Data Integrity - a Document Control Challenge

By Kevin Bogert

azimuth
COMPLIANCE CONSULTING

Data Integrity - A Document Control Challenge

The FDA has increasingly observed cGMP violations involving data integrity during inspections. The purpose of the data integrity guidance is to help manufacturers have the tools and systems in place to prevent adulterated products from entering the U.S. marketplace. This paper examines the FDA's data integrity guidance document and observations related to control of documents, both electronic and hardcopy.

The agency refers to data integrity as "the completeness, consistency, and accuracy of data. Complete, consistent, and accurate data should be attributable, legible, contemporaneously recorded, original or a true copy, and accurate (ALCOA).[1]" Data integrity does not end when the data is captured, either on a paper form or a computer system. It is critical throughout the cGMP data life cycle until final disposition of data after the record's retention period ends.

Both static and dynamic data are important to any cGMP organization. The FDA uses 'static' to indicate a "fixed-data record 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.[2]" A document control department works primarily with static data in the form of electronic and printed documents and forms.

The primary areas of focus of the data integrity guidance, as it relates to document control, are on record retention, audit trails, control of the original documents, and any blank forms or copies that were not used. The organization must ensure that additional blank forms are not printed beyond what is required to perform the task. Controls should be put in place to prevent a user from making copies of forms without a mechanism to identify the copies from the original.

In one 483, the FDA cited the company for "Issuance and use of documents is not controlled." The FDA visited the company and looked at their electronic document system and their document control process. They did not focus on the review and approval process, which must be part of a document control system, rather the investigator focused on the control of the printed documents and in particular control of blank and original documents.

The 483 observation states that "Controls have not been established to ensure submitted paper documents are original. Personnel responsible for recording GMP data can print GMP records used to record raw data from the document system. The number of documents printed is not tracked, allowing personnel to reprint forms without oversight. Personnel were observed to print more documents than needed and discard extras."

The key in this observation is the agency did not use the term document control system when referring to this company's electronic system. Rather they referred to the electronic system as a document system and that documents were not controlled. This was not the limitation of the electronic system, as it met the requirements of the industry for a document control system but not the requirements for data integrity. The inspector was looking for controls around the printing of the document and to ensure the submitted documents are the original and that blank documents were properly handled.

Electronic Document Control Definition

Most companies believe that a document control system includes functionality of a document management system with version control, audit trail, and electronic signature. It automatically manages and retains all old historic versions together with information on who changed it and why, who authorized it and who was advised of the change. It will also include periodic recall for review of selected documents without operator intervention.

The problem with this definition is that it limits the scope of a document control system to only managing the approval and control of an electronic document. The FDA considers the document throughout its lifecycle as requiring a certain level of control. This lifecycle includes approved and unapproved controlled documents as they move from creation to retirement, including their daily usage. The system should track the daily usage of the document from printing, including the number printed, until submitted back to Document Control as required to comply with data integrity requirements.

The Gap Between Document Control Department Requirements and Software Used

Three examples of requirements were identified in the observation that were not provided by the electronic system or outlined in procedures based on the 483 observation.

1. How to control unapproved documents that are used by employees.
2. How to control the printing of documents.
3. How to track the document once it is printed until it is submitted to Document Control for storage, including any copies or unused (blank) documents.

These three requirements can become a major burden on a document control department and very costly to manage when the functionality is not provided by technology or controlled through procedures.

When defining your requirements for a document control system, you should consider these areas:

- Document control features for workflow management – easy to use drag and drop workflow tools for defining approval paths,
- Scanning and Data Capture – To capture an image of the original documents,
- Records retention management (data integrity requirement),
- Hard copy document control – Places a unique control number on every printed page that is tracked by the system from time of printing until the document is returned to document control for storage (data integrity requirement),
- Audit trail and electronic signature as required by 21 CFR Part 11.

A Process to Control Unapproved Documents from Being Used by Employees

What is not known from the example provided in the observation is if this document was an unapproved copy that came out of the document system and stored on the shared drive or a draft copy that was being used by the organization prior to approval. The control of unapproved documents can be managed by a combination of IT controls of shared and local drives on company computers and company policies on the usage of unapproved documents.

