FDA 21 CFR Part 11 Revisited

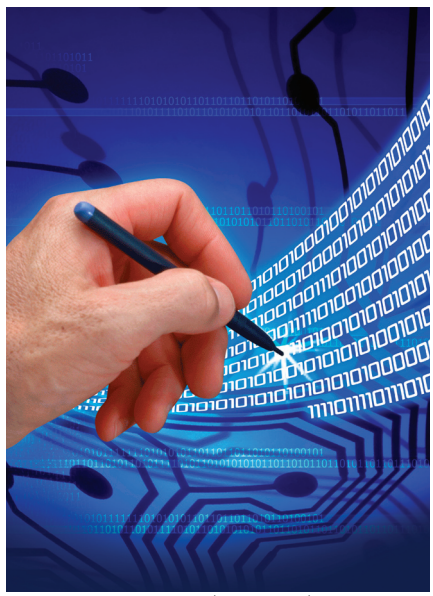
by John Avellanet

Six years after the US FDA applied a narrower scope to its interpretation of 21 CFR Part 11 on electronic records and signatures (1), the agency is ready to release the revised Part 11. The 2008 release of a draft revision of Annex 11 — Europe's version of Part 11 (2) — put pressure on the FDA to complete its long-overdue Part 11 revision.

As I made clear to members of my SmarterCompliance executive advisory group in May of last year, the agency's focus has shifted away from computer validation to electronic record integrity, including long-term information integrity and data quality. Last autumn, I was talking with FDA officials in preparation for my seminar on the specific revisions to Part 11 and Annex 11 (3), and it became clear that the revision group's work was complete. As of this writing, the revised regulation only awaits final center approval before being published. Given the recent changes in the US presidential administration, Congress, and FDA leadership, I anticipate the revised Part 11 to be released sometime later this year. For pharmaceutical, biotech, and medical device executives weary of the old "validate everything" mantra, the revised Part 11 should bring welcome relief.

Record Integrity

To understand the advantages of the revised Part 11, consider a 2003 study by the University of California-Berkeley's School of Information Management supplemented by insights from the US National Science Foundation (4). Berkeley researchers (and their NSF colleagues) calculated that for every piece of information available in front of you, there are an estimated 10 pieces of related information (rough drafts, notes, raw data, copies, various versions, and so on) stored elsewhere. So for every document or dataset included in your new drug application (NDA) to the FDA, there are 10 related documents or datasets not included.



ERKIN SAHIN (WWW.SXC.HU)

The vast majority of this excluded information is made up of items such as rough drafts archived on tape, original raw data files captured from laboratory machines, copies of certain forms, meeting minutes with personal notes written on them, and so on. But the agency would be shirking its duty to safeguard the public by merely taking your word for it that your application has just the right information included (that it and its supporting data have integrity). The complexity of different types of electronic information combined with today's technology has been a stumbling block for agency officials who expect no meaningful difference in integrity between an application submitted with ink and paper and one submitted electronically. Information submitted must have integrity (it must be complete, accurate, and attributable) for FDA officials to be able to rely upon it in making their decisions.

The NDA is just an example. This logic carries forth into all your records, not just those seen by agency reviewers and inspectors. All information you use to make decisions potentially affecting your product's safety, efficacy, and/or quality (and your level of regulatory compliance) must be accurate, complete, and attributable. So any product data captured electronically or stored electronically must have the same integrity as it would if the same information were created and stored on paper. That's simple enough to verify the day the information is created, but what about when you go back to look at it next year — or six years from now? Will production data you captured today still be accurate, complete, and attributable in 10 years? If you captured it on paper, then stored it appropriately, the answer would be an unequivocal "yes." But what about data stored, for example, in a Microsoft Word file?

Validate Everything? This is where the misinterpretations of Part 11 so

often kicked in. If the issue is whether data will have integrity stored in whatever software application or computer system, then we need to validate that software or that computer. After all, today's technology is a complex automated process that needs to be validated — or so ran the "validate everything" reasoning.

Technology is a tool, a means to an end. And your end is not a validated computer; it's a safe, efficacious, high-quality medicine. Were we to apply the technology-focused misinterpretation above to building a house, we would conclude that we can only build a solid, dependable, high-quality house by validating the electric screwdriver, nail gun, and drills involved. And if that were the case — that safe, effective, high-quality houses can be built only using validated electric tools — then Amish builders with their simple wood tools would not be as respected as they are.

If validating a computer, program, or other technology tool per se to achieve Part 11 compliance and data quality is not the answer, then what should you do? The real solution lies in moving away from a spotlight on individual technology tools toward a focus on controlling their output. For the FDA, that output is an electronic record that is "attributable, legible, contemporaneous, original, and accurate" (**5**). As I demonstrated to those attending my seminar, that is precisely how the agency has been enforcing Part 11 in warning letters and 483s over the past 18 months.

