DATA INTEGRITY

for Computer Systems: 10 Steps to Compliance

Tish Webb, QC Manager
Bayer Animal Health
August 2017

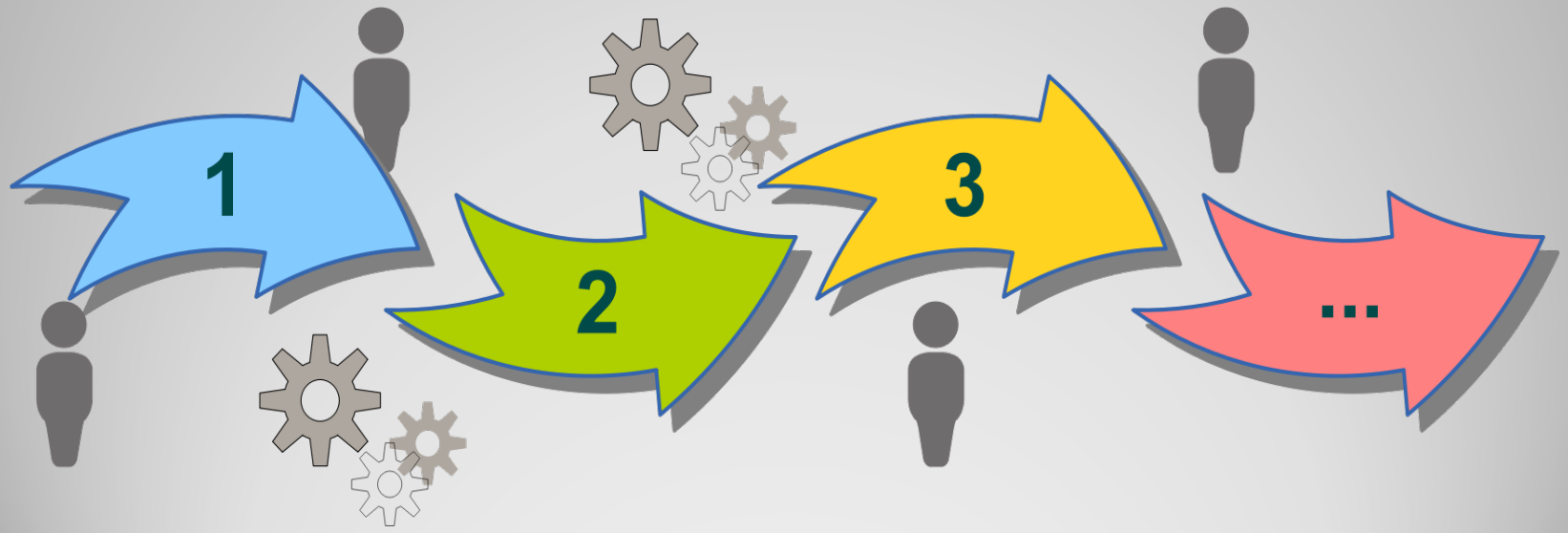
#1: Know the Regulations and Standards

- 21CFR Part 11
- 21CFR 820
- FDA Guidance
- MHRA
- GAMP
- ISO
- AAMI
- Others

What regulations govern the process?

#2: Develop Site Procedures that Conform with Regulatory Requirements

- Single or multiple procedures
- Standard templates for documents
- Training on the procedures



What do our procedures require?

#3: Know What Systems You Have

- Accurate and routinely updated system inventory
- Traceable to a specific instrument and software version
- PLCs are sometimes equipment too
- Walk down GMP areas
- Ask questions

