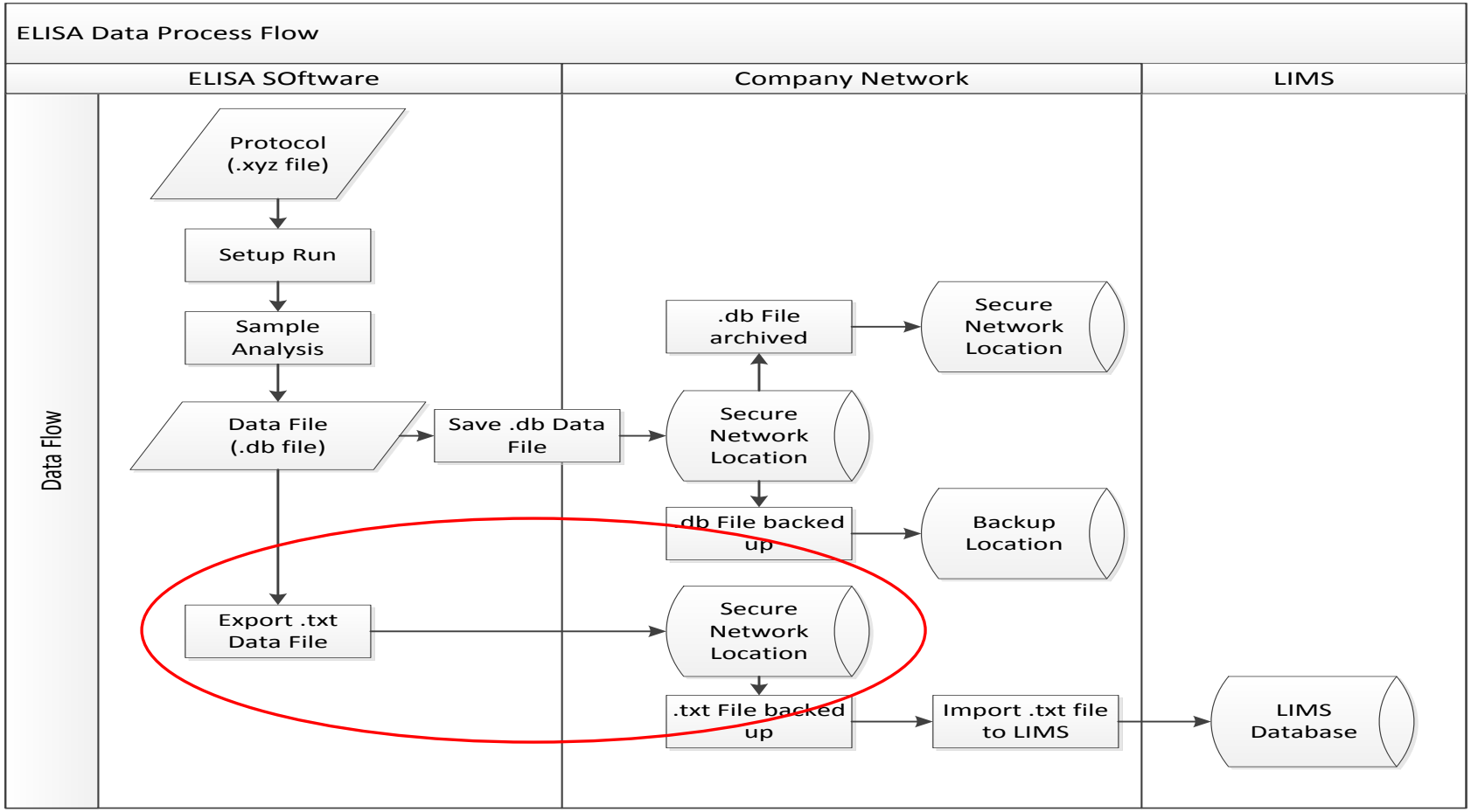
Data Lifecycle

Non-Standard Build

"Standard Build"

- ~~Date/time stamp controls~~
- ~~Network backup~~
- ~~Access controls~~
- Audit logs not backed up
- User access not controlled

Identify Potential Data Integrity Risks



“Prevent & Detect”

Firms should implement meaningful and effective strategies to manage their data integrity risks based upon their process understanding and knowledge management of technologies and business models.