First, documents must not be used by employees that are not approved unless duly justified. Second, all documents should have control numbers printed on every page. If this control number is not available, then the document should not be used. Third, draft documents should never be stored on local or shared drives once they are under the control of the document system. The document system should have a way that prevents the user from checking out a document and storing it locally or on a shared drive. And finally, IT department could implement business rules that remove documents from shared and local drives daily or restrict user access to the folders on the shared drives.

An electronic system can help you with this in many ways. The electronic system should fully control a document once it is under its control. The document system should allow you to work on draft copies of the document but store any changes back into the system not on a local or shared drive. A check-in, check-out, and collaboration functionality could provide such controls if you are prevented from saving the document outside of the electronic system. The system should turn off the "Save As" functionality in the word processor to prevent the document from being saved to another location.

A Process to Control the Printing of Documents

If the document system you are using does not have the functionality to control printing, a few steps can be implemented to control the printing of documents. Your IT department must restrict what printers are available to users. It is recommended that the only printers available are those located in document control or in a controlled area where an individual has responsibility for all printed documents. The document system should not allow the printing of documents to PDF. Depending on the system you use, these controls may not be possible. Finally, you need to stamp a tracking number on each printed copy of the document and record that information in a logbook.

There is a better way to handle this by using an electronic system that can meet the following requirements:

- Limit who can print documents from the system.
- Restrict how many copies can be printed.
- Apply a unique control number to each printed copy of the document.
- Track who printed the document, the unique identifier for each printed document, and when the document is due back to the document control department.
- Not allow the printing to PDF or any other format that would allow a copy to be saved to a hard drive.
- Restrict the user from printing a new version of a document if that user printed an older version of the document that has not been returned to the document control department.
- Prevent the user from making a copy of a document or provide a way to identify a copy from the original.

A Process to Track the Document Once it is Printed

If the system that you use does not have the capability of assigning control numbers or tracking documents, the next best thing is to have the watermark stamp a date and time printed on the document or configure the printers to place date and time at printing. A spreadsheet or form should be maintained to track all documents, the date and time printed, and a control number for each printed copy, if the system is not capable of doing this for you.

The copiers should have a marking that shows up on all copied documents or the use of check paper. An alternative is to etch the glass on the copiers, so a mark appears on all copied documents. The copiers can also be configured to add a date and time stamp to the copy. These steps will allow document control to see if the document being returned is the original or a copy.

The system should maintain a log of who printed the document, how many printed copies, the control number of each document, and when it is due back to document control or if it has been reassigned to another control number. If barcodes or QR codes are used rather than printed numbers, more information can be stored and retrieved when scanned into the document system. Scanning technology can be used to read the control number for reconciliation purposes to verify all pages have been returned. Additionally, the scanned document can be verified as an original versus a copy.

Document Control Challenge

The findings in the 483 could have been prevented. It was not only a software issue; it was a document use issue and the lack of following good documentation practices. No system can solve all your process problems no matter how the vendor configures or customizes your system. Individuals need to be responsible for their actions and follow documented procedures for controlling hard copy documents.

No matter what system you have implemented, you must have a policy in place to manage the hard copy documents. It must address the regulatory requirements and good documentation practices. Employees should be trained on their regulatory responsibility of using uncontrolled documents, controlled documents, and how to handle unused or partially completed documents.

Automating the process to eliminate the forms may be your best option. Work with your vendor to see how they can help you with this process. It will help prevent your organization from having a paper process problem and provide an electronic means to capture and analyze the data real time. A future paper will discuss automating a business process using a business process management (BPM) platform and why companies should move from a document centric to a content centric platform for all documentation and content.

About the Author

Kevin Bogert is currently a Managing Member of Azimuth Compliance Consulting, LLC.
He has more than 35 years of business experience, 30 of them in the life science industry, where he has been involved in global implementations of quality and regulatory systems. His background includes statistics, quality and regulatory systems, computer and process validation, and automation of manufacturing processes. You can reach Kevin by e-mail at kbogert@azimuthcc.com or by phone at (215) 990-9123.

[1] U.S. Food and Drug Administration. Office of Pharmaceutical Quality and the Office of Compliance in the Center for Drug Evaluation and Research. Data Integrity and Compliance With Drug CGMP Questions and Answers Guidance for Industry, December 2018.

[2] Ibid.