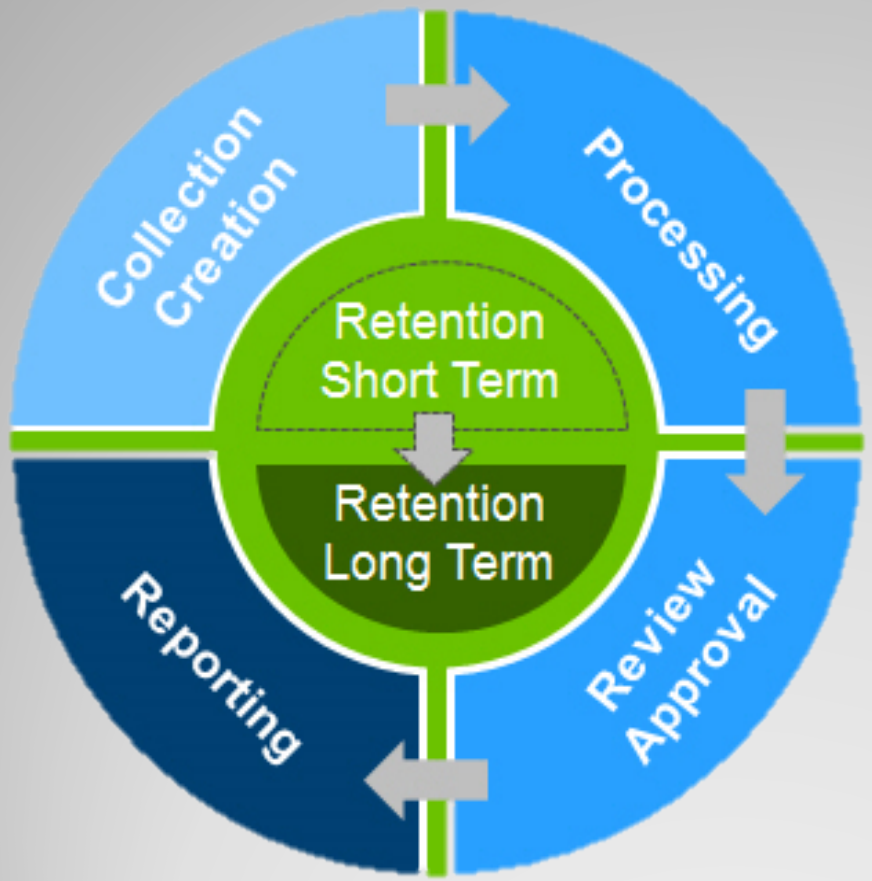
What instruments, equipment and software do we have?

#4: Understand Data Flow for the System

- Is this contained in validation documentation?
- Does the validation documentation support current state?
- Is the data flow documented?
  - It is critical to document and understand before beginning the assessment
  - Use cross functional resources

How is data created and where is stored?

Data Life Cycle: Key Steps



Consider:

- Mode of recording
- Storage locations
- ALCOA+ controls
- Involved roles
- Data types

Do you understand data flow?

Collect/Create	Process	Review	Report	Retain
Overview	Overview	Overview	Overview	Overview
Mode of recording Storage location Templates	Mode of recording Storage location Templates	Mode of recording Storage location Templates	Mode of recording Storage location Templates	Mode of recording Storage location Short/Long Term
Controls (Procedural, Functional) • Correct parameter set, meta data and data? • Complete meta data and data? • Secure location?	**Controls** (Procedural, Functional) • Correct calculations? • Correct transfer, linkage, synchronization? • Certified true copies? • Manual modifications?	**Controls** (Procedural, Functional) • Complete data incl. audit trail (paper+electronic records)? • Segregation of duties?	**Controls** (Procedural, Functional) • Completeness – Prevention of selective reporting! • Completeness – Linkage and synchronizations up-to-date!	**Controls** (Procedural, Functional) • Secure data location for short/long term storage? • Data completeness for long term archive?
Roles (involved)	Roles (involved)	Roles (involved)	Roles (involved)	Roles (involved)
Data Types Original Data Meta Data Raw Data (Original + Meta Data)	Data Types True Copies Meta Data Raw Data (Original /True Copies + Meta Data)	Data Types True Copies Meta Data Raw Data (Original /True Copies + Meta Data)	Data Types Reported Data	Data Types Original Data / True Copies Meta Data Raw Data (Original /True Copies + Meta Data) Reported Data

#5: Determine if the System is GXP Relevant

- Standardize assessment process for consistency
- Simple vs. complex systems
- Stand alone vs. embedded systems
- Product contact
- Associated with ingredient/solvent production
- Used for cleaning or sterilization
- Preservation of product status
- Produce data required for disposition
- Control a process linked to product quality
- Interface with a direct impact system

Is the system GXP relevant?

#6: Determine if the System is Part 11 Compliant

Not all Systems are GXP Relevant

Not all GXP Systems are Part 11 Compliant

Standardize Assessment Strategy

- Assess the software design for compliance
  - Compliant as designed
  - Partially compliant as designed
  - Not compliant as designed

Are GXP relevant systems Part 11 compliant?

