Managing Data Integrity and Compliance Confidence

Arjan Timmerman
Gathering & Sharing Regulatory Information

Regulatory Bodies
FDA/MHRA etc

Industry Groups
ISPE/GAMP

Customer QA

Sales and Specialists

Professional Services

Product Functionality and Design

Within
Disclaimer

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

1. facts and statistics collected together for reference or analysis.

   synonyms: facts, figures, statistics, details, particulars, specifics, features

   - the quantities, characters, or symbols on which operations are performed by a computer, which may be stored and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media.
   - things known or assumed as facts, making the basis of reasoning or calculation.
   - data is not information. Data requires interpretation to become information. To translate data to information, there must be several known factors considered. The factors involved are determined by the creator of the data and the desired information.
What is Data Integrity?

integrity
/ɪnˈteɡrɪti/

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

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

   antonyms: dishonesty

2. the state of being whole and undivided.

   synonyms: unity, unification, wholeness, coherence, cohesion, undividedness, togetherness, solidarity, coalition
What is Data Integrity?
Fat Finger, Falsification or Fraud?

- Peer Review
- Disciplinary Action
- Regulatory Action

Bob McDowall, Spectroscopy Dec 2010
http://www.spectroscopyonline.com/fat-finger-falsification-or-fraud-0
Company Culture is Important

- It is important to find a balance between compliance and business goals because both are important
  - Don’t inadvertently tempt individuals to try and avoid compliance because the compliant path is hard and complex
Where to start?

- Consistent review and oversight is key
  - Notice areas of concern and evaluate system and procedural controls
- Educate and empower employees
  - Company culture is very important
- Evaluate what is feasible for your company
  - What are your highest RISKS?
  - What are your constraints with personnel time and company funds?
  - What can you implement at your company now? and in the future?

- Do not implement procedures and policies that cannot be reasonably performed
  - Be compliant with your own SOPs
Why the new focus on Data Integrity?

Electronic Systems Improve Traceability

Provide the **controls to prevent** and **capability to detect** undesirable users actions

- Tools for QA and Regulators
  - Access Levels
  - System Policies
  - Audit Trails

Agencies have lost the trust that analysts behave with honesty and integrity
Benefits of Computerized Systems for Data Integrity

Data Integrity is NOT a new problem, more control / documentation can be implemented with computerized systems.
Why the new focus on Data Integrity?

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

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

<table>
<thead>
<tr>
<th>Product/Batch Number</th>
<th>Lack of Complete Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Products and batches listed in FDA-483, point #2</td>
<td>OOS results not documented in laboratory records. Unreported OOS results found in electronic data files.</td>
</tr>
<tr>
<td>Propoxyphene Napsylate and APAP Tablets, 100/650mg, Batch 303110A</td>
<td>Changed chromatogram headers by cutting and pasting, so during review all sample injections would appear to be in sequence, for Dissolution Testing of Tablets D1 and D5</td>
</tr>
<tr>
<td>Propoxyphene Napsylate and APAP Tablets, 100/650mg, Batch 104026B, Validation Batch</td>
<td>Original Sample Weights not recorded in notebook. Sample weights were changed by the analyst until a passing result was obtained for Assay (A2)</td>
</tr>
<tr>
<td>Acetaminophen &amp; Codeine Phosphate Tablets, 300/30mg, Batch 407148</td>
<td>Processing methods changed by analyst until the processing method resulted in a passing result. Original processing method not recorded in laboratory notebook.</td>
</tr>
</tbody>
</table>

http://www.fda.gov/aboutfda/centersoffices/officeofglobalregulatoryoperationsandpolicy/ora/oraelectronicreadingroom/ucm061813.htm
Data Integrity: Key for Quality Assurance

Underlying Everything: Regulatory bodies need to trust the data they are seeing

- **Data Integrity Guidances**: focused on chromatography
- **Review of audit trails** as in Annex 11
- **Focused Inspections**: All are focusing on Data Integrity
  - Several new guidances (at least five)
  - Static and Dynamic Data (static printed chromatograms)
    - Expect to look at the electronic data, not just printouts
  - Continual training of regulators in electronic laboratory applications
- **Ensuring the bad as well as the good data is available**
  - Specifically for reanalysis and reprocessing
- **Find the root cause of issues and OOS**
  - Right scaled Lab error and Full OOS investigations
Definition of Data Integrity

Data Integrity is the extent to which all the data are complete, consistent and accurate throughout the data lifecycle.

Data Integrity refers to completeness, consistency and accuracy of data. That data should be ALCOA.

The collected data should be Attributable, Legible, Contemporaneously recorded, Original or a true copy, and Accurate (ALCOA).

