http://www.pharmamanufacturing.com/articles/2011/087/?show=all

Ensuring Data Integrity

21 CFR Part 11 might really be called the Data Integrity Act. Here is a high-level look at what is needed to ensure compliance.

By John Avellanet, Cerulean Associates, LLC
Jun 08, 2011

Editor's Note: *This article is adapted from a presentation that Mr. Avellanet made in a webcast on April 7, 2011. This program is available here.*

Data integrity is critical to regulatory compliance, and the fundamental reason for 21 CFR Part 11. This article outlines and summarizes strategies and requirements.
First you must understand what FDA requires in terms of data integrity, and what the real-world costs are, whether you are taking proactive or reactive steps. FDA uses the acronym ALCOA to define its expectations of electronic data. The "l" originally stood for legible, which dates back to the time when FDA was dealing with scanned documents. I've updated it to "long lasting."

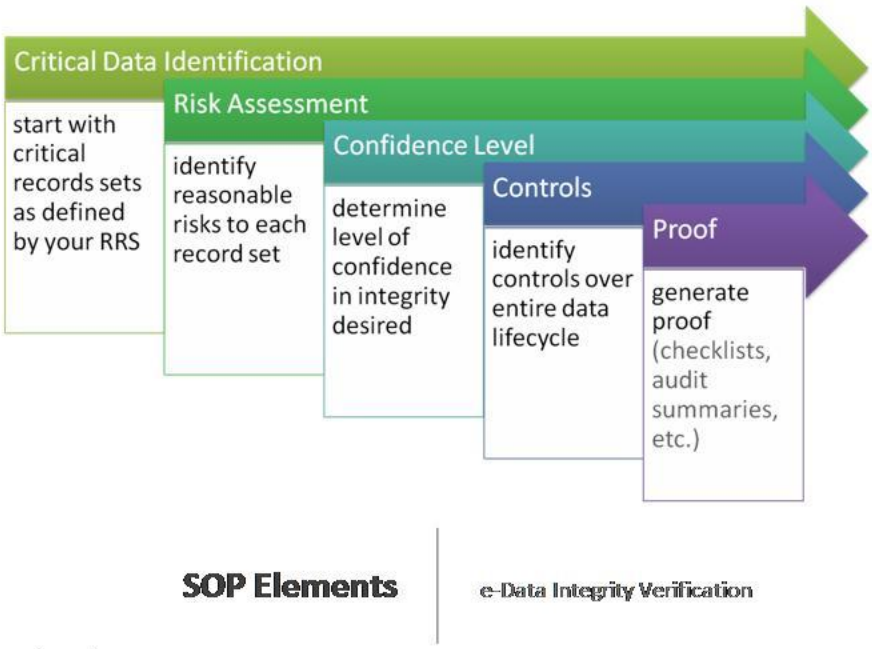
Attributable
Long-lasting (legible)
Contemporaneous
Original
Accurate

In addition, this is the definition of data integrity that FDA uses for internal training: "Data are of high quality if they are fit for their intended uses in operations, decision-making and planning . . . as data volume increases, the question of internal consistency within data becomes paramount…."

Following are the regulations that are critical to pharma and biopharma manufacturing.

• 21 CFR 11
• 21 CFR 58
• 21 CFR 201
• 21 CFR 202 & 203
• 21 CFR 210
• 21 CFR 211
• 21 CFR 600 (biologics only)
• 21 CFR 601 (biologics only)
• 21 CFR 610 (biologics only)
• 21 CFR 820 (combo devices only)
• 21 CFR 803 (combo devices only)
• 21 CFR 806 (combo devices only)
• Application Integrity Policy (AIP)

The Application Integrity Policy is what FDA pulls up when it has questions about a manufacturer's electronic data. Note that electronic information includes everything, such as emails, adverse events reports, complaints, batch records, quality control records—everything that's stored electronically.



When FDA invokes the AIP, the Agency is, in effect, saying, "We have concerns. We want to review everything this company has submitted, whether an additional application request, or request for a change in manufacturing." If FDA invokes this policy, you can expect an inspection. Not only will you have an inspection, but that inspection will focus closely on how you are controlling electronic records—i.e., it will focus on Part 11.

