



Data Integrity in the FDA-Regulated Laboratory

By Jacqueline McCulloch, RAC, Courtney Woodson and Blake Long

To assure the quality of raw materials, in process materials and finished goods, laboratory data integrity is assuming greater importance in current Good Manufacturing Practices (CGMP) for US Food and Drug Administration (FDA)-regulated industry. Data integrity and security infractions are not only 21 Code of Federal Regulations (CFR) Part 11 issues but also severe CGMP violations. The reasoning behind this complex issue is quite simple: if the integrity of laboratory data is compromised, batches of finished goods may not comply with regulatory authorization terms and, consequently, will not be released for sale. As FDA increases its focus on data integrity and reliability, inspectors are examining data based on multiple regulations and standards including CGMP, Good Laboratory Practices (GLP), Good Clinical Practices (GCP) and the Application Integrity Policy (AIP) in addition to FDA-recognized consensus standards.

This article discusses data integrity regulations and enforcement trends that have led to increased scrutiny of pharmaceutical and certain medical device laboratories by inspectors.

What is Data Integrity?

Data integrity is the assurance that data records are accurate, complete, intact and maintained within their original context, including their relationship to other data records. This definition applies to data recorded in electronic and paper formats or a hybrid of both. A good way to understand data integrity is through an analogy from the legal world. A data record is similar to a contract. A contract is valid only if all the pages of the document are complete and legible, contain the required, authentic signatures and properly state the terms and conditions. In this sense, integrity denotes validity.

Ensuring data integrity means protecting original data from accidental or intentional modification, falsification or even deletion, which is the key to reliable and trustworthy records that will withstand scrutiny during regulatory inspections. According to FDA, which

uses the acronym ALCOA, data need to be “attributable, legible, contemporaneous, original, and accurate.”

Data Integrity Regulations

FDA inspects for electronic data integrity during the pre- and postmarket product approval process under 21 CFR Part 11, which is commonly referred to as the “data integrity regulation.” When FDA published its intent to raise the enforcement profile of 21 CFR 11 (Part 11) in 2010, it listed four goals:¹

1. Assess the industry’s comprehension or continuing misinterpretations of Part 11.
2. Determine how firms are ensuring the integrity of electronic records.
3. Extend scrutiny of data, quality-related and computerized system validation-related Form 483 inspectional observations since 2007.
4. Determine next steps for Part 11, including whether to issue a revised regulation or simply draft more guidance.

History of Enforcement Trends

There has been a focus on the integrity of data generated in regulated quality control laboratories since the Able Laboratories^{2,3} and Leiner Health Products^{4,5} fraud cases took place in 2005 and 2006, respectively. The major compliance problem in the Able Laboratories case stemmed from the fact that paper copies of records differed, sometimes radically, from the electronic records contained within a chromatography data system. FDA revealed its drastic enforcement action was the result of massive record falsification and mismanagement by Able in an effort to avoid detection of several defective medications. These non-compliant acts ultimately led the company to file for bankruptcy protection in July 2005.

The Leiner Health Products 2007 Warning Letter stated “inspections found many serious deviations, some of which involved data manipulation and inadequate testing procedures.” A year-long federal investigation into the company’s production and distribution facility followed as part of an arrangement with the Department of Justice (DOJ), under which the company pleaded guilty to one count of mail fraud. The guilty plea stemmed from a December 2006 incident in which quality control officials “gave false appearance” that a batch of drugs had passed quality tests and “allowed the nonconforming drugs to be shipped to a customer.” This probe by FDA led to product recalls and layoffs. In addition, the company was ordered to pay a \$10 million fine and eventually filed for bankruptcy protection in March 2008.

In 2008, regulators uncovered a list of issues, including faked drug quality data, and banned 30 products from the US market. In 2009, FDA took enforcement action against Ranbaxy, India’s largest manufacturer of generic drugs, including its US-based subsidiary, Ohm Laboratories. DOJ, on behalf of FDA, filed a consent decree of permanent injunction against Ranbaxy.⁶ The consent decree required that Ranbaxy comply with detailed data integrity provisions before FDA would resume reviewing drug applications. Among other things, Ranbaxy was required to hire a completely independent outside auditor to serve as a data integrity expert and work with the company and FDA on internal audits. Ranbaxy brought in US consultants. The blueprint for that journey was laid out in the 55-page consent decree. The consent decree required Ranbaxy to hire both data integrity and manufacturing experts to watch operations, make recommendations and take up any issues noted with FDA. Subsequently, FDA withdrew approval of 27 Abbreviated New Drug Applications (ANDAs) held by Ranbaxy.⁷ DOJ announced a “groundbreaking” settlement on 13 May 2013 that requires the Indian drug maker to make “fundamental changes” to plants in the US and India.⁸ Since the original consent decree was signed in January 2012, it has been extended to cover four more plants that recently underwent a CGMP inspection.^{9,10} As part of the result of the consent decree, Ranbaxy chose to decommission its Gloversville, NY, facility rather than remediate it because the plant was scrutinized by US authorities for violation of regulatory norms and operating at “sub-optimal level.”

