Data Integrity
An Industry Perspective

Bob Buhlmann
Director Quality Assurance
Amgen Inc.
Data Integrity
Serving Patients is a Privilege...
This Privilege Comes with Significant Responsibilities
Ask Yourself These Questions

• If a company has a Quality Management System and they validate the computer systems they use, Why should they be concerned about Data Integrity?

• Is data a product produced at a Company?

• Can you detect potential data integrity events?
Pop Quiz – Used by Auditors

- Do you have your source electronic data (with content & meaning in data Backup & Archive)?
- Do you review your source e-data (or just printouts)?
- Does your review of source e-data include a review of meaningful metadata (such as audit trails or time/date stamps)?
  - SOP’s on data review to include review of Audit trail
  - SOP’s on data review training – users need to know data flow
- Do you have proper segregation of duties especially regarding system admin/engineer level access.
- Have you validated your system for “intended use” – not just functional testing? (especially important for commercial off the shelf COTS systems)

Prepare your staff – They will be asked these questions
Message From FDA

• “Data integrity problems mean that the quality system is deficient in some way. This takes a lot of resources to fix. A lot of this is about changing the culture within the company. When we find a data integrity problem, it is just like the tip of the iceberg, and it speaks to the overall quality system of a firm.”

So What’s the Problem

• The past several years have brought increased concern and level of regulatory attention to issues surrounding:
  – Access controls to electronic systems
  – Audit trail reviews
  – Backing up of data
  – Supplier quality management

• The top deficiencies relating to data integrity found by the FDA in 2015 were:
  – Failure to include complete data (211.194(a))
  – Audit trail, data control, and sharing password (211.68(b))
Learning Objectives

At the completion of this presentation you will have an awareness and understanding of the following topics:

- Defining Data Integrity – The Objective and Importance
- The Impact of Data Integrity Issues
- Data Integrity Elements
- Data Integrity Program
A Quick Quiz

Here is a common scenario involving data integrity for paper and electronic records. For this scenario, you are acting as a data reviewer.

As you are reviewing a GMP paper record, you notice that modifications have been made—the person who recorded the data has lined out the original value and recorded the new value, along with his or her initials and the date.

Now think about if you were looking at a similar record in its electronic form? Would you need to look for modifications to the data? If so, where would you look?
A Quick Quiz

➢ It’s not necessary—as long as the data is correct on the screen, that’s all that matters
➢ Review modified or deleted data that is captured in the audit trail
➢ None – It’s a validated system
➢ Review the supporting data, which may be in another system
Defining the Objective

- The elements of Data Integrity is what gives data its trustworthiness...
  - Reliability: Completeness and Accuracy
  - Authenticity: It is what it claims to be
  - Reviewability: It can be reviewed and interpreted with its full meaning and context

Good Documentation Practices → Trustworthiness
So What is Data Integrity?

- Data has to be complete, accurate, and consistent through its entire lifecycle.
Why is Data Important?

- Data is as important as the research and products we produce.
- Everything we do is supported by the appropriate data.
- The data creates the trust required to discover, develop, commercialize, and distribute medicines successfully.
- Records, paper or electronic, are the foundational evidence that our products are safe and effective.

When a firm fails to protect its data, it cannot serve patients...
Companies are Being Cited for Data Integrity Concerns

- There is a noticeable increase in the number of enforcement actions taken by regulators
- Actions include the refusal to accept or approve new product filings and the refusal to allow distribution
- The agency is also relying on evidence from other regulatory bodies as the basis for taking regulatory actions

A strong data integrity program is required to serve every patient, every time
Common Data Integrity Issues

Regulatory bodies have continued to find many instances of deficiencies since 2005

<table>
<thead>
<tr>
<th>Data Integrity Concepts</th>
<th>Potential Citations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Re-running samples, Copying existing data as new data, Discarding samples</td>
<td>• Testing into compliance</td>
</tr>
<tr>
<td>Not recording activities contemporaneously</td>
<td></td>
</tr>
<tr>
<td>Electronic records, including data, that may have been changed without the change being documented or justified</td>
<td></td>
</tr>
<tr>
<td>Fabricating data, Backdating, Sharing Access</td>
<td>• Releasing a failing product</td>
</tr>
<tr>
<td>Not saving electronic or hard copy data</td>
<td></td>
</tr>
<tr>
<td>Electronic records and paper records of the same event that are not in agreement</td>
<td></td>
</tr>
</tbody>
</table>
GMP regulations do not require determining intent while assessing Data Integrity, however companies should determine intent. Even with deliberate falsification of records, companies must understand the dynamics that drove and allowed the individual to do this if companies are to truly fix the issue and prevent its reoccurrence.

