



CDER Compliance Perspective: Data Integrity and CGMP

PTEA Annual Meeting

April 18, 2017

Paula Katz

Director, Manufacturing Quality Guidance and Policy

CDER Office of Compliance

Office of Manufacturing Quality

Office of Manufacturing Quality

- We evaluate compliance with Current Good Manufacturing Practice (CGMP) for human drugs based on inspection reports, evidence gathered by FDA investigators, and other sources.
- We develop and implement compliance policy and take enforcement actions against violative drug manufacturing establishments.



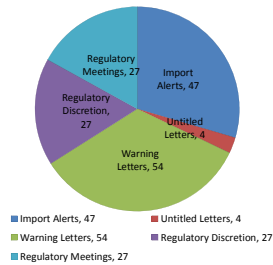
Source: FDA

2

Enforcement tools


- Regulatory Meetings
- Injunctions
- Consent Decrees
- Import Alerts
- Seizures
- Warning Letters
- Untitled Letters
- And More

2016 Enforcement Actions



3

What is data integrity?




Data integrity – requirements that data are **complete, consistent, and accurate.**

ALCOA

- **Attributable**
- **Legible**
- **Contemporaneous**
- **Original / true copy**
- **Accurate**


4

Data integrity



- CGMP = minimum requirements
- Data integrity underpins CGMP
- Lapses obscure other problems


Tip of the iceberg



<http://honghu.com/wallpaper/nature/tip-of-the-iceberg-90833.jpg>


5


Paper requirements = electronic requirements



Requirements for record retention and review do not differ by data format.

Paper-based and electronic data record-keeping systems are subject to the same requirements.





6

Data integrity: Not a new concept



21 CFR 210/211: Mostly in tact since the 1970s!

- 211.68 requires that backup data are exact and complete, and secure from alteration, inadvertent erasures, or loss.
- 212.110(b) requires that data be stored to prevent deterioration or loss.
- 211.100 and 211.160 require documentation at the time of performance and that laboratory controls be scientifically sound.
- 211.180 requires true copies or other accurate reproductions of the original records.
- 211.188, 211.194, and 212.60(g) require complete information, complete data derived from all tests, complete record of all data, and complete records of all tests performed.

7

API - ICH Q7



Computerized systems (5.4):

- Computerized systems should have sufficient controls to prevent unauthorized access or changes to data. There should be controls to prevent omissions in data (e.g., system turned off and data not captured). There should be a record of any data change made, the previous entry, who made the change, and when the change was made.
- If system breakdowns or failures would result in the permanent loss of records, a back-up system should be provided. A means of ensuring data protection should be established for all computerized systems.

Q7 Good Manufacturing Practice Guidance for Active Pharmaceutical Ingredients

8

API - ICH Q7




Computerized systems (5.4):

- GMP-related computerized systems should be validated.
- Appropriate installation and operational qualifications should demonstrate the suitability of computer hardware and software to perform assigned tasks.
- Incidents related to computerized systems that could affect the quality of intermediates or API or the reliability of records or test results should be recorded and investigated.

Q7 Good Manufacturing Practice Guidance for Active Pharmaceutical Ingredients

9

API - ICH Q7




ALCOA Principles:

- All quality-related activities should be recorded at the time they are performed. (2.15)
- Laboratory controls should be followed and documented at the time of performance. Any departures from the above-described procedures should be documented and explained. (11.14)
- CoAs (11.4)
- Agents, brokers, distributors, repackers, or relabelers should transfer all quality or regulatory information received from an API or intermediate manufacturer to the customer, and from the customer to the API or intermediate manufacturer. (17.60)
- And more!

Q7 Good Manufacturing Practice Guidance for Active Pharmaceutical Ingredients

10

Draft guidance




Data Integrity and Compliance With CGMP, draft guidance for industry (April 2016)

- Why? FDA has increasingly observed CGMP violations involving data integrity during CGMP inspections.
- 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.

Available at
www.fda.gov/downloads/drugs/guidancecomplianceregulatoryinformation/guidances/ucm495891.pdf

11

What is 'metadata'?