Ranbaxy is facing liquidated damages provisions to cover many potential violations of the law.

These are not the only cases of data integrity violations. In the last three years alone, FDA has issued more than 30 Warning Letters and Form 483 inspectional observations

“Data integrity problems break trust. In the time between inspections, we trust you to do the right thing. And if we finish an inspection and that trust has been broken, then we need to go through a few exercises to build that trust [again] before we can go forward and trust you until the next inspection.”

—FDA Center for Drug Evaluation and Research (CDER) Office of Compliance Senior Policy Advisor Karen Takahashi

related to electronic records. An uptick in the number of data integrity problems FDA is finding at manufacturing and testing facilities has prompted the drug compliance office to better define the forms in which these integrity problems can appear and the red flags that will trigger more-intensive investigations.¹¹

Overview of Data Integrity-Related Regulatory Programs

In 2009, FDA started the Post-Inspection Responses Program, which concerns the handling of FDA Form 483s. This program requires a complete response to all 483 inspectional observations within 15 business days. This should prompt a redefinition of inspection-ready, so laboratories are working compliantly and do not need to panic when facing the 15-day deadline. However, as evidenced by ongoing data integrity issues, this is not happening in a number of laboratories.

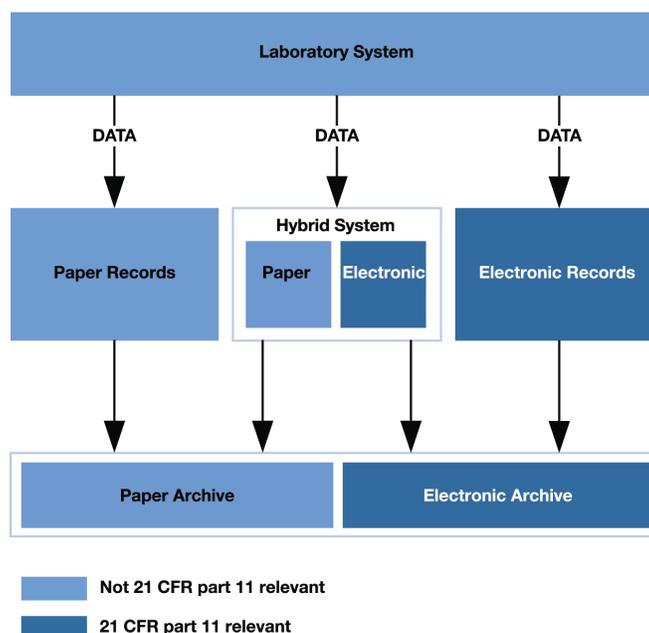
FDA announced in 2010 that it would be conducting Part 11 audits alongside normal CGMP inspections to assess how industry is interpreting 21 CFR 11. According to FDA's Pre-Approval Inspection Program 7346.832,¹² the FDA inspector has to "audit the raw data, hard copy or electronic, to authenticate the data submitted in the [Chemistry, Manufacturing and Controls] CMC section of the application, and to verify that all relevant data (e.g., stability, biobatch data) were submitted in the CMC section such that CDER product reviewers can rely on the submitted data as complete and accurate."

Following FDA's lead, the EU has published similar regulations relating to data integrity. The EU regulations were released in January 2011 and became effective on 30 June 2011. At first sight, the focus should be on the increased requirements for computerized systems regulation in Annex 11. The new version of EU GMP Chapter 4, published in January 2011 and effective 30 June 2011, requires that the raw data for batch release is defined for both homogeneous and hybrid systems. The new records retention requirements in EU GMP Chapter 4 state that if the records are supporting a Marketing Authorisation (MA), then the records have to be maintained, including the data integrity for as long as the MA is in force. The recently published EU GMP Annex for computerized systems 11, effective 30 June 2011, has several sections dealing with data integrity.