Data Integrity is defined as the extent to which all data are complete, consistent and accurate, throughout the data lifecycle.
### Key Factor in Data Integrity

<table>
<thead>
<tr>
<th>ALCOA+</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Attributable</strong></td>
<td>Who acquired the data or performed an action</td>
</tr>
<tr>
<td><strong>Legible</strong></td>
<td>Can you read and understand the data entries?</td>
</tr>
<tr>
<td><strong>Contemporaneous</strong></td>
<td>Documented at the time of the activity</td>
</tr>
<tr>
<td><strong>Original</strong></td>
<td>First recorded observation</td>
</tr>
<tr>
<td><strong>Accurate</strong></td>
<td>No errors or editing?</td>
</tr>
<tr>
<td><strong>Complete</strong></td>
<td>All data including any repeat or reanalysis performed</td>
</tr>
<tr>
<td><strong>Consistent</strong></td>
<td>All elements of the analysis, such as the sequence of events, follow on and are dated/time stamped in expected sequence</td>
</tr>
<tr>
<td><strong>Enduring</strong></td>
<td>Recorded in a permanent, maintainable form for the useful life</td>
</tr>
<tr>
<td><strong>Available</strong></td>
<td>For review, audit or inspection over the lifetime of the record</td>
</tr>
</tbody>
</table>
# ALCOA+ Table

<table>
<thead>
<tr>
<th>ALCOA + abbreviation</th>
<th>Description / Explanation</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Attributable: Who performed an action and when? If a record is changed, who did it and why? Link to the source data.</td>
<td>Who did it? Source data</td>
</tr>
<tr>
<td>L</td>
<td>Legible: Data must be recorded permanently in a durable medium and be readable.</td>
<td>Can you read it? Permanently Recorded</td>
</tr>
<tr>
<td>C</td>
<td>Contemporaneous: The data should be recorded at the time the work is performed and date / time stamps should follow in order.</td>
<td>Was it done in “real time”?</td>
</tr>
<tr>
<td>O</td>
<td>Original: Is the information the original record or a certified true copy?</td>
<td>Is it original or true copy?</td>
</tr>
<tr>
<td>A</td>
<td>Accurate: No errors or editing performed without documented amendments.</td>
<td>Is it Accurate?</td>
</tr>
<tr>
<td></td>
<td><strong>Complete</strong>: All data including repeat or reanalysis performed on the sample.</td>
<td>21 CFR 211.194</td>
</tr>
<tr>
<td></td>
<td><strong>Consistent</strong>: Consistent application of data time stamps in the expected sequence.</td>
<td>Date time stamps</td>
</tr>
<tr>
<td></td>
<td><strong>Enduring</strong>: Recorded on controlled worksheets, laboratory notebooks or electronic media.</td>
<td>Medium used to record</td>
</tr>
<tr>
<td></td>
<td><strong>Available</strong>: Available / accessible for review / audit for the life time of the record.</td>
<td>For the life time of the record</td>
</tr>
</tbody>
</table>
Attributable

- All data generated or collected must be attributable to the person generating the data. This should include who performed an action and when. This can be recorded manually by initialing and dating a paper record or by audit trail in an electronic system.

- For example:
  - During a validation exercise, test results should be initialed and dated by the person executing the test.
  - Adjustment of a set point on a process or monitoring system should be made by an authorized user and the details of the change logged in an audit trail.
  - A correction on a lab record should be initialed and dated to show when and who made the adjustment.

- Note: It is important to ensure a signature log is maintained to identify the signatures, initials and/or aliases of people completing paper records.

https://www.pharmout.net/data-integrity-alcoa/
Legible

- All data recorded must be legible (readable) and permanent. Ensuring records are readable and permanent assists with its accessibility throughout the data lifecycle. This includes the storage of human-readable metadata that may be recorded to support an electronic record.

- For example:
  - GDP will always promote the use of indelible ink when completing records.
  - When making corrections to a record, ensure a single line is used to strike out the old record. This ensures the record is still legible.
  - Controlling your paper records/forms and formatting them such that there is ample room for the information to be recorded.

https://www.pharmout.net/data-integrity-alcoa/
Contemporaneous

Contemporaneous means to record the result, measurement or data at the time the work is performed. Date and time stamps should flow in order of execution for the data to be credible. Data should never be back dated.

