Electronic Data Integrity

By Treximo

800 Hillgrove Avenue, Suite 201, Western Springs, IL 60558
treximo.com | +1(847) 295-7160

Validation Center™
validationcenter.com

Electronic Data Integrity

v.21.13

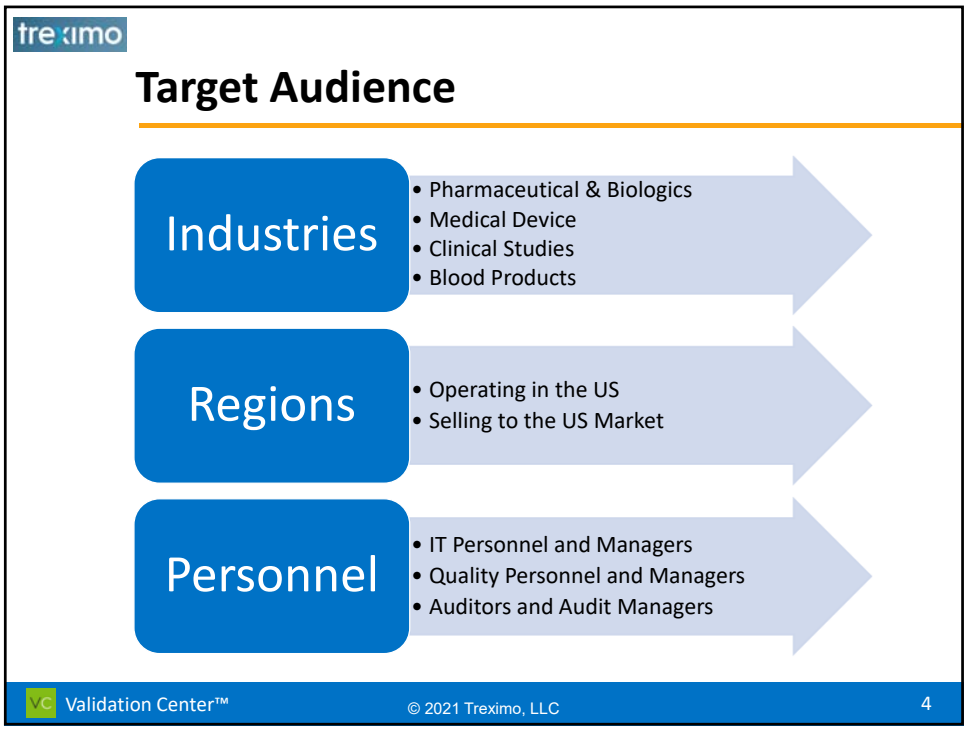
1

Your Presenter

- Debra Bartel, MBA, CQA, PMP
- VP, Life Sciences QA
- 30 years experience specializing in software quality assurance, validation and regulatory compliance, Information Systems project management, and process design.
- Prior to joining Treximo, held management positions in the pharmaceutical industry in both Quality Assurance and Information Systems organizations
- Active member of American Society for Quality (ASQ), Northeastern Illinois Section, Software Division

2

3



4

Webinar Outline

1. Data Integrity Regulatory History
2. Data Integrity Terminology
3. Electronic Data Integrity Principles
4. Examples of Data Integrity Risks

Validation Center™ © 2021 Treximo, LLC 5

5

Data Integrity Regulatory History

Part 1

6

6

"Data Integrity" Is Not New!

21 CFR 211.100 "… shall be **documented at the time** of performance"	21 CFR 820.180 "… records shall be **legible** and shall be stored to minimize deterioration and to **prevent loss**."	21 CFR 56.115 "… records shall be **accessible for inspection** and copying…"
21 CFR 600.12 "…records shall be **legible and indelible,** shall identify the **person immediately responsible**, shall include **dates**…"	21 CFR 211.194 "… showing that the original records have been reviewed for **accuracy, completeness."**	21 CFR 820.180 "… records stored in automated data processing systems shall be **backed up**."
21 CFR 820.180 "All records required by this part shall be **retained** for a period of time equivalent to…"	21 CFR 211.180 "… may be retained either as **original** records or as **true copies**."	21 CFR 606.160 "Records shall be maintained **concurrently with the performance** of each significant step…"

Validation Center™ © 2021 Treximo, LLC 7

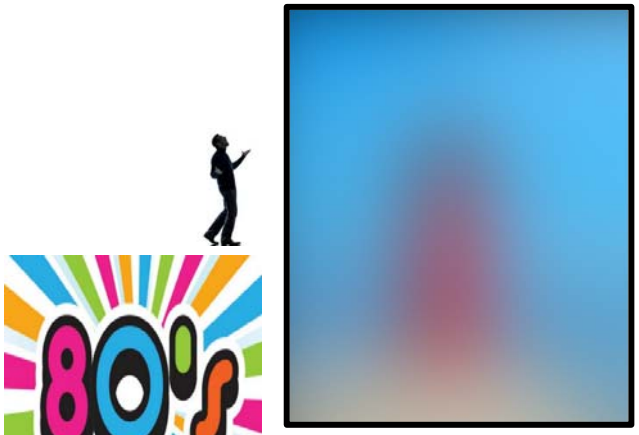
7

"Data Integrity" in the Paper World

Validation Center™ © 2021 Treximo, LLC 8

8

"Data Integrity" for Electronic World



Validation Center™ © 2021 Treximo, LLC 9

9

Regulations Brought Some Clarity

Part 11
Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ **procedures and controls** designed **to ensure the** authenticity, **integrity**, and, when appropriate, the confidentiality **of electronic records**

Part 11
Persons who use **electronic signatures** based upon use of identification codes in combination with passwords shall employ **controls to ensure** their security and **integrity**.

Annex 11
Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, **data integrity** and product quality.
As part of a risk management system, decisions on the extent of validation and **data integrity controls** should be based on a justified and documented risk assessment of the computerised system.

Validation Center™ © 2021 Treximo, LLC 10

10

But GxP Violations Persisted…

In recent years, FDA has increasingly observed CGMP violations involving data integrity during CGMP inspections.

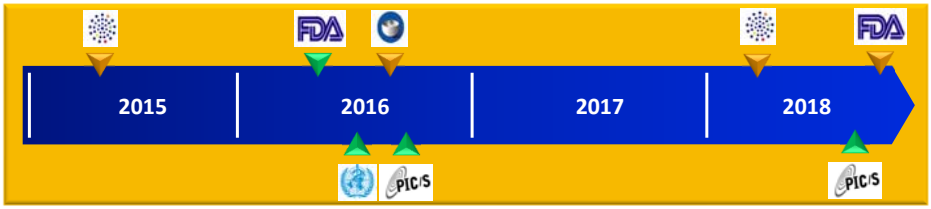
This is troubling because ensuring data integrity is an important component of industry's responsibility to ensure the safety, efficacy, and quality of drugs, and of FDA's ability to protect public health.

