DATA INTEGRITY and DATA MANAGEMENT for GXP REGULATED FIRMS

Barbara W. Unger
Unger Consulting Inc.

Regulatory agencies have cited deficiencies in GMP data integrity and data management for at least the past 15 years. Yet it appears that the industry as a whole has made limited progress in self identifying and remediating these deficiencies. Regulators continue to identify the same set of shortcomings including, but not limited to: shared passwords, lack of enabled audit trails, failure to review electronic data, failure to review and investigate all failed testing results and failure to contemporaneously record information just to name a few. Perhaps this is due to a lack of awareness regarding requirements for electronic records, or more likely, firms may assign all computer and software system responsibilities to the IT groups without engaging a knowledgeable Quality Unit and other stakeholders as active partners. Failure to integrate assessments of data management and data integrity into internal GMP audit programs perpetuates inadequate practices. Waiting for regulatory authorities to identify poor practices and procedures is never a sound idea.

In three blog entries I provide a structured look at the topic and include links to relevant documents and an extensive list of primary references with links. You will learn about the regulatory enforcement background and why we've arrived at the point where data integrity is such a significant focus; you will learn about the applicable regulations and guidance and the enforcement actions taken by global regulatory authorities in this area and you will learn what actions you can take within your own company to begin to address the topic and you will have links to the relevant references. This report includes the following divided as follows:

A. Introduction

Addressing the issue of data management and data integrity within the pharmaceutical industry can seem a daunting effort. Data management that ensures integrity of the associated data requires more than risk-based computer system validations. It requires understanding the events that precipitated this focus, understanding the intent of the governing regulations and guidance, and enforcement actions. This paper is written to remove some of the mystery from the topic and to provide readers a broad background on the topic of data management and data integrity and suggestions for how they might begin to address this issue within their company. The paper begins with a history for regulators focus on data integrity in GXP activities, and proceeds to identify the relevant global regulations and guidelines including those from FDA, EMA, MHRA, WHO, and PIC/S. Enforcement actions taken over the past ten-plus years are highlighted, and specific actions that firms might take are identified.

Data management and governance should be incorporated into a firms' Quality Management System. The Quality unit should be active in partnership with the IT functional area and provide appropriate partnering to ensure compliant solutions are put in place and managed thru their lifecycle. This should not be exclusively the responsibility of the IT department to implement and manage. Although high level processes and oversight is essential to an effective data management program, this is an area where every employee of the company has a role to play in documentation of laboratory results, completion of batch records and other record required by GxP rules.

Significant sections of the paper address QC Laboratory functions and FDA enforcement actions for two reasons:

1. The Quality Control Laboratory is currently the most common area in which to identify data management concerns, and
2. FDA publishes enforcement actions with greater granularity than other regulatory authorities. The reader should not, however, interpret this to mean that only FDA is applying enforcement actions.

Requirements for sound data management that ensure integrity of GxP data are recognized by major regulatory authorities and enforcement actions have been taken by most.

I begin by providing background for this regulatory enforcement focus to provide context for understanding today's actions.

B. Regulatory Enforcement Background

It is important to understand the history that gave rise to the current data management and data integrity focus by regulatory authorities. This focus represents an evolution over the past 30-plus years and addresses both changes in technology and learnings from GMP inspections. Assurance of data integrity is a component of the larger category of data management and applies equally to paper records and electronic records. So, let's begin with some history of how we reached this point.

The "generics scandal" of the 1980's raised the issue of falsified data submitted to FDA in support of drug approvals.[i] One outcome of this scandal was the shift in focus of the FDA pre-approval inspection (PAI) to evaluate raw laboratory data included in the marketing application and evaluate whether the site was capable of manufacture as described in the application. This scandal also prompted implementation of the *Application Integrity Policy* in 1991 which "*describes the Agency's approach regarding the review of applications that may be affected by wrongful acts that raise significant questions regarding data reliability*". Five firms are on the current CDER *Application Integrity Policy List* effective October 1, 2015.

In parallel, FDA recognized the increased reliance on computerized systems within the pharmaceutical industry. They developed and published *21 CFR Part 11*, the final rule on *Electronic Records and Electronic Signatures* in 1997. While the requirements for electronic signatures were reasonably well understood, confusion remained on both sides regarding the interpretation and enforcement of requirements for electronic records. In 2003 FDA published a *Guidance for Industry, Part 11, Electronic Records; Electronic Signatures –Scope and Application* to address enforcement priorities. FDA continues to communicate their interpretations in compliance actions such as forms 483 and warning letters, podium presentations and on their GMP Q&A web site page.