Data Integrity – Good Documentation Practices

- Use indelible (permanent blue or black ink).
- Do not use pencil, correction fluid or tape.
- Do not obliterate original entry.
- Use single line cross-out, initial, date, reason for change.
- Record data only on GMP documents.
- Do not record data on unofficial documents (paper towels, note pads, etc.).
- Record data when activities are completed.

Data Integrity

Good Documentation Practices

- Error Codes

- Codes:
  - TE – Transcription Error
  - CE – Calculation Error
  - WD – Wrong Date
  - WT – Wrong Time
  - WO – Write Over
  - EE – Entry Error
- Use of foot notes is acceptable

Documentation Practices

Changes were needed to item 2#.

Serial number ~~9431~~ 9121.
wrong entry
CDW 10-31-2005

The report printed successfully.
No errors were ~~not~~ observed
typo
CDW 10-31-2005

Report did not print.

Single Line

Reason

Initial and Date

Certificate of Analysis

Laboratory Record Review

- pH
  - Result was originally recorded as 5.4; the spec is ≥5.8 to ≤6.5. A reason for this change was recorded as entry error.
- Polysorbate 80
  - Gross weight changed from 14.5651 to 14.5129, but change was only made after net weight was calculated.

FDA Guidance
Controls to manage risks

- Implement appropriate controls to manage risks associated with each element of the system.

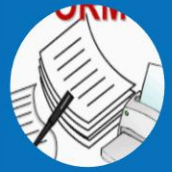
Controls that are appropriately designed to validate a system for its intended use address software, hardware, personnel, and documentation.

Start the assessment

Low Hanging Fruit

Access to clocks for recording timed events.

Accessibility of records at locations where activities take place so ad hoc data recording and later transcription to official records is not necessary.



'Free access' to blank paper forms for raw/source data recording should be controlled where this is appropriate. Reconciliation may be necessary to prevent recreation of a record.

User access rights that prevent (or audit trail) unauthorized data amendments.

Automated data capture or printers attached to equipment such as balances.

Control of physical parameters (time, space, equipment) that permit performance of tasks and recording of data as required.

Access to raw data for staff performing data checking activities.

Considerations when performing laboratory data integrity assessments

There are many different types of lab systems with different data types.

The same instrument and system can be setup and configured differently at different companies.

Paper, electronic, and hybrid systems need to be assessed.

Assess the data throughout the ***entire*** data flow and data lifecycle.

Data Integrity throughout the Lifecycle

Backup and Restore

Backup and Restore

- Analytical Laboratory
- Backup and Restore SOP
  - Failed backup required a help desk ticket
  - 3 failed backups require notification to Director of Infrastructure Technology
  - 5 failed backups require notification to CTO
- Requested backup logs for three months
- No successful backups for June or first two weeks of July
- No help desk tickets generated for month of June
- Director and CTO were not notified
- Director and CTO were not aware of failures
- Potential Data Integrity Issue

Backup and Restore

Backup and Restore

- Recent Audit – October 2017
- Requested Backup Logs for database server
  - Several failures and missed backups
- No evidence of investigation
- Requested restore test
- SOP requirement was 2 restore tests per year
- Restore test was completed June 2017
- Reviewed restore test and asked what type of record was restored
- Type of record restored?
  - 19 KB Text File
- Finding - Did not demonstrate ability to restore database

Data Integrity Assessments

- Formal Quality program
- Knowledgeable assessors
- Checklists?
- Personnel availability
  - System users
  - System administrators
- Access to the system
- Access to the data
  - Including the metadata / audit trails
- Follow the data lifecycle
- Documentation Review

The assessment

Watch the operator log onto the system

- Login
- Active Directory?

Check the menu options

- Logs
- Configuration
- How are standard tests setup?

Administrators

- How many administrators?
- Who do they report to?
- Are there shared accounts?
- How are users setup?
- What are the user levels?

The assessment

Data

- Is raw data defined?
- Where is the data saved?
- How are audit trail records maintained?
- Check Explorer and directories where data is stored
  - Are the dates and times sequential
  - Are there gaps in the data files?
- Check the recycle bin!