These data integrity-related CGMP violations have led to numerous regulatory actions, including Warning Letters, Import Alerts, and Consent Decrees [1]

[1] quotes from Data Integrity and Compliance with Drug CGMP, FDA, December 2018

11

Guidance History



2015 – March: MHRA *GMP Data Integrity Definitions and Guidance for Industry*

2016 – April: FDA [DRAFT] *Data Integrity and Compliance with CGMP Guidance for Industry*

2016 – June: WHO *Guidance on Good Data and Records Management Practices*

2016 – August: EMA *Questions and Answers: Good Manufacturing Practice – Data Integrity Compliance*

2016 – July and August: PIC/S [DRAFT] *Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments*

2018 – March: MHRA *'GxP' Data Integrity Guidance and Definitions*

2018 – November: PIC/S [DRAFT] *Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments*

2018 – December: FDA *Data Integrity and Compliance with Drug CGMP*

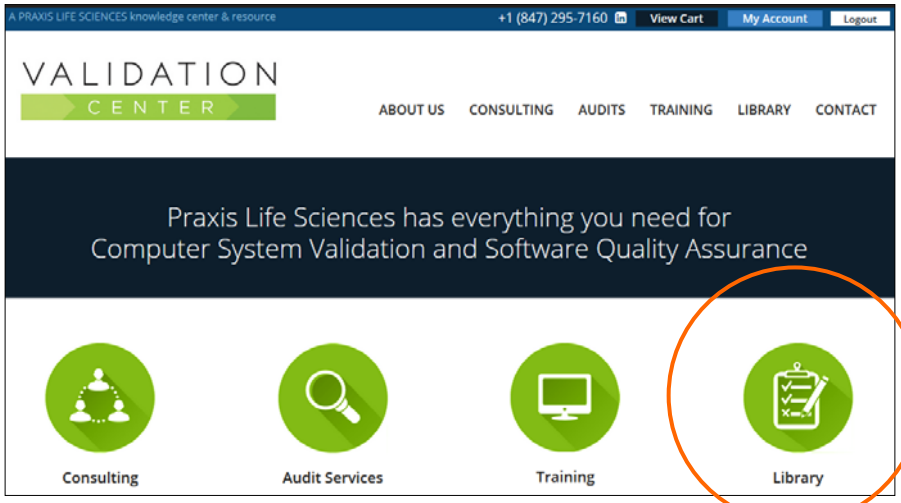
12

Clarity At Last!

Validation Center™ © 2021 Treximo, LLC 13

13

WWW.VALIDATIONCENTER.COM



Validation Center™ © 2021 Treximo, LLC 14

14

Data Integrity Terminology

Part 2

15

Integrity

Integrity (noun) | Dictionary.com
1. Adhering to moral and ethical principles; honesty
2. Whole, entire, undiminished

FDA	MHRA	PIC/S
Complete	Complete	Complete
Consistent	Consistent	Consistent
Accurate	Accurate	Accurate
	Trustworthy	
	Reliable	

16

Data | Metadata

Data **66**

Metadata

Information about the data that makes the data meaningful

- 2017-02-27 15:23:01 GMT — when data generated
- Joe L. Smith — lab analyst who ran test
- GX-0032-A — lab instrument that generated the data
- mg — unit of measure

Audit trail

```
2017-02-27 13:23:01 GMT  66  original test result
2017-02-27 13:32:32 GMT  67  changed by J.Jones
2017-02-28 11:00:06 GMT      deleted by M.Cooper
```


17

Static Data | Dynamic Data

Static Data: Data that is fixed

Dynamic Data: Data that allows user interaction which could alter the result

18

Original Data | True Copy

Original Data: Data in its original format

True Copy: Copy of Original Data that has been

1) Verified
   - Signed, dated by the verifier, *OR*
   - Generated through a validated process
2) Contains the same information as the Original Data – *including the metadata*

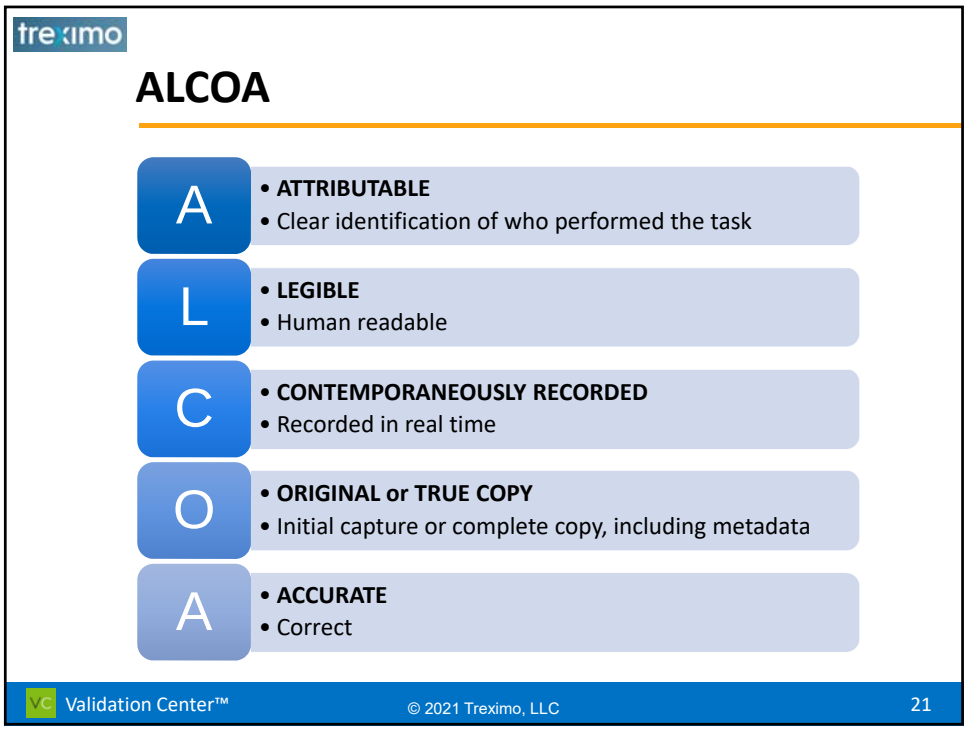
19

Audit Trail

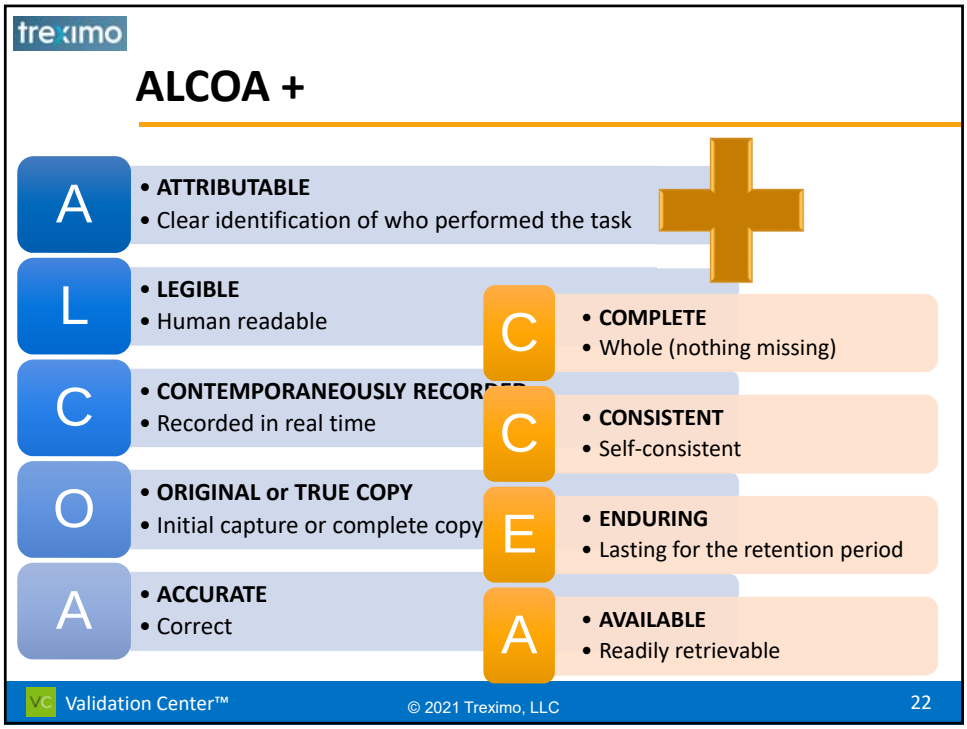
Electronic Record that allows for reconstruction of events related to the creation, modification or deletion of an electronic record