For example:

- If executing a validation protocol, tests should be performed and their results recorded as they happen on the approved protocol.
- Data that is logged, or testing that is performed electronically, should have a date/time stamp attached to the record.
- Ensure electronic systems that log data have their system clocks synchronized.
- Consider the use of a master clock system that synchronizes to the IT network so wall clocks within labs and processing areas are synchronized.
Original data, sometimes referred to as source data or primary data, is the medium in which the data point is recorded for the first time. This could be a database, an approved protocol or form, or a dedicated notebook. It is important to understand where your original data will be generated so that its content and meaning are preserved.

For example:

- Ensure validation test results are recorded on the approved protocol. Recording results in a notebook for transcription later can introduce errors.
- If your original data is hand written and needs to be stored electronically, ensure a “true copy” is generated, the copy is verified for completeness and then migrated into the electronic system.
Accurate

- For data and records to be accurate, they should be free from errors, complete, truthful and reflective of the observation. Editing should not be performed without documenting and annotating the amendments.

- For example:
  - Use a witness check for critical record collection to confirm accuracy of data.
  - Consider how to capture data electronically and verify its accuracy. Build accuracy checks into the design of the electronic system.
  - Place controls / verification on manual data entry, for example, temperature results can only be entered within a predefined range of 0-100°C.

https://www.pharmout.net/data-integrity-alcoa/
Common issues

Finally, here are a couple of common examples where ALCOA is not used resulting in poor documentation and data integrity issues:

- It is very common to see data being quickly jotted down on a sticky note or on a note pad during testing. This data is then transferred onto the approved protocol or form. Doing this, whether it be for lab results or a validation exercise, means the data is no longer original, contemporaneous and potentially inaccurate.

- When making a correction to information it is common to see the old data scribbled out, overwritten or removed using correction fluid and sometimes without an initial and date of who made the correction. This means the data is no longer legible, original and the correction is not attributable.

https://www.pharmout.net/data-integrity-alcoa/
What is Data Life Cycle?

- …from initial generation and recording through processing (including analysis, transformation or migration), use, data retention, archive / retrieval and destruction.

- …assessing risk and developing quality risk mitigation strategies for the data life cycle,

- including controls to prevent and detect risks throughout the steps of:
  - data generation and capture;
  - data transmission;
  - data processing;
  - data review;
  - data reporting, including handling of invalid and atypical data;
  - data retention and retrieval;
  - data disposal.
Securing and reviewing complete data: The regulator view of static and dynamic data
Questions and Answers on Current Good Manufacturing Practices, Good Guidance Practices, Level 2 Guidance - Records and Reports

1. Some products, such as transdermal patches, are made using manufacturing processes with higher in-process material reject rates than for other products and processes. Is this okay?

2. Do the CGMP regulations permit the destruction of an internal quality assurance audit report once the corrective action has been completed?

3. 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?

4. How does the FDA interpret the regulations (21 CFR Part 211) regarding the establishment of expiry dating for chemicals, reagents, solutions, and solvents?
www.FDA.Gov Questions and Answers
Level 2 Guidance - Records and Reports

3. 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?

... Therefore, the printed chromatograms do not satisfy the predicate rule requirements in 21 CFR Part 211. The electronic records created by the computerized laboratory systems must be maintained under these requirements...

... However, the electronic record must be maintained and readily available for review by, for example, QC/QA personnel or the FDA investigator.
Paper Does Not Always Provide the Complete Story

Printouts COULD represent original data

 SIMPLE
 pH Meter

 UV Spec
 FTIR

 HPLC
 GC

 LIMS
 ERP

 COMPLEX
 Printouts are NOT Representative

 Picture is a rendition of the image found in the MHRA GMP Data Integrity Definitions and Guidance for Industry (March 2015)
Data may be…

- **static** (e.g. a ‘fixed’ record such as paper or PDF)
- **dynamic** (e.g. an electronic record which the user / reviewer can interact with).

**Data must be retained in a dynamic form** where this is critical to its integrity or later verification, and (once printed) **chromatography records** lose the capability of being reprocessed and do not enable more **detailed viewing of baselines or any hidden fields.**

Some data generated by electronic means to be retained in an acceptable paper or PDF format

1. Where it can be justified that a static record maintains the integrity of the original data.
2. However the process must be shown to include verified copies of all raw data, **meta data, audit trail**, result files, software/system configuration settings for each record, all data processing runs (including methods and audit trails) for a reconstruction … and verification

**This approach is likely to be onerous to enable a GxP compliant record**
FDA Guidance: Reviewing Electronic Records Summary

- **Static** is used to indicate a fixed-data document (such as a paper record or an electronic image), and

- **Dynamic** means that the record format allows interaction between the user and the record content.
  - But defines as allowing the reviewer to change/edit things…???