The assessment

Data

- Check the paper records
- Look in drawers and in desks

Data Integrity Finding August 2016

- During the facility tour, many quality system documents were found in drawers and other unsecured locations. In addition, some information was recorded on unofficial records, such as notepad pages. For example,
  - Within XYZ Room, a XYZ Document, approved 07-Dec-2015, was found in a drawer. Information was recorded on blank notepad pages. An uncontrolled document titled "XYZ" was found in the drawer within the XYZ Room.
  - Laboratory records dating as far back as November 2015 were found within drawers of the QC Lab.
  - Within the XYZ laboratory, many uncontrolled copies of SOPs and worksheets were identified. Many of the records included post-it notes and other unofficial records.

The assessment

Where does the data end up?

- Is there a printout? How is it used?
- Are data files maintained on the workstation?
- Are data files maintained on a server?
- Can the data be modified? Can the data be deleted?
- How is the data reviewed?
- Is there an interface to a LIMS?

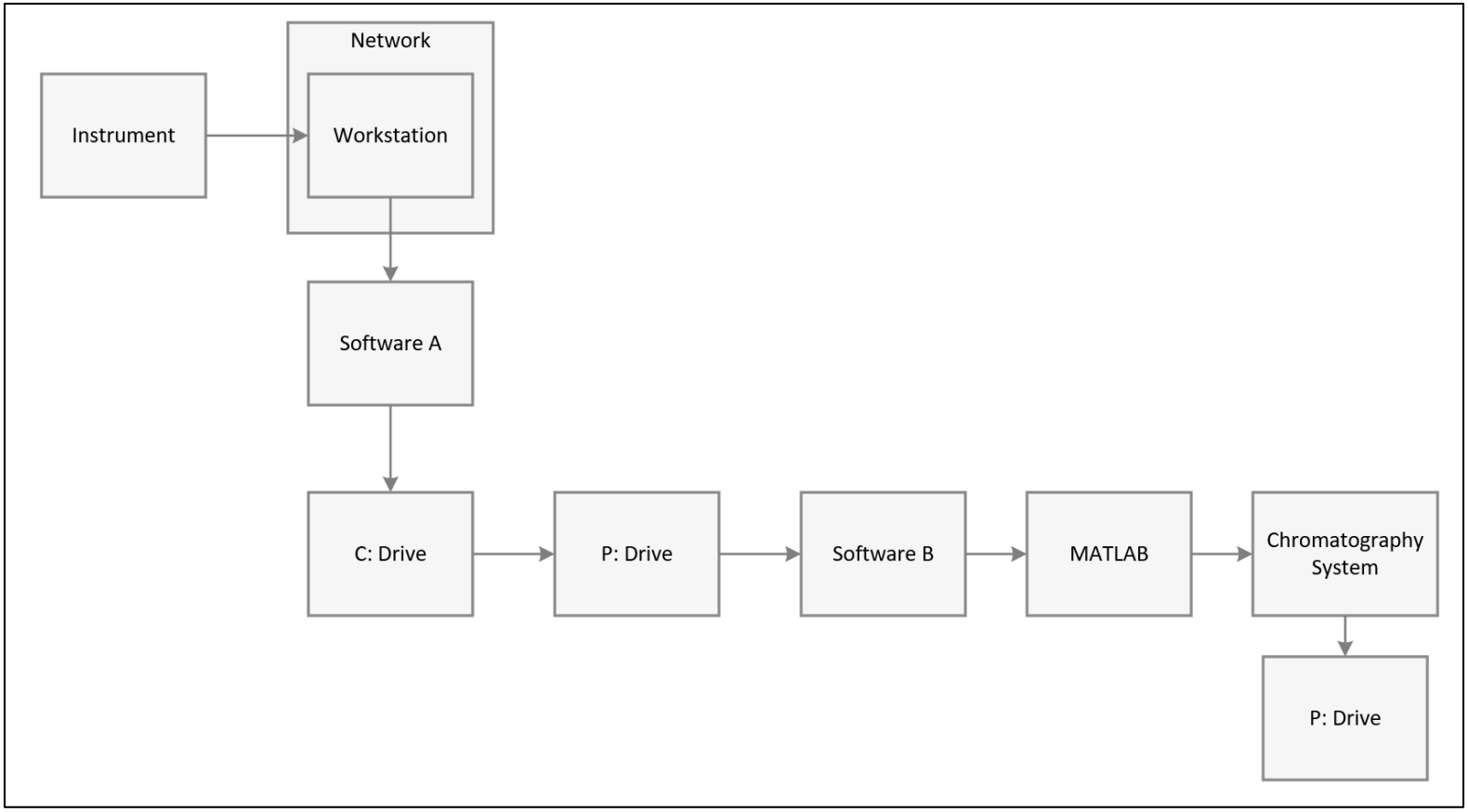
FDA Guidance

- It is not acceptable to record data on pieces of paper that will be discarded after the data are transcribed to a permanent laboratory notebook.

Similarly, it is not acceptable to store data electronically in temporary memory, in a manner that allows for manipulation, before creating a permanent record.

Electronic data that are automatically saved into temporary memory do not meet CGMP documentation or retention requirements.

Assess Data Integrity for entire data flow



FD-483 July 2016

Observation 2

Failure to ensure that computerized systems have sufficient controls to prevent unauthorized access or changes to data, or record of any data change made, the previous entry, who made the change, and when the change was made.

For example:

1) No audit trail function was enabled for the endotoxin test analysis software, which is used for all kinetic/ turbidometric endotoxin testing of [redacted]. A Quality Specialist demonstrated that they were able to access the raw data folder on the computer's network hard-drive, while logged in on an analyst account, and delete files associated with endotoxin testing. While data backups occur on a 24 hour cycle, no controls were in-place to prevent or detect changes or deletion of endotoxin test raw data performed prior to being backed up.

2) No procedures have been established governing the usage or review of audit trails for the endotoxin system software.

Sekisui Warning Letter – November 8, 2016