- Contextual information required to understand data
- Structured information that describes, explains, or otherwise makes it easier to retrieve, use or manage data
- For example: date/time stamp, user ID, instrument ID, audit trails, etc.
- Relationships between data and their metadata should be preserved in a secure and traceable manner

12

What is an 'audit trail'?



- Secure, computer-generated, time-stamped electronic record that allows for reconstruction of events relating to the creation, modification, or deletion of an electronic record
- Chronology: who, what, when, and sometimes why of a record
- CGMP-compliant record-keeping practices prevent data from being lost or obscured

13

Audit trails capture...



- Overwriting
- Aborting runs
- Testing into compliance
- Deleting
- Backdating
- Altering data



• *(not an all-inclusive list)*

14

"Static" and "Dynamic" Records



- Static: fixed data document such as a paper record or an electronic image
- Dynamic: record format allows interaction between the user and the record content such as a chromatogram where the integration parameters can be modified

15

How does FDA use the term 'backup' in 211.68(b)?



- True copy of the original data that is maintained securely throughout the records retention period.
- Should include associated metadata.
- Synonymous with "archival," not crash recovery.

16

How often should audit trails be reviewed?



- For audit trails that capture changes to *critical data*, FDA recommends review of each record before final approval of the record.
- Routine scheduled audit trail review based on the complexity of the system and its intended use.
- At a minimum, audit trails subject to regular review should include changes to:
 - history of finished product test results
 - sample run sequences
 - sample identification
 - critical process parameters

17

Who should review audit trails?



- Audit trails are considered part of the associated records.
- Personnel responsible for record review under CGMP should review the audit trails that capture changes to critical data...as they review the rest of the record.

18

Case study: Audit trail review



- Observed repeat GC injections in the audit trail from June 12, 2013.
- Audit trail showed the computer date/time settings were set back in July 2013 to June 12, 2013 (audit trails go in chronological order, but the dates didn't and showed multiple June 12ths).
- Results were reprocessed and printed to show that they had achieved passing results on June 12, 2013.
- Firm relied on this data to release the batch.
- Similar situation was observed for HPLC testing.

Warning letter?

Because your quality unit did not review the original electronic raw data, you were unable to detect rewritten, deleted, or overwritten files. (January 2015)

19

When is it permissible to exclude CGMP data from decision making?



- Data created as part of a CGMP record must be evaluated by the quality unit as part of release criteria and maintained for CGMP purposes
- Electronic CGMP data should include relevant metadata
- To exclude data from the release criteria decision-making process, there must be a valid, documented, scientific justification for its exclusion

20

Case study: Tablet press



- Errors and discrepancies observed in tablet press log.
- Firm had justification and explanation in appropriate batch records.
- SOP was followed.
- Batch release decision included all pertinent data.

Warning letter?

Not even a 483 observation!

21

Does each workflow on our computer system need to be validated?



- Yes, a workflow, such as creation of an electronic MPCR, is an intended use of a computer system to be checked through validation
- If you validate the computer system, but you do not validate it for its intended use, you cannot know if your workflow runs correctly

22

Federal Register January 1995



manufacturing process. Less dramatic events, such as faulty data entry or programming, can also trigger a chain of events that result in a serious production error and the possible distribution of an adulterated product. Thus, while increasingly sophisticated system safeguards and computerized monitoring of essential equipment and programs help protect data, no automated system exists that can completely substitute for human oversight and supervision.

23

How should access to CGMP computer systems be restricted?



- Appropriate controls to assure only authorized personnel change computerized:
 - MPCR's
 - Input of laboratory data into records
 - Other records
- Recommend restricting the ability to alter:
 - Specifications
 - Process parameters
 - Manufacturing or testing methods
- Assign system administrator role, including rights to alter files and settings, to personnel independent from those responsible for record content.
- Maintain a list of authorized individuals and their access privileges for each CGMP computer system in use.

24

Case study: Administrator privileges “If I could turn back time...”



Warning letter: *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. (May 2016)

25

Why is FDA concerned with the use of shared login accounts for computer systems?