- Computer Generated
- Independently Recorded
- Date and time stamped
- Author identified
- Secure
- Does not obscure previously recorded information
- Retained for as long as the subject record
- Suitable for reviewing and copying

20



21



22

Electronic Data Integrity Principles

Part 3

23

Access Restrictions

Expectation Actions attributable to person who performed the task

- Require User ID + Password for access to add/change/delete
- Prohibit sharing of User IDs
- Prohibit re-use of User IDs
- Prohibit sharing of Passwords… including sharing with IT Support staff
- Eliminate use of Generic accounts, e.g., System Admin, Vendor Maintenance
- Require periodic revision of Passwords
- Log-out or require re-authentication after period of inactivity
- Lock-out after defined number of invalid Password attempts

Validation Center™ © 2021 Treximo, LLC 24

24

Access Restrictions

Expectation Access limited to only features needed to perform job

- Limit access to minimum possible, especially access to:
  - Change, delete, inactivate/void data and records
  - Set up new users and change access levels
  - Change system settings and configuration, e.g., date/time, access levels, product specifications, processing parameters, test methods
  - Change software
- Segregate duties to reduce the likelihood of data integrity issues, for example:
  - Limit access to change critical settings, delete records, etc. to persons outside of the organization responsible for the electronic data and records

25

Access Restrictions

Scenario 1	Scenario 2	Scenario 3
A Doc Center user has access to author, edit and publish SOPs. Should this user have access to the change validated document workflows? Should this user be able to give access to another user?	A Lab user has access to enter product testing results. Should this user have access to change the product specifications? Delete results for failing tests?	IT technical support user has access to apply software patches. Should this user have access to author, edit, and delete production data? Should this user be able to give access to another user?

26

Access Restrictions

Expectation Controls for authorizing and tracking user access

- Implement formal procedure for managing system access… including IT, vendors
  - Define training requirements for each access level
  - Define responsibility for authorizing requests for each access level
  - Document and approve all access requests
  - Retain access authorization records and training records
  - Implement process for temporary access, e.g., for system maintenance
  - Immediately remove access when leaving company, changing positions, or ending temporary access
  - Periodically audit access levels and associated users

27

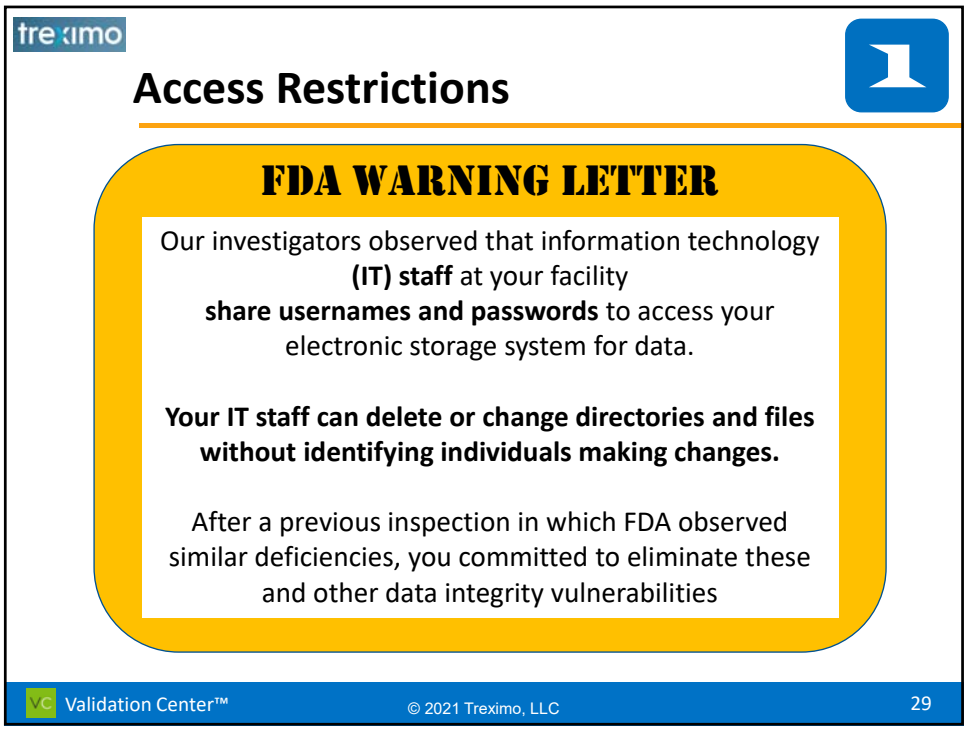
Access Restrictions

FDA WARNING LETTER

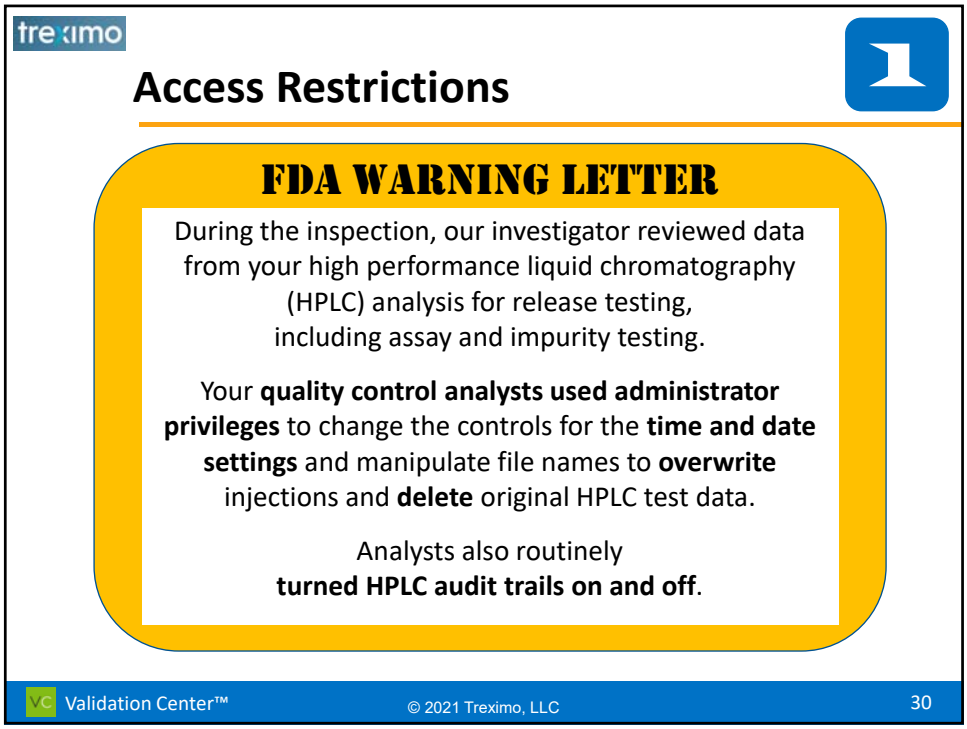
All employees had administrator privileges and shared one user name, so actions **could not be attributed** or traced to specific individuals.
This exposed your electronic data to manipulation and/or deletion without traceability.

Analysts also **shared the username and password for the Windows operating system** for the GC workstations and no computer lock mechanism had been configured to prevent unauthorized access to the operating systems.