Challenges of Maintaining Laboratory Data Integrity

The first challenge in ensuring the integrity of laboratory data involves utilization of hybrid systems (see **Figure 1**). If both are used, paper and electronic records need to be synchronized.

Figure 1. Data Handling Alternatives



Computerized systems add a second challenge to laboratory data integrity due to the potential for electronic data manipulation. Such manipulation can include human errors when data are entered by mistake or intentionally falsified, and selection of good or passing results to the exclusion of those that are poor or failing.

One example of how to overcome some of the challenges of managing data integrity is in the manual entry of critical data. After manual entry of the critical data is complete, a verification of the data entry can be performed by a second person or can be verified with the use of a validated computerized verification process.

The third challenge comes from system interfaces. If interfaces are used to transfer data from instrument to system or between systems, such as between the chromatography data system (CDS) and laboratory information management system (LIMS), the probability of data integrity issues due to human error is decreased but the validation burden and effort to maintain a validated state are higher due to the increased amount of validation testing needed when transferring data from one computer system to another.

Ensuring Data Integrity in the FDA-Regulated Laboratory With AIQ and CSV

Demonstrating the integrity and security of laboratory data, records, results and information is paramount for a successful audit or inspection for any Good Pharmaceutical Practices (GxP)-regulated laboratory. Laboratory best practices for meeting regulatory and compendial requirements are changing to meet FDA's emerging expectations for data integrity. Analytical instrumentation used within GxP analytical laboratories is computerized either via firmware inside the instrument or via software installed on a workstation situated next to the instrument. All analytical instruments must be qualified and computerized systems validated.

The current regulatory guidance regarding the qualification of analytical instrumentation and validation of computerized systems is conflicting; qualification and validation are typically considered separate activities with little, if any, interaction between the two disciplines. The American Association of Pharmaceutical Scientists (AAPS) produced guidance on analytical instrument qualification (AIQ) in the form of a white paper, which has been incorporated as General Chapter <1058> within the United States Pharmacopoeia (USP). This approach focuses on the instrument with little emphasis on computerized system validation. In contrast, the Good Automated Manufacturing Practice (GAMP) Good Practice Guide for Validation of Laboratory Computerized Systems from the International Society for Pharmaceutical Engineering (ISPE) looks exclusively at the computerized system and ignores instrument qualification. The major problem and practical reality are that a computerized system cannot be validated without qualifying the analytical instrument, and vice versa.

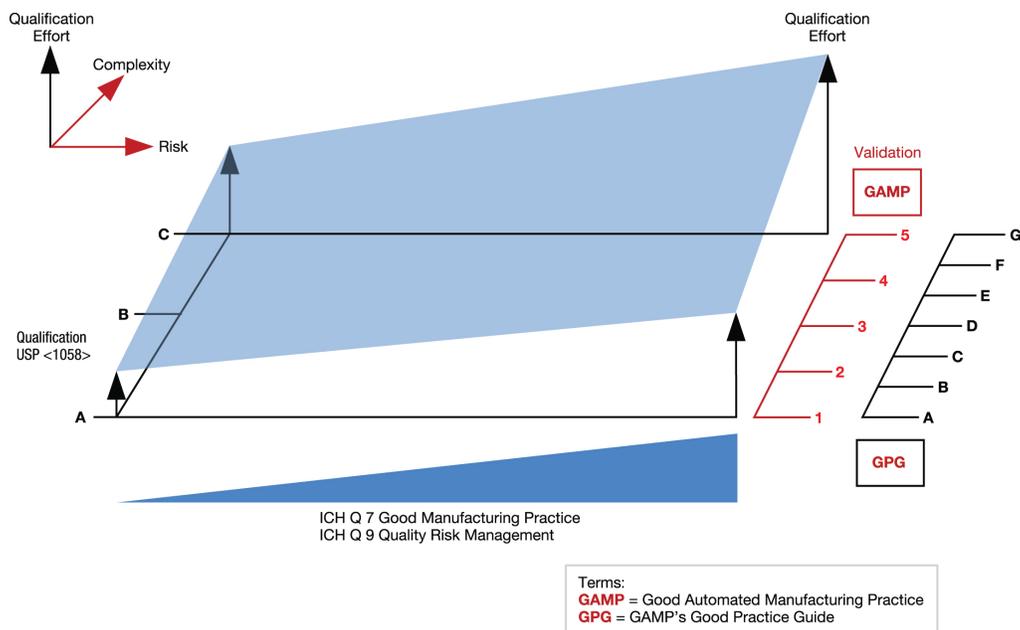
R&D Laboratories Not Exempt From Data Integrity Scrutiny