A firm must:

- exercise appropriate controls to assure that only authorized personnel make changes to computerized records,
- ensure actions are attributable to a specific individual.

26

Case study: Shared logins




- No passwords were required to login
- Anyone who accessed the system had full software administrator privileges.
- An analyst stated that **someone else had used their login** to delete and modify data.

Warning letter?


Provide specific details of the steps you have taken to prevent unauthorized access to your electronic data systems and to ensure that data systems retain complete, accurate, reliable, and traceable results of analyses performed. (November 2015)

27

How should blank forms be controlled? 

- Blank forms (e.g., worksheets, laboratory notebooks, and MPCRs) should be controlled by the quality unit or by another document control method.
- Numbered sets of blank forms may be issued and should be reconciled upon completion of the activity.
- Incomplete or erroneous forms should be kept as part of the permanent record along with written justification for their replacement.


28

Case study: Blank forms 

- Uncontrolled blank and partially completed CGMP forms
- Supervisor photocopied a blank OOS form and transcribed the information because of "mistakes" in the original
- Did not follow own SOPs
- Firm stated that they "do not consider this OOS form to be an official document until it is initiated into the QA system"

Warning letter?
Your quality unit is responsible for reviewing and approving these critical production records to ensure that, if an error occurred, a comprehensive investigation is conducted. Uncontrolled destruction of CGMP records also raises concerns, because retention of CGMP records must follow established procedures approved by your quality unit. (January 2017)

29

Can electronic copies be used as accurate reproductions of paper or electronic records? 

- Yes
- Provided copies preserve the content and meaning of the original data, which includes associated metadata and the static or dynamic nature of the original records.

30

Electronic copy of a paper document



31

Can you retain paper printouts/static records instead of original electronic records from computerized laboratory instruments?



- If it is a complete copy of the original record.
- For example, pH meters and balances may create a paper printout or static image during data acquisition as the original record.
- Electronic records from certain types of laboratory instruments are dynamic records, and a printout or a static record does not preserve the dynamic format which is part of the complete original record.


32

Stand-alone electronic instrument




Source: Omega.com

33

Can electronic signatures be used instead of handwritten signatures for master production/control records? 

- Yes.
- Part of the intent of the full signature requirement is to be able to clearly identify the individual signing the record.
- Appropriate controls to securely link the signature and associated record.

34

When does electronic data become a CGMP record? 

- When it is generated to satisfy a CGMP requirement.
- You must document, or save, the data at the time of performance.
- You may employ a combination of technical and procedural controls to meet CGMP documentation practices.
- Computer systems, such as LIMS or EBR systems, can be designed to save after separate entries.

35


Case study: “Mock sheets” 

- Operators used “mock” sheets to capture critical manufacturing data.
- Batch production records were completed and backdated days after operations ended.
- Discrepancies between the “mock” sheets and the complete batch production record
- No evidence that batch production records were accurate

Warning letter?

Failure to record activities at the time they are performed, and destruction of raw data. (May 2016)

36

What is wrong with using samples during 'system suitability' or test, prep, or equilibration runs? 

- FDA prohibits sampling and testing with the goal of achieving a specific result or to overcome an unacceptable result.
- System suitability should use a standard or a properly characterized secondary standard.
- All data should be included in records retained and subject to review, and be included in decision making unless there is documented scientific justification for its exclusion.

37

Case study: Stability samples 


This is only a test. If it were an actual sample, it would be reported in the official data package.

- Trial injections of "stability samples" saved in the "test" folder.
- Official samples analyzed after trial injection.

Warning letter?


Your response indicates that the "Test" folders were used to equilibrate the analytical columns and to determine when the system was ready for analysis. It is your responsibility to follow validated methods that include specific procedures to assess the suitability of your instruments... (March 2015)

38

Is it acceptable to only save the final results from reprocessed laboratory chromatography? 

- No.
- Analytical methods should be capable and stable.
- If reprocessed, written procedures must be established and followed.
- FDA requires laboratory records include complete data derived from all tests.


39

Can internal quality tips, e.g., suspected data falsification, be handled outside the quality system? 