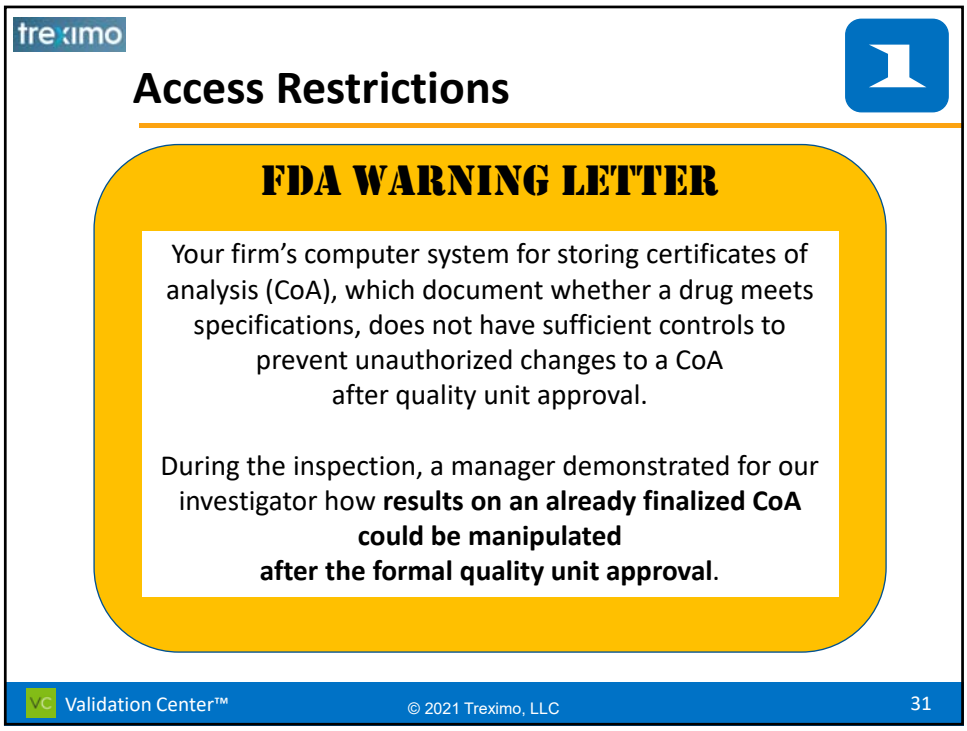
28



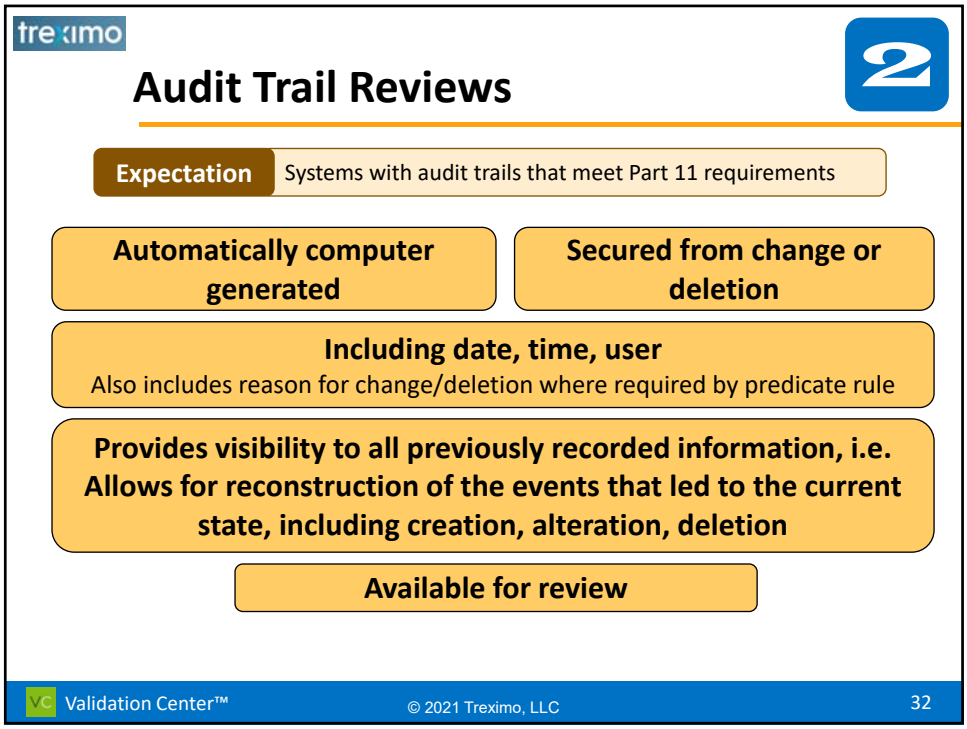
29



30



31



32

Audit Trail Reviews

Expectation Audit trails allow detection of potential data integrity issues

- Verify that situations such as these can be detected by looking at the audit trail:
  - Alteration of data or records – *especially after approval*
  - Data and record deletion
  - Aborted lab testing runs
  - Testing into compliance
  - Changes to critical process parameters
  - Back-dating
- If needed, work with technical expert or software vendor to improve audit trail 'readability', e.g., via new views, reports

33

Audit Trail Reviews

Expectation Review of audit trails during approval of **critical** data

- For **critical data and records,** include an audit trail review in the approval processes (SOPs)

  Examples of critical data and records:
  - Product testing results and sample run sequences
  - Manufacturing process parameters
  - Study conclusions

  - **Responsibility:** Same role that has responsibility for data review, per regulations, e.g., Quality Unit for manufacturing Batch Record Review
  - **Method:** Review audit trail online or via validated report

34

Audit Trail Reviews

Expectation Risk-based review of audit trails for **other GxP data**

- For **non-critical GxP data and records,** implement processes (SOPs) for risk-based review of audit trails
  - **Frequency:** Based on criticality, e.g., to patients, products, study outcomes and likelihood of data integrity issues, e.g., unauthorized deletions or changes
  - **Responsibility:**
    - Organization responsible for record content
    - Checked by QA during internal audits
  - **Method:** Review audit trail online or via validated report
  - **Document** outcome of each review

Validation Center™ © 2021 Treximo, LLC 35

35

Audit Trails

FDA WARNING LETTER

Your firm uses software to document, maintain, and track customer complaints electronically.

However, as stated by your firm's Director of Quality Assurance (QA) & Regulatory Affairs (RA) during the inspection, the **software does not generate time-stamped audit trails** to independently record the date and time of operator entries and actions that create, edit, or modify electronic records.

Validation Center™ © 2021 Treximo, LLC 36

36

Audit Trail Reviews

2

FDA WARNING LETTERS

A file containing the moisture content results for an API batch had been deleted.

This **deletion was not identified and reviewed as part of your batch release decision**.

Your firm lacks systems to ensure that all electronic data generated in your Quality Control laboratory is secure and remains unaltered.

Your firm's **review of laboratory data does not include a review of an audit trail** or revision history to determine if unapproved changes have been made.

37

Electronic Copies

3

Expectation "True Copy" principles applied for all GxP copies

- Implement policies that must be applied whenever electronic records are copied or migrated for GxP purposes
  - All content and meaning from the original must be preserved
  - All of the information must be accurate and complete
  - All of the metadata (e.g., the audit trail) must be retained
  - The record must remain readily available
- Implement procedures (SOPs) for creating and verifying "True Copies"
- Validate programs used to create "True Copies"

38

Electronic Copies

3

FDA WARNING LETTERS

Due to a transition to a new complaint handling computer system, the following **complaints were missing a code and were not included in trending**:

a) 99 complaints for inflammatory mass
b) 88 complaints for Dysarthria. When this data was added to the system, three separate signals exceeded threshold
c) 11 complaints for Loculation
d) 104 complaints for Incision Pain

39

Back Up, Protection & Retention

4

Expectation Records protected from loss

- Implement back-up and disaster recovery processes for
  - Records, data, metadata
  - Software, system settings, configurations, and run-time parameters
- Establish risk-based frequency for
  - Performing back ups
  - Auditing back up media
  - Executing disaster recovery tests

- Establish risk-based standards for location of back up media
- Validate back up and recovery processes.