1. Failure to maintain complete data derived from all laboratory tests conducted to ensure compliance with established API specifications and standards.

Our investigator found that you failed to maintain complete data from all laboratory analyses, and that you relied on the incomplete information to determine whether your drugs met established specifications. For example:

a. Numerous data files were found in the recycle bin folder on the computer connected to gas chromatography instruments GC-4 and GC-6. Specifically, our investigator found deleted data for residual solvent testing for **(b)(4)** lot **(b)(4)** in the recycle bin. Your records show that you retested the lot without documented justification or an investigation. You retained only the final test result.

b. During the inspection our investigator requested residual solvent release test data for two of your API, **(b)(4)** and **(b)(4)**. You were unable to retrieve this data.

Any data created as part of a CGMP record must be retained so that it can be evaluated by the quality unit as part of release criteria and maintained for CGMP purposes.

We acknowledge that you commit to revising your SOP for archiving data. Your response is inadequate because it does not explain your failure to maintain complete records prior to the inspection. You also did not address validation of the systems you use to archive your data.

Because your methods, facilities, or controls for manufacturing, processing, packing, or holding do not conform to CGMP, your API are adulterated within the meaning of section 501(a)(2)(B) of the Federal Food, Drug, and Cosmetic Act (FD&C Act), 21 U.S.C. 351(a)(2)(B).

We reviewed your July 8, 2016, response in detail and acknowledge receipt of your subsequent correspondence.

During our inspection, our investigator observed specific deviations including, but not limited to, the following.

1. Failure to maintain complete data derived from all laboratory tests conducted to ensure compliance with established API specifications and standards.

associated audit trails as part of the batch release process.

3. Failure to ensure that your analytical methods used to test API are appropriately validated and verified.

Our investigator found that your microbiological test methods were not adequately verified and that stability test methods were inadequately validated. For example:

a. **(b)(4)** of your nonsterile API are intended for use in the manufacture of sterile finished dosage forms for U.S. distribution. You did not appropriately verify your test methods for total aerobic microbial count and total combined yeasts and molds. Specifically, you did not show that these methods are capable of recovering microorganisms in the presence of the API.