Research and development laboratories also have come under increased scrutiny within recent years as FDA and other global regulatory agencies attempt to oversee the pharmaceutical product lifecycle from early development to final product release more thoroughly. While regulations have been in place since the 1970s, historically, FDA has concentrated its review process on the manufacturing aspect of pharmaceutical products. This has changed with the added scrutiny on data integrity.

Research laboratories should recognize the importance of the following points, as they relate to generating data that will withstand FDA scrutiny.

- Resources—While resources also include personnel, particular attention should be paid to equipment and facilities. All testing equipment should have undergone a rigorous qualification process to ensure its suitability for the testing required. Also, a regular maintenance and calibration schedule should be set. All of these activities should be documented and recorded in logbooks or electronic systems dedicated to each instrument and activity. There should be physical accountability that laboratory samples, test samples, reagents, etc., are traceable. The life of the laboratory sample should be documented until final disposal, including all test samples and test portions.
- Characterization—Detailed records should be kept regarding characterization testing of any raw materials used in development and any intermediate process

Figure 2. Different Approaches of USP, GAMP, GPG and Application of ICH Risk-Based Considerations



steps. Records should include as much information as possible, such as raw material manufacturer and lot numbers, descriptions of the testing performed and any equipment used.

- **Protocols**—Protocols for both the studies and the testing involved should be established and followed consistently. These protocols facilitate reproducibility of test methods and data to strengthen the validity of generated data. A research laboratory lends itself to unexpected and out-of-trend results; therefore, procedures also should be established for handling non-trending data and deviations from the approved procedures.
- **Results and Record Retention**—Data should be recorded in a timely manner, ideally in real time, in bound notebooks or electronic systems. These data should be reviewed by personnel who are knowledgeable about the test performed and the results generated. A final study report should document the research testing outcome and interpretation of results and include specific commentary on any deviations that may have occurred during the course of the study. After the study's completion, all records should be archived safely yet be accessible should the need arise for regulatory review at a later date. The laboratory must have policies and procedures to ensure records are retained and protected in a manner that ensures activities are legally defensible.

Overcoming Data Integrity Challenges With Laboratory Automation and Technology

The integrity of laboratory data can be challenged, for example, by sources of variation inherent in the use of computerized systems, by intentional falsification or by accidental data loss or corruption. Historically, while several laboratories have a working LIMS, there is no universal, mandatory national information technology (IT) system, and few laboratories are truly “paperless.” Nonetheless, some common practices and tools for any laboratory computerized system to control such challenges include user rights administration, security tools, user access records, audit trails and records management. These must be monitored properly and controlled to ensure data integrity. Revision control is of particular importance for re-analyzed data. In addition, operational checks enforced by a computerized system can verify user permissions and enforce a certain sequence of permitted steps according to a defined workflow. The use of pre-defined workflows is also important so data cannot be entered out of context.

Some developers define “built-in” validation checkpoints within systems. Examples include:

- input pattern/mask that forces the user to enter data into a defined format
- checks for valid data entered by the user to avoid data type issues (classification identifying various types of data, such as real, integer or Boolean)
- drop-down lists for data selection wherever possible, instead of data entry by the user
- double entry checks to ensure key fields are not duplicated
- pop-up calendars for date input to avoid entering the incorrect date format

Strategy for Control of Data Integrity

A critical element of robust compliance, which supports value-driven analysis and a low-risk audit defense strategy, lies in understanding the interrelatedness among the laboratory compliance levels illustrated in **Figure 2**. All levels are fundamental parts of the laboratory quality system. Analytical instruments must be qualified to show they are working properly before any analytical methods are developed or validated using them. The analytical instruments also must be qualified before the computerized systems managing the resulting data are validated.

Following from *Guidance for Industry Part 11, Electronic Records; Electronic Signatures—Scope and Application*,¹³ the regulated company must identify all raw data associated with making CGMP decisions and determine the format (paper/electronic) in which the data will be maintained. If the raw data are to be maintained in electronic format, the integrity of the record must be assured.