What to Expect

So what does the new focus on record integrity and data quality mean in the day-to-day business world of projects and resource allocations? Or, to paraphrase the words of one of my chief information officer (CIO) clients, how do you budget for record integrity?

To get there, begin by taking the first step: understanding some key differences between the original and revised versions of Part 11. While I went over details in last year's seminar, "Understanding and Implementing the Revised FDA Part 11 and EU Annex 11" (a recorded version is available at www.ceruleanllc.com), three of the most promising differences I found will help you get started: discretionary audit trails, risk-based security, and the elimination of "open" and "closed" systems.

"Open" and "Closed" Systems: One of the more confusing aspects of the original Part 11 (and its misinterpretations) was the concept of "open" and "closed" computer systems. The simplest way to conceive of the difference was that a *closed* system had little to no input from anyone but the person sitting at the keyboard — no Internet, no wireless access, nothing but a keyboard and a power cord. Anything else was considered an *open* system.

The need to identify different rules for closed and open systems was viable in the early 1990s when Part 11 was first discussed (many of us clearly remember the days before widespread Internet access, before wireless networking, and so on). In the 21st century, however, closed systems are largely nonexistent. Indeed, at one conference several years back, a member of the Part 11 revision committee commented, "The only truly closed system I know of today sits in a dark closet, unplugged, gathering dust."

Discretionary Audit Trails: Under the original Part 11, automated audit trails seemed to be required virtually everywhere. Whether all that logging and tracking actually added to anything beyond cost and overhead was always questionable, and the revised Part 11 tackles that question head-on. Deciding whether an audit trail is needed for your electronic information — much less whether it should be automated or manual — needs to be based firmly on documented risk assessments. This new reliance on risk management and ability to use manual logs rather than automated auditing should cheer all executives facing tightened budgets.

Risk-Based Security: Another welcome revised Part 11 change will be the shift away from prescriptive security and controls toward reliance on risk management and industry security standards. Many not-for-profit and nonprofit organizations offer recommendations of security for the risks you face with your electronic information, product safety, quality, efficacy, or level of compliance. Three of the most widely known are Common Criteria (www.commoncriteria.org), the International Organization for Standards (www.iso.org), and the US National Institute of Standards and Technology's Information Technology Laboratory (www.crsc.nist.gov).

Getting Prepared

There are still no "silver bullets" for Part 11 compliance. If anything, the shift in emphasis from technology to record integrity will limit your ability to buy off-the-shelf compliance or outsource your responsibilities. Your records and your data are in your control far more than the automation involved in a computer system or software application. The implication is that anyone can comply if they get the right direction from a credible source at a reasonable price.

When I was CIO for a combination medical device and biotech company, I spent a lot of money learning lessons from my many mistakes. Now when I advise executives in my SmarterCompliance program, I'm very careful about where I suggest they spend money on computer validation and record integrity. To help you avoid making some of the same mistakes I made, here is some of the advice I offered program members back in 2007 and 2008 on preparing for the revised Part 11.

Know-How: Assess your current information technology (IT/ICT) compliance advisors and validation consultants in light of their familiarity with the FDA's expectations regarding data quality and records integrity. Keep in mind that the old Part 11 used the word *integrity* more than 50 times. Insistence on validating computer tools as the means to achieve long-term data quality and records integrity will only place you squarely back in the old 20th-century misinterpretations.

STEVE WOODS (WWW.SXC.HU)

Research: Review the original Part 11 from 1997 (**1**), the FDA guidance on computerized systems used in clinical investigations (**6**), the European Union's drafted Annex 11 revisions, and associated Chapter 4 revisions of the European GMPs (**7**). Highlight each mention of *record* or *records, data integrity* or *quality, risk-assessment* and other such relevant terms. For the purpose of your analysis, replace the words *computer* and *software* with *tools* (or *equipment* if you're used to a manufacturing environment). This should give you a good idea of where the revised Part 11 will end up as well as a tentative checklist of what you need to examine for compliance.

Outsourcing: For contracts, quality agreements, technical agreements, or other addendums with contract research organizations (CROs), contract manufacturing organizations (CMOs), clinical sites, IT/ICT outsourced suppliers, data backup and records archival vendors, and so forth (any other company besides yours that either creates or stores information on your behalf), include the ability to conduct independent verifications of their controls and access to your records (both electronic and paper). Information is most vulnerable in storage, whether it is written in a laboratory notebook, saved on a flash- or hard-drive, backed up on tape, or burned onto a CD or DVD. Either ask outsourcing suppliers to provide you either a certificate of compliance from an independent auditor that conducts Part 11 or Annex 11 audits, or conduct an audit yourself.

Back-Up: You can quickly vet independent auditors or consultants by asking five simple questions: How many times does Part 11 mention integrity? How long do "burned" CDs last compared with "pressed" or manufactured CDs? Why? How can you recognize a degraded CD on sight alone (simply by holding it in your hand and looking at it with the naked eye)? And what is the typical failure rate of data backup and archival tapes (assuming appropriate storage)?

