How FDA will enforce 21 CFR part 11

The FDA announced on July 8, 2010 that it will be "… conducting a series of inspections in an effort to evaluate industry's compliance and understanding of Part 11 in light of the enforcement discretion described in the August 2003 'Part 11, Electronic Records; Electronic Signatures — Scope and Application' guidance…." So … 13 years after promulgating the regulation and seven years after moderating their enforcement model – by exercising enforcement discretion regarding selected aspects of the regulation – the agency is still not comfortable about ***something***. What can it be? While we cannot speak on the agency's behalf, the words "in light of the enforcement discretion" imply to us that the agency is looking to 1) understand the disparate risk-based approaches taken by companies with respect to validation, audit trails, legacy systems, copies of records and record retention, and 2) determine how effective these approaches have been in establishing and maintaining data integrity (i.e., data completeness, accuracy and validity). Perhaps FDA will revise the regulation and/or issue new guidance that will reflect its ideas of what it perceives as the "best of breed" in terms of activities that most effectively and efficiently result in compliance with 21 CFR part 11. Who knows?

We choose to focus our thoughts regarding this FDA's initiative on data integrity because it is one of the main points that the FDA focuses on during its inspections. And it is because anything that calls data integrity into question will result in regulatory observations which, to date, have mainly been based on the predicate regulations that were put in place to promote data integrity. Therefore, enforcement discretion notwithstanding, we feel that companies will have to demonstrate the following basic quality measures to the agency: 1) all computerized systems that support regulated activities can be relied upon to operate as intended and identify all instances of incomplete, inaccurate and/or invalid data; 2) all regulated activities (e.g., changes to clinical data) can be reconstructed; and, 3) all regulated records (e.g., study data, manufacturing data) are available from the start of the respective process to the date of inspection and can be retrieved in a timely fashion. The way to do it would be to have complete, easy to follow and easy to explain documentation in support of the above-listed items; anything less may give the agency the perception that data integrity issues exist even if such may not be the case.

Listed below are some, but certainly not all, documentation pitfalls to avoid in this context:

- Lack of validation documentation that focuses on systems risks (e.g., nature and complexity of interfaces, number of bug fixes) in establishing the testing strategy (e.g., nature and scope of regression testing)
- Lack of challenges to the computerized system in the area of identifying incomplete, inaccurate and/or invalid data
- In a complex database system, lack of details regarding what tables, records, etc., constitute the audit trail
- Lack of policies, and/or documented confirmation of compliance to processes regarding ensuring the retention, continued availability and easy retrieval of regulated records/data
- Lack of a complete and/or accurate record of what changes were implemented to computerized systems that support regulated activities and how they were tested and documented
- Lack of documentation regarding training of personnel who were involved with system development, validation, deployment and maintenance
- Lack of documentation regarding how compliance to 21 CFR part 11 is actually achieved (e.g., confirming required functionality through testing, confirming

compliance to procedures, such as logical security, backup and recovery, through the internal audit program).

The bottom line is that documentation must stand on its own. Given that FDA may look at processes and records from several years ago and that staff who implemented computerized applications may no longer be around, it becomes imperative that you do what you must to ensure that all of your documentation for computerized applications is such that it does not raise data integrity-related questions that cannot be addressed in a timely fashion.