Without an understanding of the true root causes for human misbehavior, companies may be forced to take widespread actions that may not be indicated, especially when factored with the preventive data integrity measures already in-place. 
Data Integrity – What to Look For
Data Integrity Risk Factors

- Personnel
  - Not Aware
  - Not Trained
  - Culture

- Data Review
  - Insufficient
  - Not Done
  - Not in SOP

- Processes
  - Not Validating for Intended Use

- Outsourcing
  - QC Lab Manufacturing
### Main Elements Data Integrity Program

<table>
<thead>
<tr>
<th>Prevent</th>
<th>Detect</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Personnel (Internal/External)</td>
<td></td>
</tr>
<tr>
<td>• Validation</td>
<td></td>
</tr>
<tr>
<td>• Security Controls</td>
<td></td>
</tr>
<tr>
<td>• Documentation Control</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Data Review</td>
</tr>
<tr>
<td></td>
<td>• Audits</td>
</tr>
<tr>
<td></td>
<td>• Investigate/Corrective &amp; Preventive Actions</td>
</tr>
<tr>
<td></td>
<td>• Impact to Products and Patients</td>
</tr>
</tbody>
</table>
Personnel - Internal

State and enforce high standards of ethics and integrity by:

- Training employees on proper data handling and reporting
- Start from the Top – Corporate Staff - Build into Company Values and Code of Conduct
  - Does your company have these properly defined and disseminated
- Emphasize that everyone in the company is responsible for data integrity
Finding

- Review of Electronic Data & Metadata: Data review practices fail to include adequate review of source electronic data and meaningful metadata (such as audit trails or other metadata such as reprocessing records, history files, alarm records, etc.) to assure the integrity of reported data.

- **For example,** Missing adequate SOPs and Training that define Data Review to include a review of the system’s source electronic data and meaningful metadata (which may in some cases reside in audit trails and in other cases reside in other metadata) to assure the integrity of reported information.
Personnel - External

When utilizing contractors and vendors for GxP services:

- Internal Audits must include reviews for data integrity controls
- Quality Agreements and Contracts must include data integrity controls
Validation

- Computerized systems must be validated for intended use

- Identify the Risks:
  - Controls to prevent & detect data integrity issues

- Include Data Life Cycle requirements
  - Collection, Process, Review, Reporting, Archiving

- Identify Critical Data and Records

- Backup and Recovery
  - Need metadata
  - Readily retrievable & viewable
Security Controls

- Protect at both the physical level (building/room) and the informational level (network and application)
- Access Controls
  - Identify each user uniquely
  - Establish password controls
  - Enforce segregation of duties
- Include Cyber Security – Be protected from the outside ...But be Prepared
Finding

➢ There is inadequate assurance of periodic review of security access rights.

➢ **For example,** Security access rights still enabled in some systems for persons who have left the site or changed roles
Documentation Control

- Managing the life of the data (paper-based and/or electronic) from initial creation, review and approval, storage (including archival), through obsoletion (in accordance with data retention rules)

- Ensure policies and procedures define the requirements for both paper and electronic data and their usage
## Good Documentation Practices

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Paper Records</th>
<th>e-Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legible</td>
<td>• Print name or use signature log</td>
<td>• Name associated to login ID</td>
</tr>
<tr>
<td>Contemporaneous</td>
<td>• Dated in sequence of actions</td>
<td>• Time/date stamped in sequence of actions</td>
</tr>
<tr>
<td>Permanent</td>
<td>• Pen (black or blue)</td>
<td>• Audit modifications or deletions</td>
</tr>
<tr>
<td></td>
<td>• Don’t use pencil or white out</td>
<td>• Don’t use annotation tools</td>
</tr>
<tr>
<td>Attributable</td>
<td>• Signature or initials</td>
<td>• Login or e-signature</td>
</tr>
<tr>
<td>Traceable</td>
<td>• Attach supporting data</td>
<td>• Link to supporting data</td>
</tr>
<tr>
<td>Time/Date Stamped</td>
<td>• Dated</td>
<td>• Time/date stamped</td>
</tr>
<tr>
<td>Changes</td>
<td>• Single line cross-out</td>
<td>• Audit trail</td>
</tr>
</tbody>
</table>

cGMP requirements apply to both paper and e-records
Lab Instrument Example

- Lab instruments timestamp can be altered by user
Main Elements for Data Integrity