40

Back Up, Protection & Retention

Expectation Records protected from loss

- Retain electronic records in a location with physical security:
  - Secured room with minimal number of persons able to access
  - Appropriate temperature and humidity controls
  - Protection from fire and water damage
- Implement controls to secure from external (cyber) hazards, such as:
  - Record corruption or damage
  - Record theft

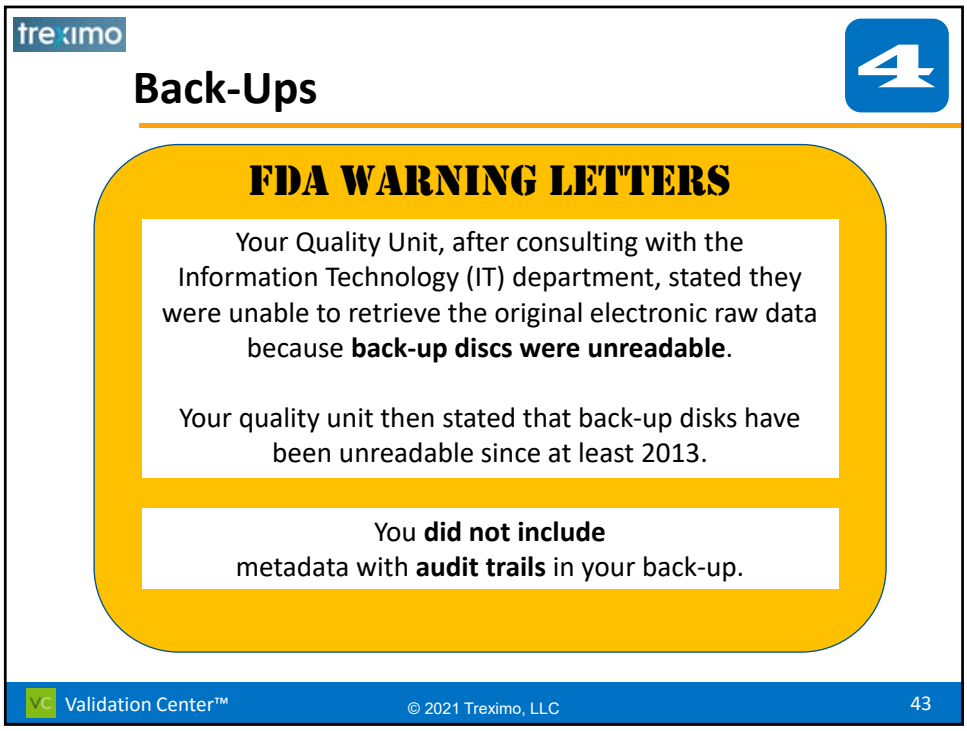
41

Back Up, Protection & Retention

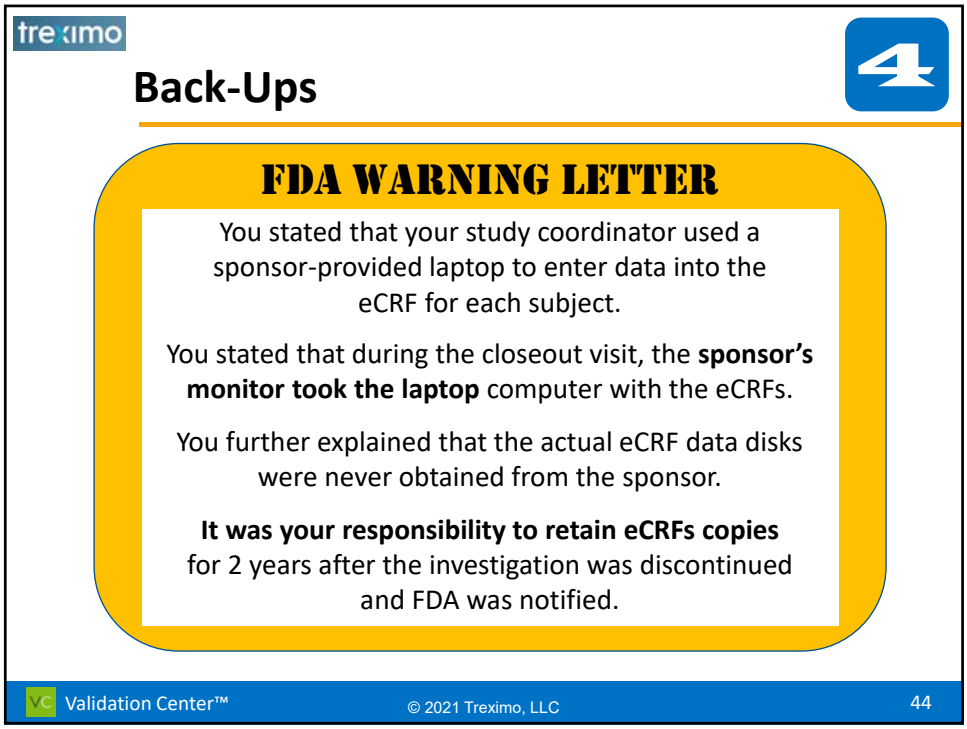
Expectation Records readily available for the entire retention period

- Document the retention period for all GxP records generated and/or retained electronically
  - Include metadata (e.g., audit trail) in the scope for retention
- If records are archived outside the system:
  - Validate the archival process
    - Retest when technology is changed
  - Document the procedure for accessing or restoring the records and metadata
  - Periodically test the access or restore process

42



43



44

Back-Ups

4

FDA WARNING LETTER

You confirmed that there are no meeting minutes for the year during which two meetings were held.

You explain that due to a computer crash **all minutes and data for that time frame were lost**. You stated that you would "re-create" the meeting minutes and provide them at a later date.

It is inappropriate and an unacceptable record keeping practice for the IRB to re-create minutes.