In light of these two events, the generic drug scandal and the rule on *Electronic Records and Electronic*

Signatures, the current warning letters and forms 483 that cite issues associated with data integrity should come as no surprise. As early as 2000, a warning letter issued to Schein Pharmaceuticals[ii] cited lack of control over computerized laboratory systems including lack of password control and broad ranging staff authority to change data. FDA issued a 15-page form 483 to Able Laboratories in New Jersey in 2005. Failing laboratory results were identified that were not reported, and among the observations was failure to review electronic data including audit trails. Warning letters citing deficiencies in the broad area of data integrity were issued to *Actavis Totowa LLC* site in the US, in 2007. Three warning letters were issued to two Ranbaxy sites in 2006 and 2008 HERE, HERE, and HERE.

Based on these compliance actions, FDA announced a pilot program in 2010 to evaluate data integrity as part of routine GMP inspections. FDA planned to use the information gained from these inspections to determine whether revisions to Part 11 or additional guidance on the topic were necessary. FDA also committed to take appropriate enforcement actions on issues identified during the inspections. The program is described in a *slide deck* presented by Robert Tollefsen at a variety of industry conferences in 2010. In the slide deck FDA stresses that they will "*continue to enforce all predicate rule requirements, including requirements for records and recordkeeping*." In fact, deficiencies in Part 11 are rarely, if ever, cited in warning letters citing data integrity deficiencies because almost all are failures to comply with the predicate rules.

FDA found the problems were widespread during this pilot evaluation, and enforcement actions in this area continue. With this background on the topic we now move to address the regulations and guidance published in this area.

C. Applicable Regulations and Guidance

An official definition of "data integrity" is not found in the regulations. FDA and other regulatory authorities expect that data will have attributes described in the acronym ALCOA. This acronym was first referenced in the September 2013 *Guidance for Industry, Electronic Source Data in Clinical Investigations* and addresses the attributes of clinical "source data." As applied to GMP, that means data are expected to be:

Accurate	Data must be accurate. Where appropriate, correctness should be 2nd person verified. This extends, for example, to data / information that are presented in multiple locations such as an equipment log, laboratory notebook, and electronic chromatography data where data should be in agreement.
Legible	Data and results must be legible / readable. Electronic data much also have the capability to be made human readable.
Contemporaneous	Thus, data are recorded at the time of the event / action, not transcribed at a later date. Data are not transcribed from post-it notes or scrap paper to the official documents such as batch records or laboratory notebooks.

Original	Original data are similar to "raw data". The following is taken from the MHRA guidance and appears to also represent FDA's opinion: "**Original record:** Data as the file or format in which it was originally generated, preserving the integrity (accuracy, completeness, content and meaning) of the record, e.g. original paper record of manual observation, or electronic raw data file from a computerized system." The paper print out of a chromatogram is no longer considered the official raw GMP data because it does not include the complete information, including but not limited to meta-data, audit trails, and system configuration for the analysis in question. FDA addresses this in their GMP Q&A.
Attributable	This term requires the ability to determine who collected the data, when it was collected, from which instrument it was collected and who made any data modification or data manipulations. For example, for HPLC chromatography, this includes all integration events. Use of shared passwords renders makes it impossible for the reviewer to attribute the data to a specific person.

Requirements meant to ensure data integrity preceded Part 11 and are found in 21 CFR 211 and in other parts of 21 CFR governing GxP areas. The two regulations that are most frequently cited in warning letters are 21 CFR 211.194 and 21 CFR 211.68[1]. These require maintenance of complete laboratory records and adequate controls over computer systems respectively. 21 CFR 211.188 is frequently cited and requires that production and control records shall include complete information in addition to 21 CFR 100(b) which requires that actions are documented at the time they are performed.

The first regulation that specifically addressed electronic records and electronic signatures became effective as 21 CFR Part 11 in 1997. Interpretation and enforcement of this new rule resulted in confusion among both FDA investigators and the regulated industry. In 2003 FDA published a guidance meant to clarify their interpretation. Current interpretation and actions that prompt enforcement may be found in FDA presentations given at industry symposia, Q&A on their web site, forms 483, and warning letters. These information is valuable to read because it will always have greater specificity than the text in regulations and guidance.

FDA is not unique in establishing and updating requirements and guidance regarding data management meant to ensure data integrity. EMA revised and expanded Annex 11 of their GMP Guide in 2011 to provide additional clarification for computer system requirements. This same annex was adopted by PIC/S. MHRA took the lead in the EMA region to identify and detail their requirements for data integrity. In December 2013 they *announced* that the pharmaceutical industry is expected to review data integrity during self-inspections. In January of 2015 they published a guidance document on the subject and a revised version of the *guidance* was published in March 2015.

MHRA defines terms commonly used in the data integrity area, and provides detailed examples of expectations. MHRA expects that a 'robust data governance' approach will ensure that data are complete, consistent and accurate, regardless of the format in which data is generated, used or retained. An important statement in the guidance is that manufacturers "…*are not expected to implement a forensic approach to data checking*…".