Accreditation to the International Standard *ISO/IEC 17025: 2005 General Requirements for Competence of Testing and Calibration Laboratories* is an advantage to maintaining data integrity. The main difference between good analytical practices and accreditation is the amount of documentation produced. Although any good analytical laboratory uses qualified analysts, checks the performance of equipment used for testing and validates analytical methods, many times, the outcome of the tests is not fully documented. ISO/IEC 17025 accreditation requires formal documentation for nearly everything in the laboratory workflow.

Raw data produced by the laboratory equipment or computerized system must be reviewed periodically per companies’ procedures to ensure data validity and integrity. The raw data to be reviewed, as well as the related review task, must be defined in the system management definition or in a corresponding standard operating procedure (SOP).

Examples of raw data review requirements include:

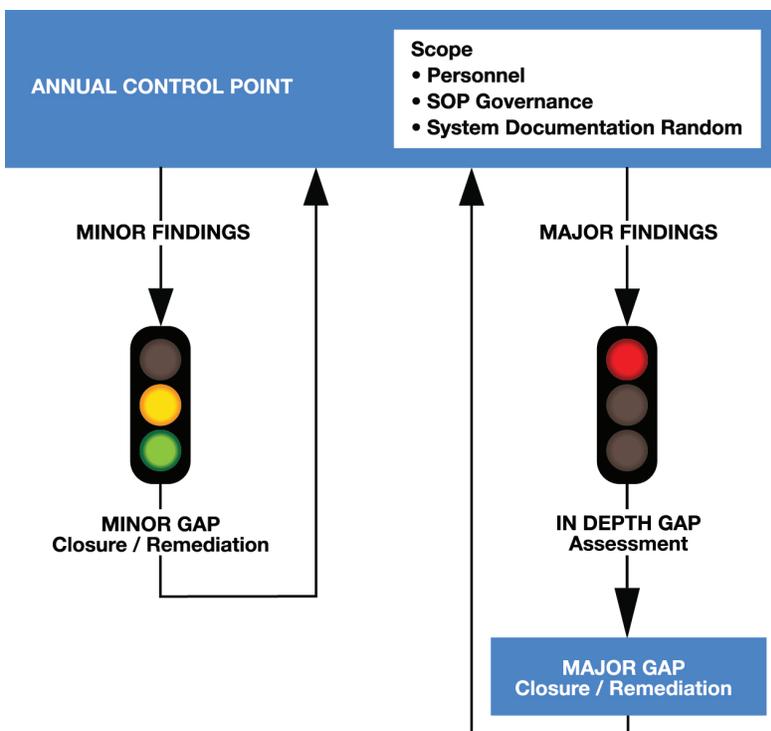
- Are raw data and corresponding records clearly and immutably linked?
- Is a date and time stamp provided with the data and is this clearly and immutably linked to the original condition?

The periodic review results, including any gaps identified and the corresponding remediation activities, must be documented. An annual assessment of laboratory procedural controls is best to ensure:

- compliance of laboratory personnel
- proper coverage and implementation of SOPs
- “real life” implementation of SOPs (verified through sample checks of system documentation)

Control points can be developed from system validation deliverables, in addition to system backup and restore, audit trail, electronic records and electronic signature and infrastructure requirements. Control points should be included in an annual assessment tool to determine the state of control (see **Figure 3**). The assessment structure should enable compliance with control points to be determined through reporting major and minor findings. It also should describe whether the system is fit for use with the possibility of minor gaps to be remediated, and whether remediation activities are to be implemented to close gaps resulting from major findings.

Figure 3. Annual Control Point Assessment



Additional Best Practices

Documenting everything and maintaining good records using good documentation practices are reminders that quality is the responsibility of each analyst and must be incorporated into every aspect of an analysis, including the paperwork. It is also important to establish, maintain and follow approved procedures and document results in records.

Conclusion

FDA-regulated laboratories are under intense scrutiny and data integrity enforcement actions are increasing due to violations in recent years. Ensuring data integrity is critical in both pre- and postmarketing approval activities.

Laboratories should document an overall data integrity approach by outlining informatics based on workflow. This approach can be set forth in a laboratory data integrity strategy. Operational and procedural control points should be monitored routinely and audited to identify any need for remediation and put the laboratory in the most defensible position.