- No.
- Fully investigate under the quality system to:
 - Determine the effect of the event on patient safety and product quality and on data reliability
 - Determine root cause.
 - Ensure the necessary corrective actions are taken.


Report suspected data integrity problems:
DrugInfo@fda.hhs.gov with “CGMP data integrity” in the subject line.

40

Should personnel be trained in detecting data integrity issues as part of a routine CGMP training program? 

- Yes, detecting data integrity issues is consistent with the CGMP requirements for personnel qualifications.
- Personnel must have the education, training, and experience, or any combination thereof, to perform their assigned duties.

41

Is the FDA investigator allowed to look at my electronic records? 

- Yes.
- All records required under CGMP are subject to FDA inspection.

See FDA guidance, *Circumstances that Constitute Delaying, Denying, Limiting, or Refusing a Drug Inspection* (October 2014)
<http://www.fda.gov/downloads/RegulatoryInformation/Guidances/UCM360484.pdf>

42

Case study: All Thumbs



- Investigator observed analyst using a thumb drive and asked to see the contents of the drive.
- The analyst ran away. With the drive.

Warning letter?

During the inspection, an analyst removed a thumb drive from a computer controlling an HPLC. When asked to provide the drive, the analyst instead exited the room with the thumb drive. After approximately 15 minutes, management provided our investigator with what they asserted was the thumb drive in question. It is impossible to know whether management provided the same thumb drive that the analyst had removed. (December 2015)

43

How does FDA recommend data integrity problems identified during inspections be addressed?



- Demonstrate effective remediation by:
 - Hiring third party auditor
 - Determining scope of the problem
 - Implementing corrective action plan (globally)
 - Removing individuals responsible for problems from CGMP positions
- FDA may re-inspect

44

Responding to Data Integrity Failures



Data Integrity section in recent FDA Warning Letters with data integrity citations, requests firms respond with 3 key pieces:

- Comprehensive Evaluation (Scope)
- Risk Assessment (Scope)
- Remediation and Management Strategy (including corrective action plan)

45

Comprehensive investigation



A comprehensive investigation should include:

- **Detailed investigation protocol and methodology:** summary of all laboratories, manufacturing operations, and systems to be covered; justification for anything to be excluded.
- **Interviews of current and former employees** to identify the nature, scope, and root cause of data inaccuracies. Should be conducted by a third party.
- **Assessment of the extent of data integrity deficiencies.** Identify omissions, alterations, deletions, record destruction, non-contemporaneous record completion. Describe all operations with data integrity lapses.
- **Comprehensive retrospective evaluation** of the nature of the data integrity deficiencies. Qualified third party with expertise specific to firm's breaches should evaluate the lapses.

46

Risk assessment & management strategy



A current **risk assessment** of the potential effects of data integrity failures on the quality of your drugs.

Should include analyses of risks to patients due to release of drugs produced with data integrity lapses as well as risks posed by ongoing operations.

47

Management strategy



A management strategy for your firm that includes the details of your global corrective action and preventive action plan. Your strategy should include:

- A **detailed corrective action plan** that describes how you intend to ensure the reliability and completeness of all of the data you generate, including analytical data, manufacturing records, and all data submitted to FDA.
- A comprehensive description of the **root causes** of your data integrity lapses, including evidence that the scope and depth of the current action plan is commensurate with the findings of the investigation and risk assessment. **Indicate whether individuals responsible for data integrity lapses remain able to influence CGMP-related or drug application data at your firm.**
- **Interim measures** describing the actions you have taken or will take to protect patients and to ensure the quality of your drugs, such as notifying your customers, recalling product, conducting additional testing, adding lots to your stability programs to assure stability, drug application actions, and enhanced complaint monitoring.
- **Long-term measures** describing any remediation efforts and enhancements to procedures, processes, methods, controls, systems, management oversight, and human resources (e.g., training, staffing improvements) designed to ensure the integrity of your company's data.
- A status report for any of the above activities already underway or completed.

48



ACKNOWLEDGEMENTS:

Sarah Barkow
Karen Takahashi

THANK YOU!
QUESTIONS?

49