What Warning Letters Tell Us

Some excerpts from FDA Warning Letters from a few years ago provide a better understanding of what the Agency is driving at with data integrity.

• January 2008: "It was observed that the data stored on the computer can be deleted, removed, transferred, renamed or altered [without control]."

• April 2008: "There is no audit trail or log of data changes that are made to the information in the database. Data cannot be verified against source records, since such records are not maintained."

In such cases, data can't be verified because the original source records (e.g., certificate of analysis) have been scanned in and then thrown away. As a result, I have no way of knowing whether or not this is the original. Anyone can go into Adobe and change the record. Thus, FDA says, you have no tracking or controls on this, so we cannot rely on it.

Components | Mix procedural and automated controls

Below are excerpts from some more recent Warning Letters, from last year. Note the focus on record accuracy:

• May 2010: "Your firm failed to check the accuracy of the input to and output from the computer or related systems of formulas or other records or data and establish the degree and frequency of input/output verifications."

• April 2010: "Your firm's laboratory analysts have the ability to access and delete raw chromatographic data . . . Due to this unrestrictive access, there is no assurance that laboratory records and raw data are accurate and valid."

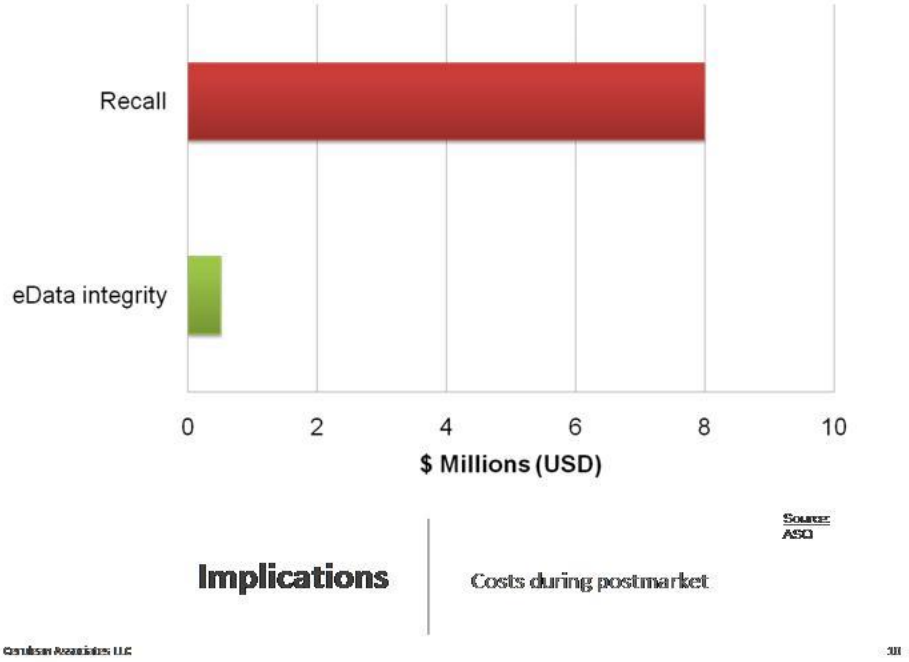
In the last example, FDA says there is no assurance of accuracy or validity. . . . The Agency has to stand in for the public, and cannot trust the data.

What the Agency is driving with Part 11 is the need for data to be trustworthy. Here are some of the questions that FDA inspectors are trained to ask about data control. They are all framed in common sense:

• Are original data entered directly into an electronic record at the time of collection or are data transcribed from paper records into an electronic record?
• Are there edit checks and data logic checks for acceptable ranges of values?
• How are the data secured in case of disasters, e.g., power failure? Are there contingency plans and backup files?
• Are there controls in place to prevent, detect, and mitigate effects of computer viruses on data and software?
• Are there records of critical computerized systems maintenance?
• Are there written procedures (SOPs and guidelines) to assure the integrity of safety and efficacy data?
• Are there records describing the names of authorized personnel, their titles, and a description of their access privileges to the data?
• How are the data transmitted from the firm to/from its suppliers?