References

1. FDA to conduct inspections focusing on 21 CFR Part 11 requirements relating to human drugs. FDA website. <http://www.fda.gov/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDER/ucm204012.htm>. Updated 5 December 2010. Accessed 1 March 2014.
2. FDA report accuses Able Laboratories of engaging in massive fraud to cover up defective medications. News Inferno website. <http://www.newsinferno.com/fda-report-accuses-able-laboratories-of-engaging-in-massive-fraud-to-cover-up-defective-medications>. Posted 13 July 2005. Accessed 1 March 2014.
3. Able Laboratories Inc., Cranberry, NJ, FDA 483 Inspectional Observations, dated 05/02-07/01/2005. FDA website. <http://www.fda.gov/aboutfda/centersoffices/officeofglobalregulatoryoperationsandpolicy/ora/oraelectronicreadingroom/ucm061813.htm>. Updated 13 August 2012. Accessed 1 March 2014.
4. Leiner Health Products, LLC 28-Aug-07. FDA website. <http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2007/ucm076485.htm>. Updated 8 December 2009. Accessed 3 March 2014.
5. "Leiner agrees to forfeit \$10M in mail-fraud case." *Charlotte Business Journal*. http://www.bizjournals.com/charlotte/stories/2008/05/12/daily16.html?st=s_cn_hl. Posted 12 May 2008. Accessed 3 March 2014.
6. U.S. Files Consent Decree for Permanent Injunction against Pharmaceutical Ranbaxy Laboratories [press release]. DOJ website. <http://www.justice.gov/opa/pr/2012/January/12-civ-105.html>. Issued 25 January 2012. Accessed 3 March 2014.
7. "US FDA removes 27 Ranbaxy ANDA approvals in consent decree." Pharmabiz website. <http://pharmabiz.com/NewsDetails.aspx?aid=70765&sid=2> Posted 22 August 2012. Accessed 3 March 2014.
8. Generic drug manufacturer Ranbaxy pleads guilty and agrees to pay \$500 Million to resolve false claims allegations, cGMP violations and false statements to the FDA. DOJ Web site. [press release]. USDJO website. <http://www.justice.gov/opa/pr/2013/May/13-civ-542.html>. Updated 13 May 2013. Accessed 3 March 2014.

9. FDA prohibits Ranbaxy's Toansa, India facility from producing and distributing drugs for the U.S. market [press release]. FDA website <http://www.fda.gov/newsevents/newsroom/pressannouncements/ucm382736.htm>. Issued 23 January 2014. Accessed 4 March 2014.
10. "Ranbaxy falls further into regulatory quagmire with latest FDA ban: Agency extends strict consent decree to fourth Ranbaxy facility." FiercePharma website. <http://www.fiercepharma.com/story/ranbaxy-falls-further-regulatory-quagmire-latest-fda-ban/2014-01-24> Updated 24 January 2014. Accessed 4 March 2014.
11. "Uptick in data integrity problems leads FDA to better define types and red flags. International Pharmaceutical Quality website." <http://www.ipqpubs.com/news/uptick-in-data-integrity-problems-leads-fda-to-better-define-types-and-red-flagsbb/>. Posted 16 May 2012. Accessed 4 March 2014.
12. Drug Compliance Programs. FDA website. <http://www.fda.gov/drugs/guidancecomplianceregulatoryinformation/ucm252671.htm> Updated 7 March 2014. Accessed 13 March 2014.
13. *Part 11, Electronic Records; Electronic Signatures—Scope and Application*. FDA website. <http://www.fda.gov/regulatoryinformation/guidances/ucm125067.htm>. Updated 15 January 2014. Accessed 13 March 2014.

About the Authors

Jacqueline McCulloch, RAC, is a senior consultant with Clarkston Consulting and has more than 25 years of experience working in quality systems compliance, regulatory submissions and strategy. **Courtney Woodson** is a senior consultant with Clarkston Consulting and has more than 10 years of information systems experience, with the last six years focused on leading technical projects for Life Sciences industry clients. **Blake Long** is a consultant with Clarkston Consulting and has more than 15 years' experience in R&D and clinical FDA regulated environments employing GxP practices.

Cite as: McCulloch J., Woodson C, Long B. "Data Integrity in the FDA-Regulated Laboratory." *Regulatory Focus*. April 2014. Regulatory Affairs Professionals Society.

© 2014 by the Regulatory Affairs Professionals Society. All rights reserved. Reprinted with the permission of RAPS.