45

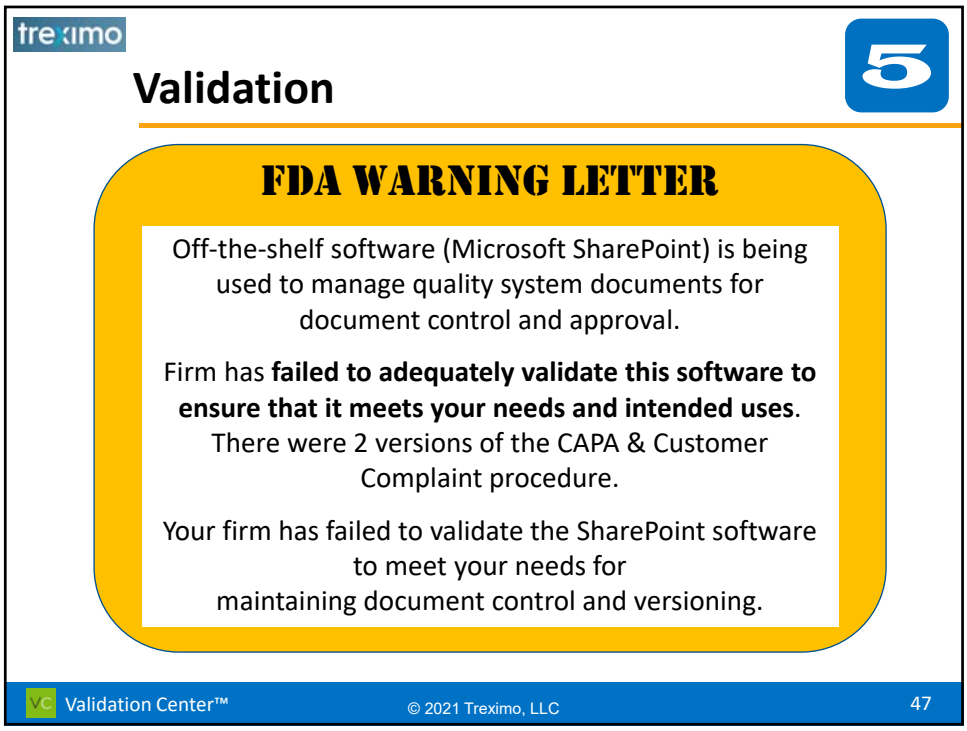
Validation

5

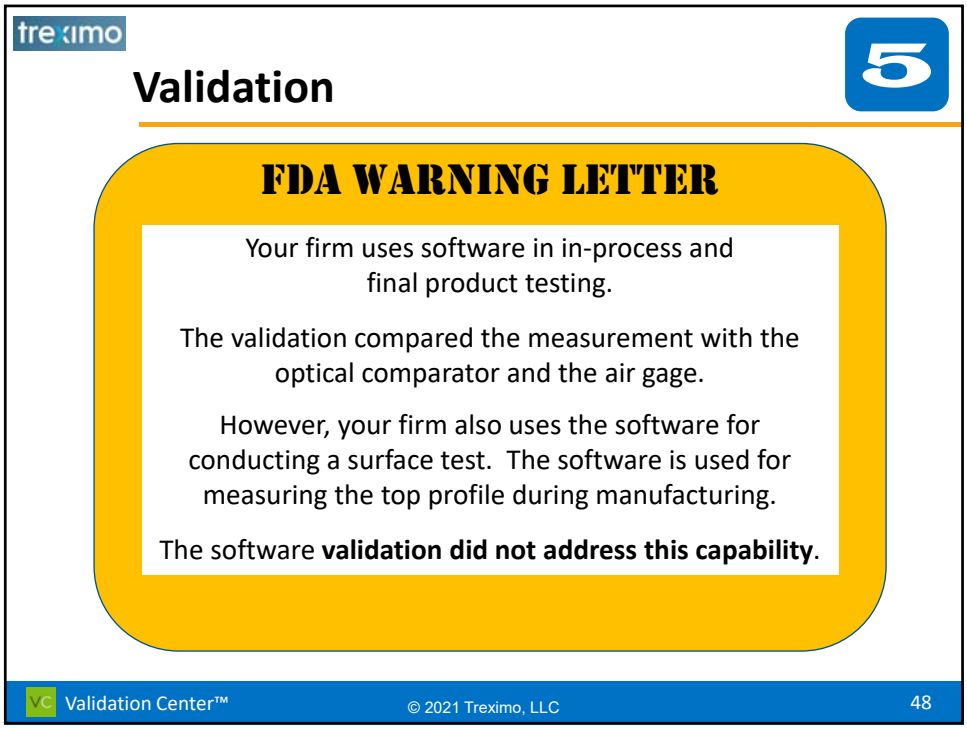
Expectation Electronic systems validated for company-specific uses

- Confirm that purchased (COTS) and cloud (SaaS) systems have been validated for company-specific uses, e.g.:
  - Workflows
  - Settings / Configurations, e.g., drop down lists of critical values, security groups, audit trail settings, password expiration
  - Calculations and formulas
  - User-created reports
  - Connections to company equipment
- Perform validation for any gaps found in vendor's generic "validation"

46



47



48

Unacceptable Practices

Expectation Practices where data can 'disappear without a trace' eliminated

Eliminate practices such as:

EXAMPLES

- Recording data on a piece of paper, and then **discarding the paper** after the data is transcribed into the system
- Storing electronic data in **temporary memory**, in a manner that allows for manipulation, before creating a permanent record
- Placing records (e.g., chromatograms) in long-term storage at the **end of the day** rather than upon completion of the run.

49

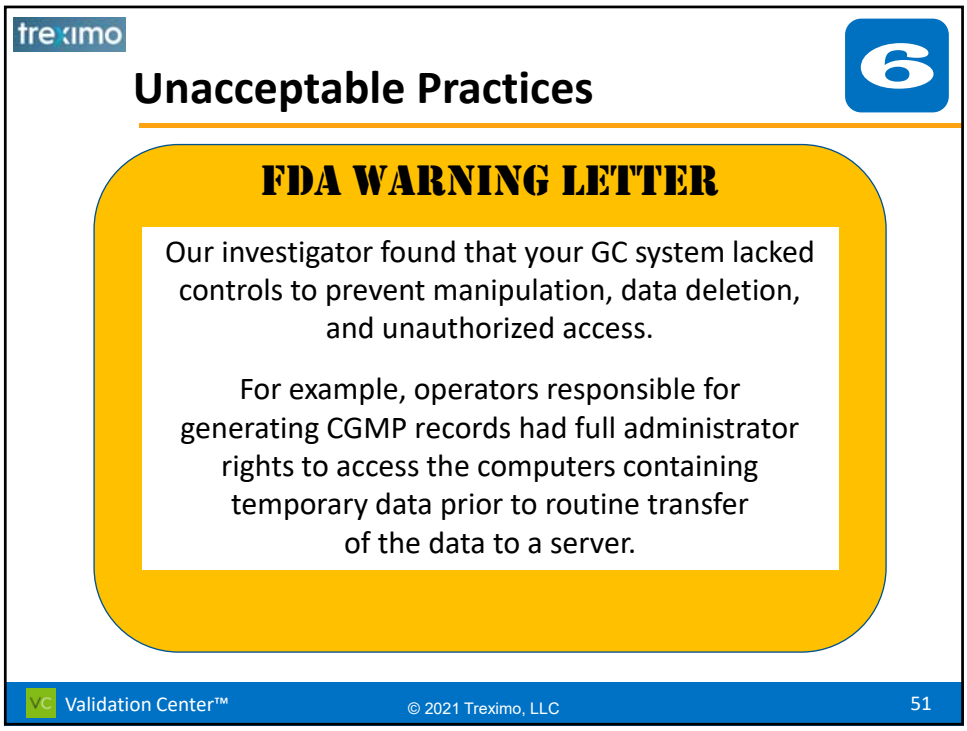
Unacceptable Practices

Expectation Practices that enable "testing into compliance" eliminated

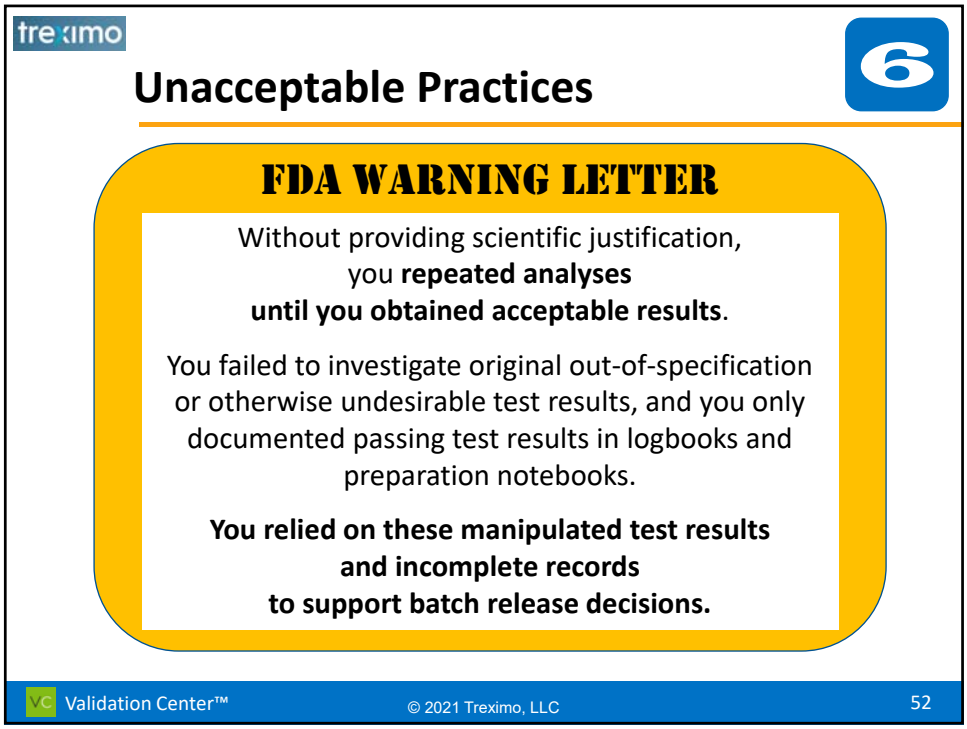
"Testing into Compliance"
Re-sampling, re-testing, or re-processing with the goal of achieving a specific result or overcoming an unacceptable result