#7: Understand the Level of Risk the Data Poses to Patient Safety

- High risk – Data directly associated with material / product from receipt to release.
  - Batch control systems, vision systems, lab systems, critical utility monitoring systems
- Medium risk – Data in the systems supports product disposition decisions but is not the primary source of the raw data.
  - Deviation management systems, document management systems
- Low risk – Data in the systems support GMP processes but do not directly impact product quality.

What risk does the data pose to patient safety?

#8: Develop Risk Assessment and Remediation Plan for Each GXP Relevant System

- Assess high risk systems first
- Detail the requirements for security and documentation controls
  - Document the technical or procedural controls in place for each requirement
  - Document if the requirement is met or there is a gap
  - Traceability to CAPA for gaps
- Interim control strategy for CAPA that will take longer to complete

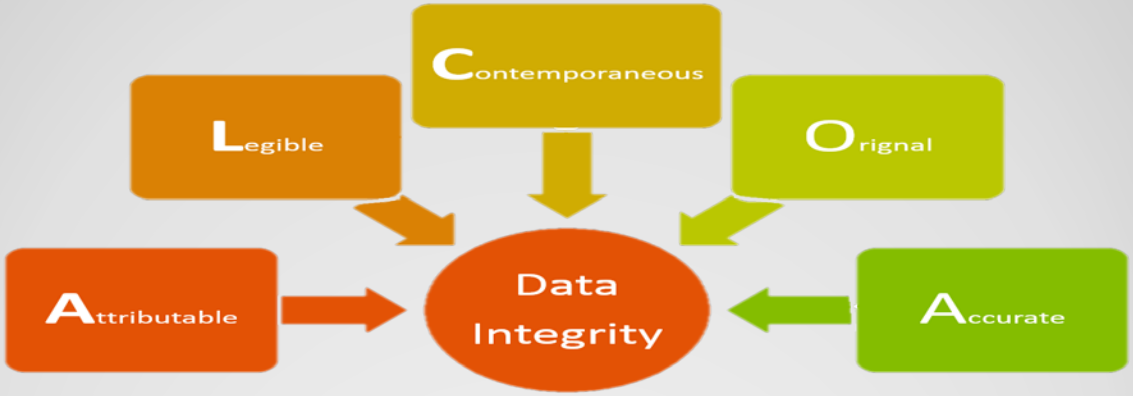
What is the current state?

Documentation Processes

- System design and controls
- Validation and life cycle package focusing on data flow, system configuration, data access, authorization and testing
- Procedures for operation and use and if needed, agreements with IT
- Procedures for administration
- Periodic controls to ensure data integrity
- Access rights
- Audit trails

What do we assess?

- Is data saved contemporaneously?
- How is the data reviewed?
- Is an audit trail or activity log implemented?
- Do the contents of the audit trail follow ALCOA principles?
- Is the audit trail reviewed prior to disposition?
- Are electronic records restricted from modification after e signature?
- Can audit trails be enabled/disabled or deleted by the routine user?
- Are date and time settings protected?
- Do roles and privileges align with segregation of duties? Is original data obscured when modifications are made?
- Does the system make testing into compliance detectable?
- Have these parameters been tested?



How do we assess the system?

#9: Close the Gaps

Some Gaps can be Closed Quickly

Procedural Controls

Updates to Configuration

Others May Require More Time

New Equipment

New Software

Interim Control Strategy:

Procedural Controls with Audit Oversight

Outsource Testing to Labs with Appropriate Controls

How do we close gaps?

Separate Role for Administrator – Segregation of Duties

- Individual with knowledge of the system/equipment
- No data collection capabilities
  - Control technically or procedurally
    - Configure role to not allow data collection
    - Define in SOP and routinely audit

Administration Procedures Documented

- Add/disable users, assign/remove group access
- Backup, Archive and restore
- Periodic and audit trail reviews

Closing the Gaps: System Administration

Built-in Functionality

- Audit trail and content configuration of audit trail
- De-activate or rename standard admin account
- Remove generic login and replace with individual login
- Protect from time/date setting changes
- Secure file storage for data and configuration
  - Move local folder to file server
  - Restrict access rights
  - Prevent deletion of data

Add-on Tools

- Regular centralized/secure backup with verification
- Implement system event log by use of local group policies (Windows/Active Directory)
- Log file creation, changes, and deletion
- Implement report to detect unauthorized changes or deletion

Closing the Gaps: Technical Controls

Standard Operation Procedures

- Access request
- Data governance
- Data review electronic and paper

Use Logs / Logbooks

- Individual user accounts can't be created
- Date/time cannot be locked

Issued Records for Recording and Affixing Static Results

Closing the Gaps: Procedural Controls

#10: Use Lifecycle Management Approach

- Software supplier audits
- Robust change management process
- Computer system assessment and validation procedures
- Periodic review of systems
- Maintaining software updates
- Periodic Audits of conformance to life cycle process
- Training – culture shift

How do we sustain?