- (Printouts allowed if) **includes associated metadata** and the **static or dynamic nature of the original records**

- Electronic records from certain types of laboratory instruments are **dynamic records**, and a **printout or a static record does not preserve the dynamic format**
WHO Guidance: Reviewing Electronic Records Summary

- A PDF or printout is fixed or static and the ability to expand baselines, view the full spectrum, reprocess and interact dynamically with the data set would be lost in the PDF or printout.

- Data integrity risks may occur when persons choose to rely solely upon paper printouts or PDF reports:
  - If the reviewer only reviews the subset of data provided as a printout or PDF, these risks may go undetected.

- Paper printouts of original electronic records from computerized systems may be useful as summary reports... verify that the printed summary is representative of all (electronic)results.

- A risk-based approach to reviewing data requires process understanding and knowledge of the key quality risks... requires understanding of the computerized system, the data and metadata and data flows.

Guidance on Good Data and Record Management Practices
Released June 2016 As WHO_TRS_996 Annex 5
Do you archive your Empower Data?
Do you Archive your Empower data?

- There is a difference between **Backup and Archive**!
  - And you need to have both

- Backup might be arranged by IT department
  - Do you regularly check your backups for recovery?
  - Do you have a disaster recovery plan?
  - Is this process validated?
  - Is your backup taking a long time?

- Guidance on **Backup**
  - EU and PIC/S Annex 11 describe in: Section 7 Data Storage
  - MHRA guidance describes: in Data Retention section, Backup
  - FDA guidance describes: in Question 1 (a)
  - WHO guidance describes: in Annex 5 Retention of Original Records
Do you Archive your Empower data?

- What about Archive?
  - Do you Archive the Empower Data? And System Audit Trail?
  - Is this process audit trailed?
  - Do you keep indexes?
  - If so, do you check when you upgrade the software?
  - Do you delete your data when needed (data retention)?
  - Is all described in your SOP’s?

- Guidance on Archive
  - EU and PIC/S Annex 11 describe in: Section 17 Archiving
  - MHRA guidance describes: in Data Retention section, Archive
  - FDA guidance describes: in Question 1 (a), a bit cryptic
  - WHO guidance describes: in Annex 5 Retention of Original Records
Data Integrity Regulatory Findings
Why is Data Integrity Important?

- We rely on accurate information to ensure drug quality
- Data integrity problems erode confidence
- We rely largely on confidence that the firm will do the right thing when we are not there

FDA presentation in June 2015

2nd Most Common Citation

- Your firm failed to exercise appropriate controls over computer or related systems to assure that only authorized personnel institute changes in the master production and control records, or other records (21 CFR 211.68(b)).
  – Cited in 15 warning letters
FD

FDA presentation in June 2015

2nd Most Common Citation

- Cited in numerous warning letters:
  - Audit trails were disabled
  - A shared username and password was used by many analysts
  - Users were able to manipulate, delete, or overwrite electronic raw data
- Firm’s laboratory practice is to print chromatograms and delete electronic raw data files
FDA presentation in June 2015

Most Common Citation

- Your firm failed to ensure that laboratory records included **complete data** derived from all tests necessary to assure compliance with established specifications and standards (21 CFR 211.194(a)).
  - Cited in 21 warning letters
FDA presentation in June 2015

Most Common Citation

• Cited in numerous warning letters as failure to retain complete data:
  – “trial” sample injection data was not kept as part of the data for a batch
  – Sample weights, sample preparation and sample dilutions were not retained
  – Deleted data detected in audit trails
  – Overwriting data
  – Ripped up data found in the garbage
Most Common Citation

- Firm deleted all electronic raw data supporting HPLC release testing
- Standards were injected and used as sample results
- Duplicate logbooks were kept
- Complete raw data to support test method validation was not retained
- Integration parameters for HPLC analysis were not retained
Failure to prevent unauthorized access or changes to data, and to provide adequate controls to prevent manipulation and omission of data.

During the inspection, an FDA investigator discovered a lack of basic laboratory controls to prevent changes to your firm’s electronically stored data and paper records.

Your firm relied on incomplete records to evaluate the quality of your drugs...

Our investigator found that your firm routinely re-tested samples without justification, and deleted analytical data. We observed systemic data manipulation across your facility, including actions taken by multiple analysts and on multiple pieces of testing equipment.