Remember that Part 11 was introduced quite a while ago, before FDA could envision computing's limits.

Today, Apple's iPhone contains more computing power than all of the computers worldwide in 1990. Remember that regulators are not concerned with technology integrity, but rather record integrity.



Sitting in Storage

One of the most important things to understand is that we need to take a lifecycle approach to data integrity. Remember that adverse events records will have to be stored for 10 years, and batch records for seven or eight years. The key is to focus on the record.

Documents and e-data spend more than 80% of their lifespan in an archived (e.g., stored) state, according to ARMA [Authority on Managing Records and Information].

It's important to recognize that the records we've created and used are going to spend most of their lifetimes sitting in storage, with nobody looking at them. This is absolutely critical to understand, because if you don't build in controls to spot check those archived records, you may find that they're gone.

Carnegie Mellon studied data storage and found that, on average, two percent of data we store electronically literally vanishes—portions of hard drives are gone. Consider your CD's. After years pass, you'll see holes where data has evaporated . . . the key point to understand is that we have to build in controls.

You don't want to have to tell an FDA inspector that "you don't know" where the two percent of data went.

Following are some proactive and cross-functional best practices for ensuring data integrity.

• Form a cross-functional e-data working group
• Clearly define accountabilities vs. responsibilities
• Rely upon your records retention schedules
• Take advantage of and reuse IT controls
• Plan for at least one data migration during record lifecycle
• Incorporate e-data archive audits into internal quality audits
• Verify progress (and identify gaps) with a Part 11/Annex 11 mock FDA audit

Do not:

• Overlook the record lifecycle and focus on systems
• Rely on one-time validation of a system
• Assume e-data is “safe” in storage
• Turn it over to IT or to Validation or to Records Management
• Avoid tracking regulatory expectations in your regulatory intelligence program
• Forget that e-data is your proof of safety, efficacy, and compliance
• Lose sight of the costs–minimum 12:1 ROI

Remember that you need procedural controls. The following are the components of an effective data integrity SOP: Start with critical records sets, as defined by your RRS [record retention schedule]. Identify reasonable risks to each records set. Determine confidence level in integrity required. Set controls over the entire data lifecycle, then generate proof (checklists and audit summaries for instance).

Remember that the final SOP needs to fulfill FDA’s ALCOA acronym.

Here are other SOPs companies ask about. All of these might be things to consider, depending on how you manage data, who is involved, and how many people are involved. Obviously, the requirements for a 10-person virtual company will differ from those for a 5,000-person operation.

Additional SOPs should cover:

• Virtual Data Storage Verification (“cloud computing”)
• Secure Archived e-Data and Media Handling
• Data Maps–Creation and Maintenance
• Data Integrity/Controls Matrices–Creation and Maintenance
• Data Migration Protocols
• Data Transfers and Verification
• Maintaining Long-Term Confidentiality and/or Privacy
• Data Sampling and Archive Auditing
• Scanning of Paper Records for e-Data Archival
• Transfer and Retrieval of Long-Term e-Data Archives
• Secure Disposal of Clinical Patient & Adverse Event e-Data
• Qualification of Record and Data Storage Providers

Focus on FAQs

Below are questions that I am often asked. Each of these is very particular and the responses will be very specific to the company and context involved, but they are important to think about:

• What if we don’t have a records retention schedule?
• How much detail do we need in our data maps?
• Should we do a data-integrity/controls-matrix for each product or each system?
• Can we configure our network and computers for default data integrity?
• When can inspectors ask for system access?
• Do we have to keep all of our electronic raw data?
• How do we translate “data integrity” into budgets and projects?
• What are records that prove “safety and efficacy”?
• How do we document controls associated with records and personnel system usage?
• How best can we take advantage of IT, records and archival, quality management, and regulatory affairs?

It can be useful to take a very concrete “kick start” approach to ensure an effective Part 11 compliance approach within your organization.

1. Show sample enforcement actions that have cost and humiliated other firms.
2. Discuss how data integrity controls can limit risks and costs, with a focus on ROI.
3. Suggest next steps such as a management workshop to build momentum, talk to management and get a sponsor.