Data Integrity
An Industry Perspective

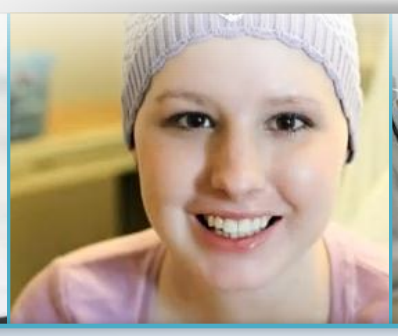
Bob Buhlmann
Director Quality Assurance
Amgen Inc.

Data Integrity

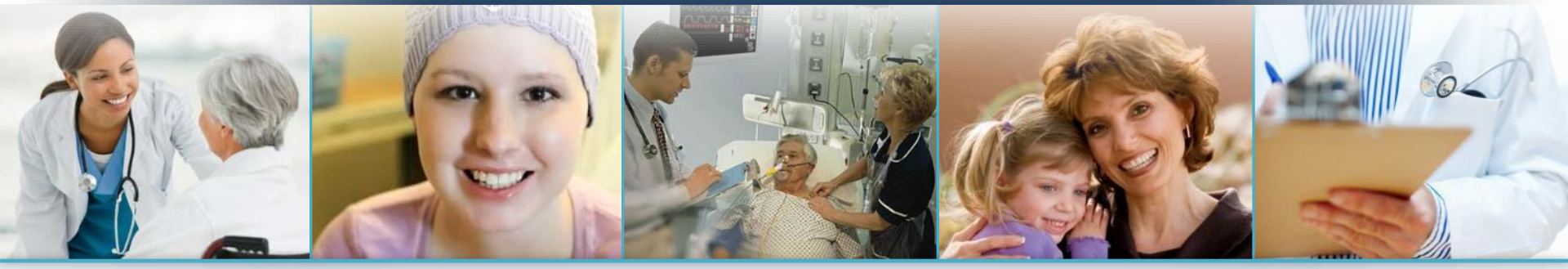




Serving Patients is a Privilege…


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.”

  Paula Katz, director of Guidance and Policy in the Office of Manufacturing Quality/Office of Compliance, Center for Drug Evaluation and Research at FDA, October, 2015 – Gold Sheet