- Update laboratory procedures (SOPs):
  - Define acceptable reasons (if any) for re-sampling, re-testing, and reprocessing
  - Define how to document and authorize use of the acceptable reasons for re-sampling, re-testing, and re-processing, e.g., *brief explanation in audit trail, full explanation and supervisor approval in lab notebook*
  - Require retention of **ALL** test results

50



51



52

Reports of Data Integrity Issues

Expectation Potential data integrity issues investigated & corrected

- Implement formal procedures (SOPs) to manage reported and suspected data integrity lapses through the quality systems, e.g., within the CAPA program.
  - Determine of the extent of the issue, e.g. limited to one area
    or product vs. systemic
  - Determine the effect of the issue on patient safety, product quality, or data reliability
  - Determine the root cause
  - Ensure that corrective action is taken
  - Monitor effectivity and new instances is same issue

53

Reports of Data Integrity Issues

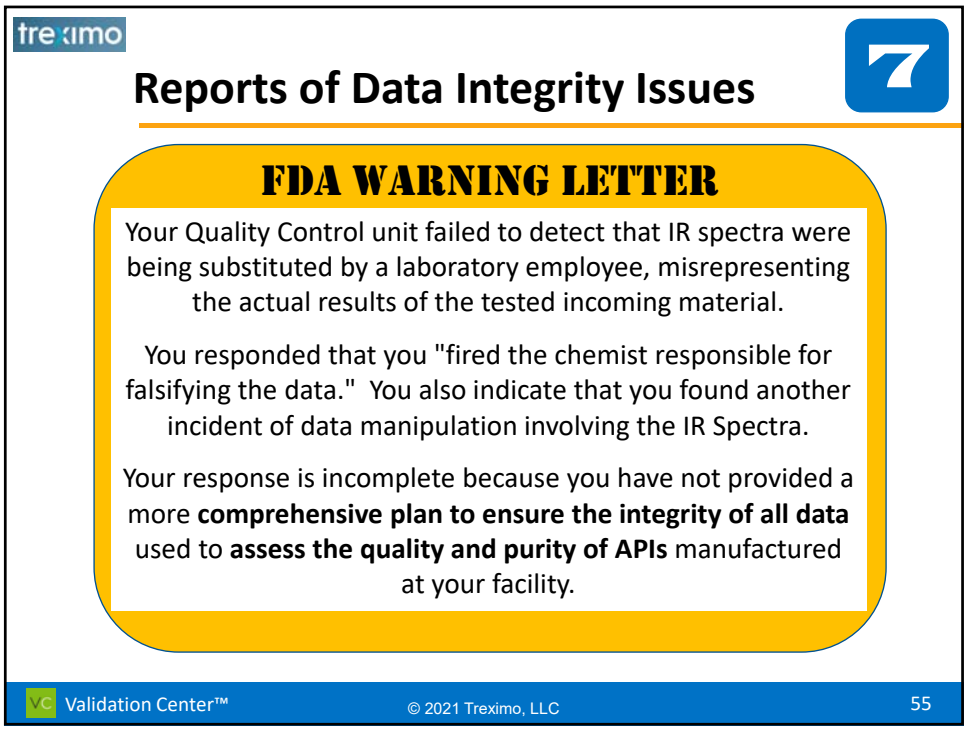
FDA WARNING LETTER

A “File Note” signed by the QC Head established that the printed **data** used for batch disposition decisions from the hard drive was **not necessarily** the **complete** data for a batch.

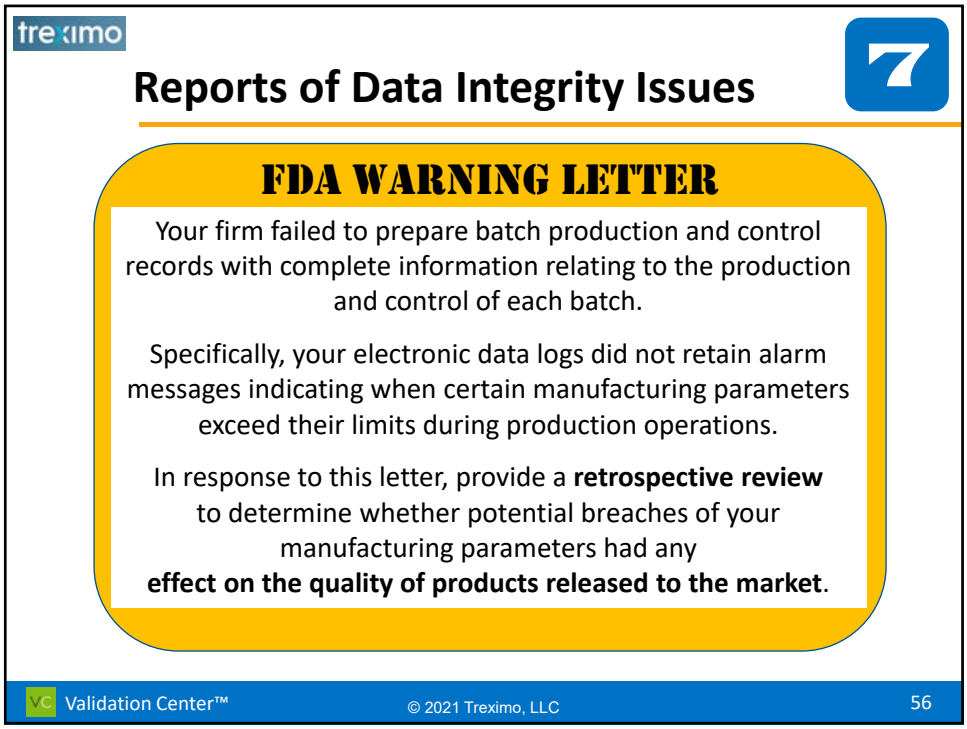
Our inspection found that this data was selected for use.

The audit trail capability of this QC “commercial” laboratory instrument was not enabled, even after creation of the “File Note.”