Prevent
- Personnel (Internal/External)
- Validation
- Security
- Documentation Control

Detect
- Data Review
- Audits

Respond
- Governance
- Findings/Investigations
- Corrective/Preventive Action
Data Review

➢ Good Documentation Practices
  ✓ Legible, Contemporaneous, Permanent, Attributable, Traceable, Time/Date Stamped

➢ System Audit Trail
  ✓ Tracks actions of System Administrator
  ✓ Reviewed periodically based on risk
  ✓ Defined in Administrators SOPs

➢ Data Audit Trail
  ✓ Tracks actions of users, reviewers, and approvers
  ✓ Is reviewed when the data is reviewed
  ✓ Defined in User Operational SOPs
Audits

- An independent audit program that utilizes auditors who are qualified by education, experience and training to evaluate the quality systems used for collecting, analyzing, reporting and retaining information and data.

- The audit program will include periodic audits to confirm adherence to established requirements for data integrity.
Finding

- Access to data systems are not matched by role or function to job description
  - *For example,* The Owner who is the COO of the company has security access to the database server which can pose a potential data integrity issue.

- QC laboratory managers have been granted an additional administrative account which is a shared account with more rights as needed.
  - Check who has system access within the company
  - Personnel is not taken off the access list when leaving or changing jobs within the company
## Comparing Paper and Electronic Records

<table>
<thead>
<tr>
<th>Activity</th>
<th>Paper Records</th>
<th>Electronic Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOP Approval</td>
<td>• Review the document content and apply wet signature</td>
<td>• Review the document content and apply e-signature</td>
</tr>
<tr>
<td>Batch Record Review</td>
<td>• Review the data in paper Batch Record</td>
<td>• Review the electronic data on screen</td>
</tr>
<tr>
<td></td>
<td>• Review supporting data which is also paper</td>
<td>• Review supporting data which may be in another system</td>
</tr>
<tr>
<td></td>
<td>• Review modified/deleted data that’s lined out, initialed and dated</td>
<td>• Review modified/deleted data that’s captured in audit trail</td>
</tr>
</tbody>
</table>

Many processes are similar, however some require a new way of thinking
## Main Elements for Data Integrity

<table>
<thead>
<tr>
<th>Prevent</th>
<th>Detect</th>
<th>Respond</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Personnel (Internal/External)</td>
<td>• Data Review</td>
<td>• Governance</td>
</tr>
<tr>
<td>• Validation</td>
<td>• Audits</td>
<td>• Findings/Investigations</td>
</tr>
<tr>
<td>• Security</td>
<td></td>
<td>• Corrective/Preventive Action</td>
</tr>
<tr>
<td>• Documentation Control</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Governance/Findings/Actions

- Develop Data Integrity Policy and Procedures to address data ownership throughout the lifecycle
- Consider the design, operation, and monitoring of processes / including control over intentional and unintentional changes to information
Governance/Findings/Actions

- Investigate/Correct/Prevent - Establish and follow procedures for conducting an independent, fair, balanced, and documented review

- If warranted, conduct an in-depth documented investigation of alleged instances of falsification, fabrication, or other misconduct involving Data Integrity issues
  - Include – SME, Quality, HR, and Legal
  - Communicate to Management promptly
And Finally...

- Data integrity is everyone’s responsibility!
- Data Integrity is not a checkbox exercise
- Data Integrity is a significant component of the Quality Management System, providing foundational assurance to stakeholders that the company operates in compliance with regulatory requirements and that its products are safe and effective for their intended use.
- Regulators will assume that non-compliance or faulty data is intentional and not accidental. Inspectors around the world have made it very clear that good intentions are no defense against compromised data.
Thank You