ASSESSMENT
measurement
Mission
GOALS
Direct
summative
AFFECTIVE
Program
Rubrics
Valid
Course
test
objectives
COGNITIVE
indirect
FORMATIVE
Curriculum map
Portfolio
focus group
performance
Reliable

Examples

No.	Question	Answer	Controls	Gap	Actions
1. Data Flow					
1.1	Is data flow defined?	Yes	Defined in validation XXX and SOP XXX	No	None
1.2	Are definitions of original data, metadata, raw data, true copy, and processed data defined?	No	Original data, metadata, raw data, and true copy defined	Yes	Revise procedure XXX to include the definition of processed data
1.3	Does the defined set of raw data include complete and accurate data?	Yes	Complete copy of raw data is maintained by the system and locked from further changes	No	None

No.	Question	Answer	Controls	Gap	Actions
2. System Configuration					
2.1	Are critical configuration settings defined?	Yes	Defined in configuration spec XXXX	No	None
2.2	Have the configuration settings been tested?	Yes	Configuration specs were tested in user acceptance testing XXXX	No	None
2.3	Are data and time settings defined and protected from modification by the users on application and operational system?	No	Protected on the application but not protected on the operational system	Yes	Update system setting to allow modification by admin only

No.	Question	Answer	Controls	Gap	Actions
3. Access and Authorizations					
3.1	Are roles and privileges defined and mapped to business roles?	Yes	Defined in configuration spec XXXX	No	None
3.2	Do the defined roles cover segregation of duties for admin and users?	Yes	Defined in configuration spec XXX and tested in user acceptance testing XXXX	No	None
3.3	Are unique user ID implemented for each user and admin of the system?	No	Log used to identify each user, date, and samples analyzed.	Yes	Replace equipment with one where unique ID can be used
3.4	Are built-in standard accounts deactivated?	No	No controls over built in accounts	Yes	Remove access to accounts and test

No.	Question	Answer	Controls	Gap	Actions
4. Procedures and Agreements					
4.1	Do SOPs for admin, maintenance and use of the system exist?	Yes	SOPs XXX (admin) and XXX (user/maint.)	No	None
4.2	Does the admin SOP outlined user access process, routine access reviews, and backup/recovery/ restore process?	Yes	SOP XXX outlines the requirements	No	None
4.3	Does the user SOP detail entering and modifying critical data? Paper vs. electronic records?	No	The SOP does not require electronic data be compared to printed records	Yes	Update SOP to include the paper must be compared to the electronic record
4.4	Are agreements in place with local IT or IT service providers?	Yes	IT changes for server. Config and user changes by system admin	No	None

CAPA #	Gap	Due date	Assigned To	Actions
17-001	Definition of processed data not outlined in SOP	10/5/2017	J. Doe	Revise procedure XXX to include the definition of processed data
17-002	System date/time not locked from editing by user	09/15/2017	J. Doe	Update system setting to allow modification by admin only
17-003	Unique user ID not available in system configuration for users	6/30/2017	J. Doe	Procure and validation replacement system that is Part 11 Compliant
17-004	No controls over built in accounts	9/15/2017	J. Doe	Remove access to accounts and test
17-005	The SOP does not require electronic data be compared to printed records	9/15/2017	J. Doe	Revise SOP to require electronic and paper data comparison.


grazie
dakujem
gràcies
merci
thanks
gracias
ありがとう
спасибо
hvala
obrigado
spas
díky
mochchakkeram
bedankt
danke
bakka bér
شكراً
thank you
gracias
grazas
Arigatō
ačiū
grazie
감사합니다
Tak
köszönöm
gràcies
eskerrik asko
merci
obrigado
aitäh
asante
dziękі
kiitos
ngiyabonga
terima kasih
tack
Salamat
dankie
dankon
dank
Շնորհակալություն