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

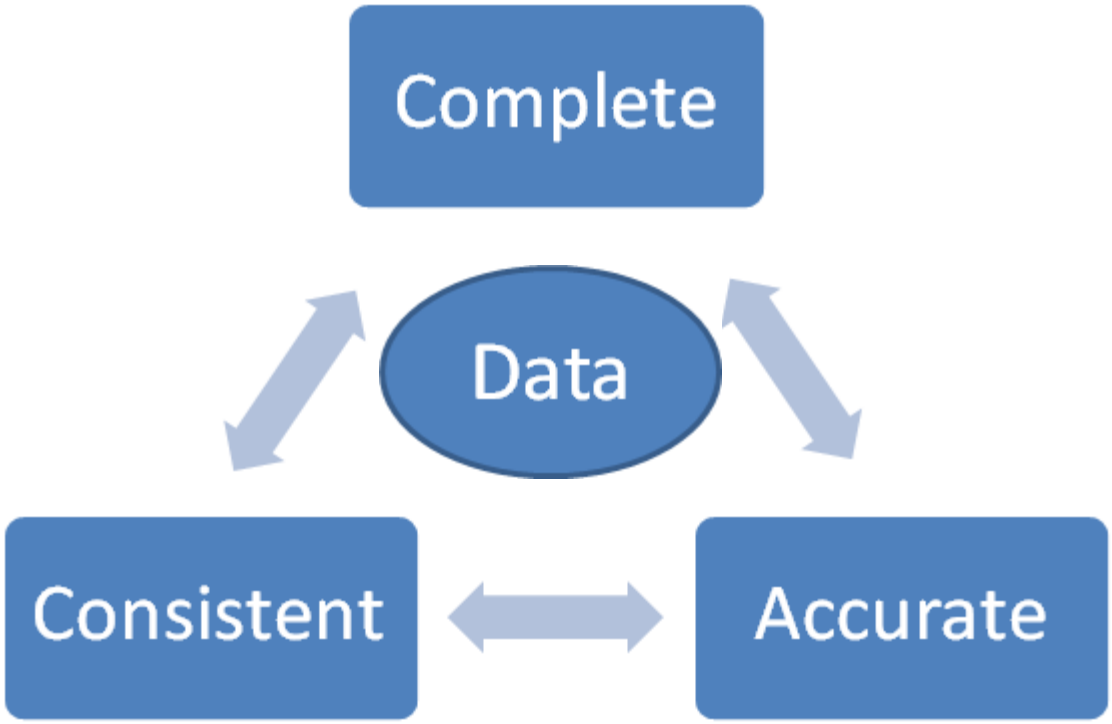
Defining the Objective

- 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

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

Data Integrity Concepts	Potential Citations
Re-running samples, Copying existing data as new data, Discarding samples	• Testing into compliance
Not recording activities contemporaneously	
Electronic records, including data, that may have been changed without the change being documented or justified	
Fabricating data, Backdating, Sharing Access	• Releasing a failing product
Not saving electronic or hard copy data	
Electronic records and paper records of the same event that are not in agreement	

Data Integrity Continuum

System Error

Individual Mistake

Existing Requirements

Individual Malfeasance

Institutional Malfeasance

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.

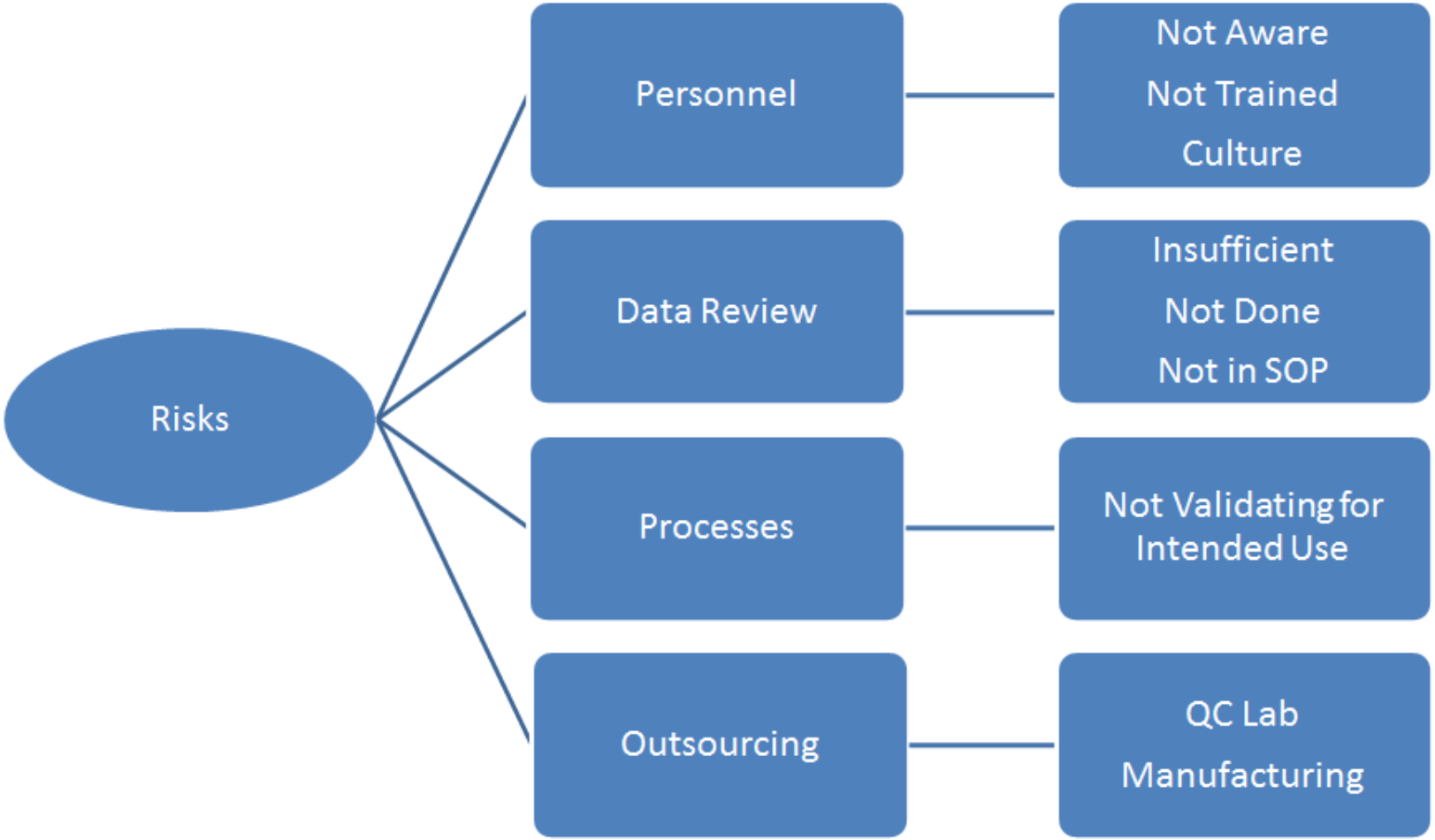
Without an understanding of the true root causes for human misbehavior, companies may be forced to take widespread actions that may not be indicated, especially when factored with the preventive data integrity measures already in-place.