54



55



56

Outsourced Activities

Expectation Data Integrity practices for GxP service & material providers

Examples of GxP providers:
Third Party manufacturing, testing, warehousing, distribution, clinical trial execution

- Supplier Qualification
  - Verify providers' data integrity practices during initial qualification
  - Periodically check providers' data integrity practices during re-qualification
- Quality Agreements
  - Include responsibilities and expectations regarding data integrity

57

Outsourced Systems

Expectation Data Integrity practices for cloud (SaaS, PaaS, IaaS) systems

- Supplier Qualification
  - Verify providers' data integrity features and practices during initial qualification
  - Periodically check providers' data integrity practices during re-qualification
- Contracts, Quality Agreements and/or Services Level Agreements (SLAs)
  - Include responsibilities and expectations to ensure data integrity

58

Training

10

Expectation All personnel trained in detecting data integrity issues

- Periodical training in
  - Responsibilities for data integrity
  - Detection of potential data integrity issues
  - Reporting of potential data integrity issues

- Include all employees and temporary staff with responsibilities for:
  - Creation and modification of GxP data and records
  - Retention and protection of GxP data and records
  - Development and maintenance of the electronic systems used to generate, retain, and store GxP data and records

Validation Center™ © 2021 Treximo, LLC 59

59

Examples of Data Integrity Risks

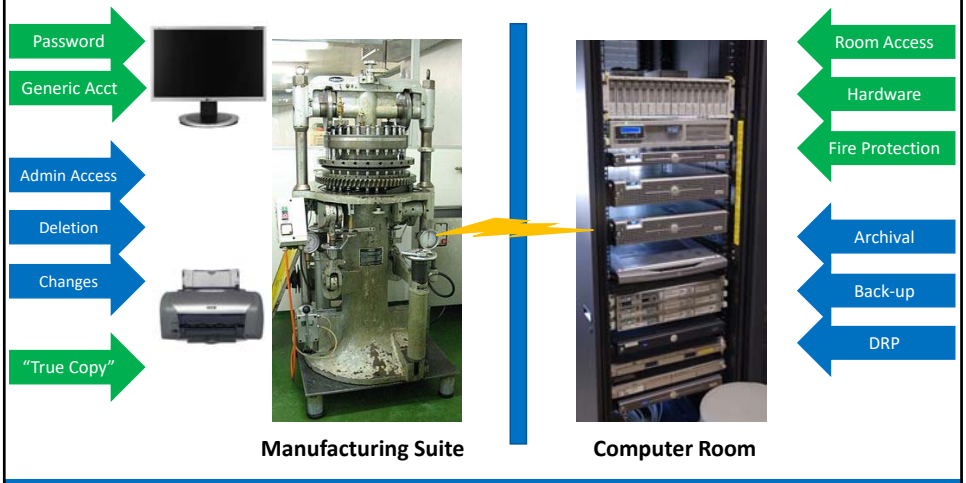
Part 4

60

60

Scenario 1

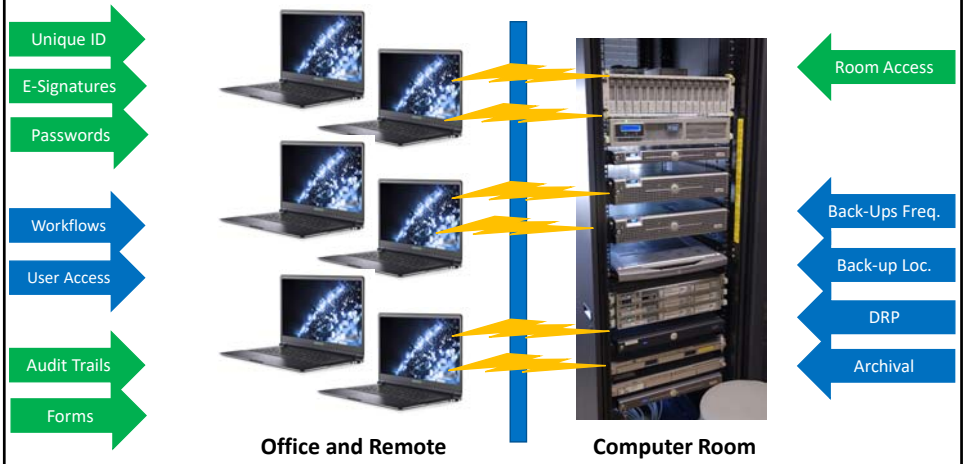
Scenario: Software Controlled Manufacturing Equipment



61

Scenario 2

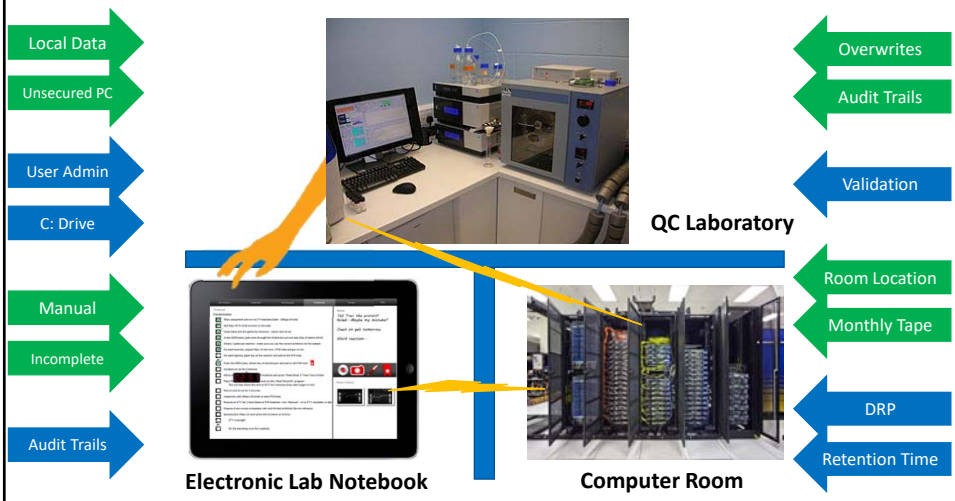
Scenario: Document Management System



62

Scenario 3

Scenario: Lab Instrument Software and Electronic Lab Notebook (ELN)

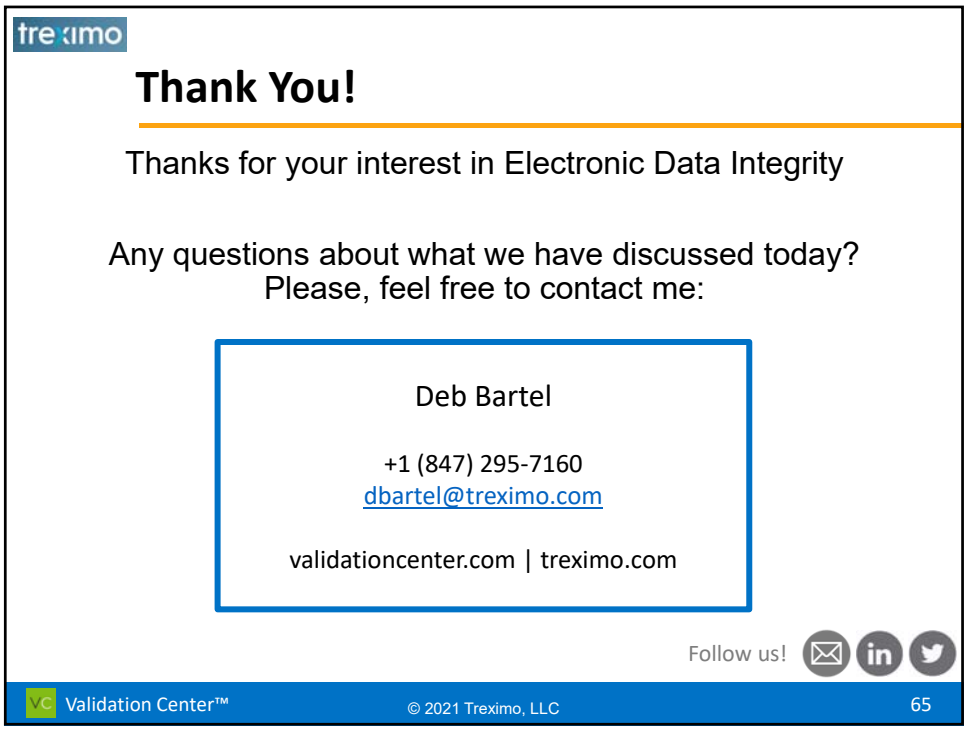


63

How Can Treximo Help?

- **Data Integrity Audits & Compliance Plans**
- **Computer System Validation Services**
- **Online and Classroom CSV Training**
- **ValidationCenter.com Library of Template and SOPs**

64



65