Sekisui Warning Letter – November 8, 2016

2. Failure to prevent unauthorized access or changes to data, and failure to provide adequate controls to prevent omission of data.

Our investigator observed that your laboratory systems lacked controls to prevent deletion of and alterations to electronic raw data. You do not have adequate controls for seven of **(b)(4)** high performance liquid chromatography (HPLC) systems and one of **(b)(4)** gas chromatography systems. For example, the audit trail on HPLC 15 did not record the **(b)(4)** batch **(b)(4)** assay. Your records indicate that the assay was performed on March 3, 2014, but your audit trail shows no assays performed between February 28 and March 4, 2014. Moreover, your analyst demonstrated to our investigator that he could change the data, including injection time and date, without the changes being captured in the audit trail, prior to printing the results.

We acknowledge that you have committed to upgrading your analytical systems to be compliant with CGMP requirements. However, procuring new instruments, installing new and upgraded data acquisition software, and enabling various features on software are not sufficient alone. These steps will be effective only if you implement appropriate procedures and systems to ensure that your quality unit reviews all production and control data and associated audit trails as part of the batch release process.

3. Failure to ensure that your analytical methods used to test API are appropriately validated and verified.

We reviewed your July 8, 2016, response in detail and acknowledge receipt of your subsequent correspondence.

During our inspection, our investigator observed specific deviations including, but not limited to, the following.

1. Failure to maintain complete data derived from all laboratory tests conducted to ensure compliance with established API specifications and standards.

Our investigator found that your microbiological test methods were not adequately verified and that stability test methods were inadequately validated. For example:

a. **(b)(4)** of your nonsterile API are intended for use in the manufacture of sterile finished dosage forms for U.S. distribution. You did not appropriately verify your test methods for total aerobic microbial count and total combined yeasts and molds. Specifically, you did not show that these methods are capable of recovering microorganisms in the presence of the API.

Sekisui Warning Letter – November 8, 2016

Data Integrity Remediation

Your quality system does not adequately ensure the accuracy and integrity of data to support the safety, effectiveness, and quality of the drugs you manufacture. We strongly recommend that you retain a qualified consultant to assist in your remediation. In response to this letter, provide the following.

A. A comprehensive investigation into the extent of the inaccuracies in data records and reporting. Your investigation should include:

- A detailed investigation protocol and methodology; a summary of all laboratories, manufacturing operations, and systems to be covered by the assessment; and a justification for any part of your operation that you propose to exclude.
- Interviews of current and former employees to identify the nature, scope, and root cause of data inaccuracies. We recommend that these interviews be conducted by a qualified third party.
- An assessment of the extent of data integrity deficiencies at your facility. Identify omissions, alterations, deletions, record destruction, non-contemporaneous record completion, and other deficiencies. Describe all parts of your facility's operations in which you discovered data integrity lapses.
- A comprehensive retrospective evaluation of the nature of the testing data integrity deficiencies. We recommend that a qualified third party with specific expertise in the area where potential breaches were identified should evaluate all data integrity lapses.

B. A current risk assessment of the potential effects of the observed failures on the quality of your drugs. Your assessment should include analysesof the risks to patients caused by the release of drugs affected by a lapse of data integrity, and risks posed by ongoing operations.

- A status report for any of the above activities already underway or completed.

Sekisui Warning Letter – November 8, 2016

Data Integrity Remediation

C. A management strategy for your firm that includes the details of your global corrective action and preventive action plan. Your strategy should include:

- A detailed corrective action plan that describes how you intend to ensure the reliability and completeness of all of the data you generate, including analytical data, manufacturing records, and all data submitted to FDA.
- A comprehensive description of the root causes of your data integrity lapses, including evidence that the scope and depth of the current action plan is commensurate with the findings of the investigation and risk assessment. Indicate whether individuals responsible for data integrity lapses remain able to influence CGMP-related or drug application data at your firm.
- Interim measures describing the actions you have taken or will take to protect patients and to ensure the quality of your drugs, such as notifying your customers, recalling product, conducting additional testing, adding lots to your stability programs to assure stability, drug application actions, and enhanced complaint monitoring.
- Long-term measures describing any remediation efforts and enhancements to procedures, processes, methods, controls, systems, management oversight, and human resources (e.g., training, staffing improvements) designed to ensure the integrity of your company's data.
- A status report for any of the above activities already underway or completed.