Each of those questions can be answered only through experience, often painful experience. Last March, when I gave a speech in Washington, DC on records management for small companies, one attendee was the president of a data backup company in northern Virginia. He vociferously protested the last question while all the attendees were present — but then after the talk, he came up and apologized. "I recognized several of my clients in the audience," he said, "and I couldn't let them think they had anything to worry about. But I've already called my head technician, and we're going to conduct a full test on every single tape we have starting tomorrow morning. I need to figure out our current risks."

If you want more advice on finding and choosing an independent consultant appropriate for you and your organization, I wrote a popular article last year based on my own experiences as a company executive trying to find good consultants and outsourcing providers (**8**).

A Holistic Approach: The Part 11 shift to records integrity and data quality will require you to blend the traditionally disparate disciplines of IT/ICT and records management. The IT/ICT folks (along with any validation consultants) can handle the technical aspects, but records-management experts will be needed to address long-term record integrity, quality control, and retention. Quality assurance also must be involved as "experts" on the personnel, product, and process aspects. Just as you need architects, builders, and tools to construct a house, so do you need this triumvirate of quality, records management, and IT/ICT to achieve validated systems that ensure electronic record integrity and data quality. The revised Part 11 takes a holistic, risk-based approach in which the technology tools, the quality processes, and the people involved are the underlying system. Your goal is information integrity. Who from your company needs to be involved to ensure that every record you create today is still just as accurate, attributable, and complete 10 years from now (when you're ready to submit that NDA)?

The FDA has taken all the industry complaints to heart and tried to put aside those previous misinterpretations about validating isolated technology tools. The revised Part 11 is all about records integrity and data quality so that both industry and the agency can reliably use information to make good decisions about product safety, efficacy, and quality (as well as regulatory compliance). If you are not comfortable with exactly what to do and how to go about it, then work with an independent consultant who has experience with both Part 11 and records management. Ask him or her to help you craft a revised Part 11 strategy for your company along with a set of audits and checklists you can use both internally to audit compliance and externally to qualify suppliers and partners that create or hold information on your behalf.

Start Now

If you need a more detailed roadmap and a multiple-page checklist for complying with the revised Part 11, you can find them (along with additional reference materials) in my revised Part 11 recorded seminar online at www.ceruleanllc.com. You can also download half a dozen articles and case studies from the site's resource library to help further prioritize tactics and budget activities for Part 11 and records integrity compliance.

No executive has ever been in trouble with the FDA because of computer tool problems or sloppy computer software coding. Several executives and business

owners, however, have bowed their heads in resigned frustration as inspectors detailed their lack of controls over records and data quality for proving product safety, efficacy, and quality. In our 21st-century knowledge-driven economy, if you expect to rely upon electronic records, then focus on controlling them.

Reference

1 Electronic Records, Electronic Signatures. *Code of Federal Regulations,* Title 21, Chapter 1, Subchapter A, Part 11. US Food and Drug Administration: Rockville, MD, 20 March 1997.

2 Directive 2003/94/EC. Annex 11: Computerized Systems. *EudraLex, Volume 4.* European Commission: Brussels, Belgium, 2003; ec.europa.eu/enterprise/pharmaceuticals/eudralex/vol-4/pdfs-en/anx11en.pdf.

3 Avellanet J. *Understanding and Implementing the Revised FDA Part 11 and EU Annex 11.* Cerulean Associates: Williamsburg, VA, September 2008. www.ceruleanllc.com/Seminars/eSeminar203131.htm.

4 Lyman P, Varian H. *How Much Information?* University of California at Berkeley, School of Information Management and Systems: Berkeley, CA, October 2003.

5 Wilson S. FDA Regulatory Perspective: Data Integrity. NIH Roadmap Program, Fourth Steering Committee Meeting: *Feasibility of Integrating & Expanding Clinical Research Networks.* US FDA Center for Drug Evaluation and Research: Rockville, MD, May 2006.

6 CDER. *Guidance for Industry: Computerized Systems Used in Clinical Investigations.* US Food and Drug Administration: Rockville, MD, May 2007; www.fda.gov/cder/guidance/7359fnl.htm.

7 Directive 2003/94/EC. Annex 11: Computerized Systems. *EudraLex, Volume 4.* European Commission: Brussels, Belgium, 2003; http://ec.europa.eu/enterprise/pharmaceuticals/pharmacos/docs/doc2008/2008_04/gmp_chap_4_consult_200804.pdf.

8 Avellanet J. Getting the Results You Expect from Consultants. *BioPharm Int.* 21(4) 2008: 32–36; www.ceruleanllc.com/resources/choose_a_consultant_get_results.htm.

John Avellanet *is managing director of Cerulean Associates LLC, PO Box 498, Williamsburg, VA 23187-0498; 1-757-645-2864, fax 1-877-322-5701; john@ceruleanllc.com; www.ceruleanllc.com.*