Unintended Error

Deliberate Falsification

Data Integrity – What to Look For

Data Integrity Risk Factors



Main Elements
Data Integrity Program

Prevent	• Personnel (Internal/External) • Validation • Security Controls • Documentation Control
Detect	• Data Review • Audits
Respond	• Investigate/Corrective & Preventive Actions • Impact to Products and Patients

Prevent

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.

Prevent

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

Prevent

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

Prevent

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

Prevent

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

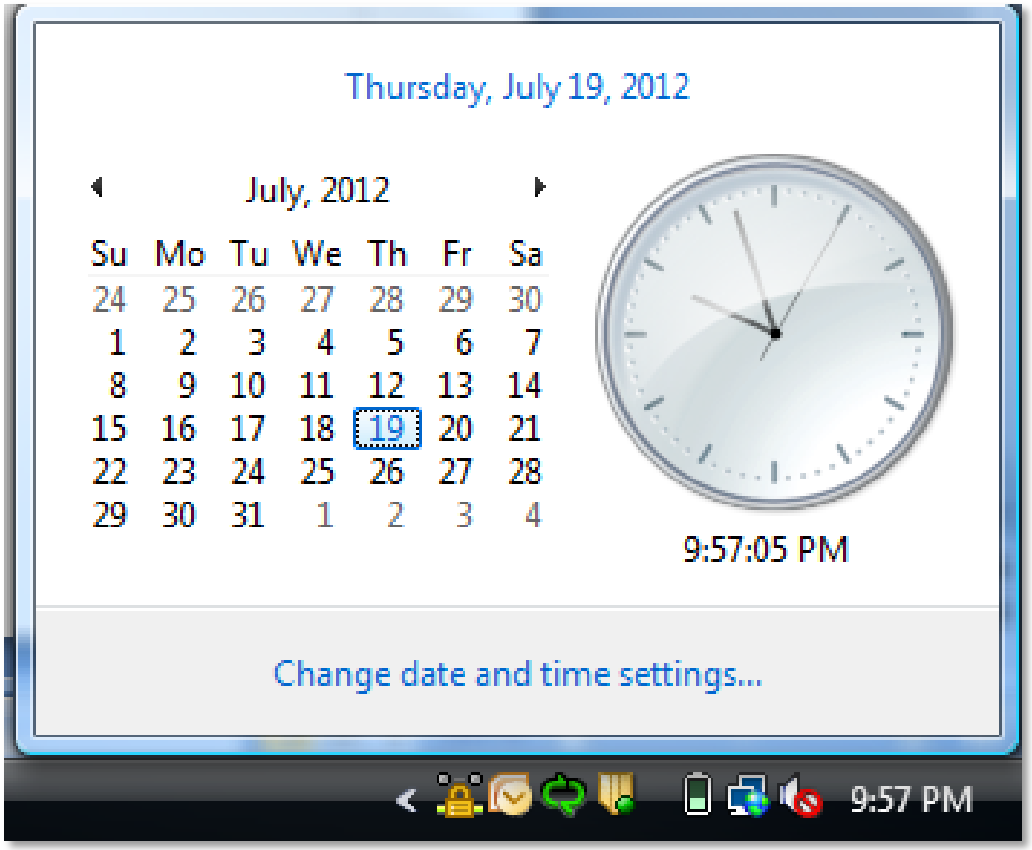
Good Documentation Practices

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

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

Detect

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

Detect

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 witin the company

Comparing Paper and Electronic Records

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

Many processes are similar, however some require a new way of thinking

Main Elements for Data Integrity

Prevent	• Personnel (Internal/External) • Validation • Security • Documentation Control
Detect	• Data Review • Audits
Respond	• Governance • Findings/Investigations • Corrective/Preventive Action

Respond

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

Respond

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 intend 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