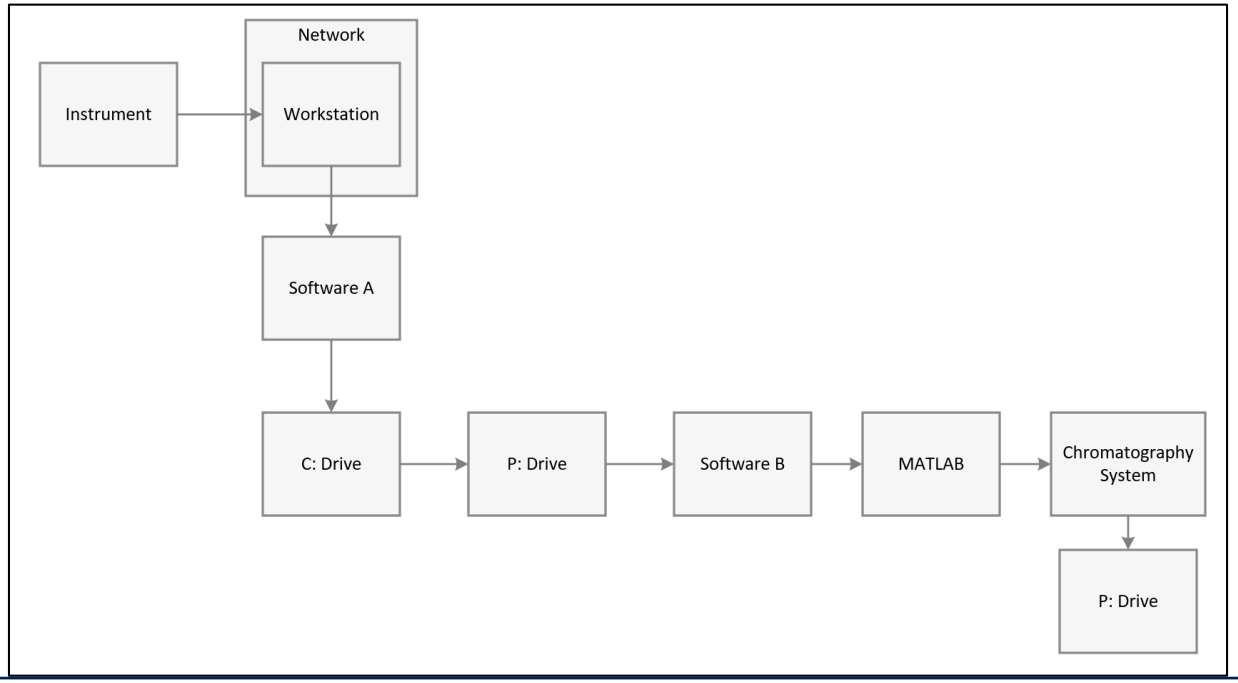
application data at your firm.
- Interim measures describing the actions you have taken or will take to protect patients and to ensure the quality of your drugs, such as notifying your customers, recalling product, conducting additional testing, adding lots to your stability programs to assure stability, drug application actions, and enhanced complaint monitoring.
- Long-term measures describing any remediation efforts and enhancements to procedures, processes, methods, controls, systems, management oversight, and human resources (e.g., training, staffing improvements) designed to ensure the integrity of your company's data.
- A status report for any of the above activities already underway or completed.

Exercise

1. Review previous warning letter and identify controls and processes necessary to ensure data integrity requirements are met.

Exercise

2. Identify data integrity controls that should be implemented to mitigate the data integrity risks associated with the data flow.



Training Summary

- **Review of Data Integrity Basics**
- **Review of Laboratory Data Integrity Issues Found in Audits and Inspections**
- **Implement Electronic Controls around Data Integrity**
- **Exercise**

Questions

Chris Wubbolt

QACV Consulting, LLC

Telephone: 610-442-2250

E-mail: chris.wubbolt@QACVConsulting.com