Specifically, your Quality Control (QC) analysts used administrator privileges and passwords to manipulate your high performance liquid chromatography (HPLC) computer clock to alter the recorded chronology of laboratory testing events.
Statements of EU Non GMP Compliance

- EU GMP Certificates have been publicized for some time
  - Recently opened a database of **Non Compliance Reports**
    (or statements of non compliance)

- **SUMMARY**
  - Deliberate falsification of results / hiding non conformities
  - Failed injections deleted
  - Discrepancies in raw data / lack of raw data
  - Inadequate review and control of computerized laboratory results and systems
  - Insufficient Qualification of Equipment
  - Quality Control deficiencies including; inadequate records, lack of specificity in analytical methods, failure to investigate unknown peaks
Summary of EU Non Conformances

Data Manipulation
- Falsification of documents
- Discrepancies between electronic data and data reported on paper
- Re written training records
- Falsified entries
- Unreported / unauthorized trial injections of samples
- Raw data chromatogram files deleted
- Retesting samples until passing results obtained

Poor Laboratory Controls
- Failure of Lab controls
- Insufficient management of data, change control and laboratory controls
- No user requirements
- Shared password
- Failure in integrity and security of data
- Analysts routinely perform “trial” injections of sample aliquots prior to performing the official/reported analysis
- PC admin account used to change time back and overwrite failing results
- No system validation of electronic record generating systems

Incomplete Data Review
- OOS results marked as Passed
- Weakness of QA department around Data integrity
- No procedure for audit trail
- Hide non conformities from QA
Regulators are Focused on Data Integrity

- Observe ALL data both reported and non-reported (orphan data)
  - Are the analysts **cherry picking** only the good results?
  - Are failing results being **deleted, hidden or ignored**?
    - Invalidated without justification or approval
  - Are samples being ‘tested into compliance’
    - samples re-analysed /repeated until they pass or
    - manipulated by processing to ensure they pass.

- Is data secure?
  - Proper access and privileges
  - Archive, business continuity, disaster recovery
  - Is there hidden or deleted data?

- Can the story of the data be recreated?
  - Audit trails, metadata, versions
Inspection Themes

No Validation or Change Control

CSV

Technical Controls

Delete Privileges

Unsecured Data

Sharing Accounts

DATA MANIPULATION

Procedural Controls

Poor Review of Electronic Data including audit trails

Poor OOS or Lab Error Investigations

All Data: Good and Bad

No Audit Trail

©2017 Waters Corporation  COMPANY CONFIDENTIAL
What YOU can do?
To balance the focus on electronic data, a useful approach is to map the workflow within the laboratory. Identify and list all of the steps performed for each analytical technique (from sample receipt to approval of results) and each laboratory operation.

The mapping should identify:
- What actions are performed
- How those actions are performed
- How they are recorded
- Any decisions made
- The extent to which the process is manual or automated
- The possible risks associated with the step (e.g., how could fraud be prevented or detected)

One of the purposes of data-integrity auditing is to actively look for evidence of fraud.
Role of your Vendor
Compliance for System Components

**People**
- Culture for data integrity
- Governance and data review
- Unique user accounts
- Scientific skill
- Training
- Safeguards against fraud

**Quality Separations**
- Quality standards & reagents
- Instrument calibration & maintenance
- Qualification
- Method validation
- System suitability
- Quality Columns

**Laboratory Computerized Systems**
- Built-in data integrity controls
- Computerized system validation
- Traceability
- Periodic review

**IT Components**
- Secure centralized storage
- Network qualification
- Disaster recovery plan
- Backup and restore process
Compliance for System Components

Quality Separations
- Quality standards & reagents
- Instrument calibration & maintenance
- Qualification
- Method validation
- System suitability
- Quality Columns

Vendor Assessment

Laboratory Computerized Systems
- Built-in data integrity controls
- Computerized system validation
- Traceability
- Periodic review
Customer Responsibilities

- The customer is ultimately responsible for their compliance
- Validation and compliance cannot be “outsourced” but assistance can provided by your vendor
- Customer must be able to defend how things are configured validated and used if audited
Help me Deal with Regulators

- Why you should not invite / demand your vendor takes part in your inspection?

- Vendors do not know **your product, procedures or SOPs**
- Vendors have **not been trained** in how to participate in audits at your company
- Customers use the same software in different ways,
  - may connect to LIMS or ELNs in unknown ways.
- Calling the vendor strongly **suggests you do not know** your equipment / instruments / tools

- It could be very easy for your **vendor to say something contrary** to your procedures
Summary

**DO**
- review data and audit trails
- perform and record training
- use a change control process
- create Standard Operating Procedures
- select compliance-ready systems
- archive your data
- train users and prepare your response for
  - Multiple Analyses
  - Multiple Results
  - Review of ALL data including Audit Trails

**DON’T**
- share accounts or passwords
- provide delete privileges to users
- disable the audit trails
- hide or exclude data
- forget to backup your data
- rely on your vendor to be a part of your audit when things get tricky