[1] *Unger Consulting Inc*. data, available upon request

The World Health Organization (WHO) recently published a 35-page draft document on their website, *Guidance on Good Data and Record Management Practices* for GXP regulated activities. This also addresses both paper records and electronic records. The guidance includes a detailed set of examples for each and seems closely aligned with the MHRA guidance from March 2015.

Armed with the knowledge of the background for data integrity, and understanding the regulations and guidance on the topic, we proceed to evaluate inspection observations and warning letters. Again, these are primarily FDA focused enforcement actions because FDA enforcement actions are most readily available.

D. Inspection Observations, Warning Letters, WHO Notices of Concern, and EU Inspections

As mentioned earlier, enforcement actions for deficiencies in data integrity span more than the past ten years, include both the GMP and GCP sectors of the industry and have been made by FDA, EMA authorities, and WHO. The summary reports of non-compliance written by the MHRA and other EU authorities and published in *Eudra GMDP* appear very similar to FDA forms 483 and warning letters. WHO has published at least two Notice of Concern announcements in 2015 that also appear similar (HERE and HERE). Obviously firms that are still receiving these observations in forms 483 and deficiencies in warning letters missed opportunities to learn from publicly available information. Many have suffered expensive consequences, both financial, and in reputation. It is worth noting that enforcement actions have been taken simply when conditions exist where it is not possible to identify invalid or altered records. Regulators do not need to identify actual data falsification before they take action.

"Audit trails" are frequently cited in enforcement actions. It is important to remember that audit trails in electronic records are the equivalent of the "line-out, initial and date, explain" process used to identify and correct mistakes made in paper records. In the absence of appropriately configured and enabled audit trails it is *impossible* for a reviewer or auditor to ensure the data are valid and have not been altered or deleted. Warning letters have been issued for permitting *conditions* to exist where data may be changed or deleted; inspectors do not need to identify confirmed examples of inappropriately modified or deleted data.

As early as 2000, a warning letter issued to Schein Pharmaceuticals cited lack of control over computerized laboratory systems[1] including lack of password control and broad ranging staff authority to change data. Table 1 shows that selected enforcement actions based on data integrity have continued into 2015 with similar inspection observations, warning letter deficiencies, EMA findings and WHO actions. This is not meant to be a complete listing but rather to demonstrate ongoing, consistent enforcement actions in this area over ten-plus years. The comment column provides an abbreviated listing of some of the deficiencies that were identified. I encourage readers to evaluate the original document at the links provided.

Table 1. Selected Enforcement Actions for Data Integrity Problems

FISCAL YEAR	COMPANY	COMMENT
2000	Schein Pharmaceuticals	Warning letter to Schein Pharmaceuticals cites inadequate control over laboratory computer systems including password control and authority to change data. See specifics in endnote #2.

2005	*Able Laboratories, Cranbury NJ*	The 15-page form 483 was among the early forms 483 addressing the broad category of data integrity. The inspection resulted in withdrawal of ~ 50 ANDAs and the firm is no longer in business.
2006	*Ranbaxy, Paonta Sahib*	Failure to maintain documentation of operation conditions and settings, nor were complete raw data retained; SOP provides for discarding of data.
2006	*Wockhardt*	Failure to maintain complete and accurate records is a repeat deficiency cited at previous inspections; Logbook did not contain complete and accurate information; data were not documented at the time of performance.
2007	*Actavis Totowa LLC, NJ*	Electronic data files are not checked for accuracy; data discrepancies between electronic data and data documented in laboratory notebooks.
2008	*Ranbaxy, Paonta Sahib*	Written records were signed by individuals who were not present in the facility on the day of the signing;
2009	*Ranbaxy, Ohm Laboratories in Gloversville NY*	Analysts were given access to delete data, user account privileges were inadequate
2011	*Cetero Research*	This untitled letter was issued to a firm located in the US that conducted BA/BE studies in support of NDAs and ANDAs. As part of follow up, FDA sent a letter to the firms that contracted with Cetero Research for BA/BE studies requesting specific information to establish validity of the BA/BE information in the drug application. We also include one of the *forms 483*.
2013	*Wockhardt Ltd*	This letter was the second one in 2013 to cite the new FDASIA power to deem product adulterated if they are manufactured at a site that "delays, denies or limits" an inspection; investigators found batch records for 75 lots torn in half in the waste area; HPLC raw data files can be deleted from the hard drive using the common PC login used by all analysts
2013	*Wockhardt Ltd*	Practice of performing trial injections before the "official" injection; documentation entries not made as the activities were performed; HPLC data could be deleted from standalone instruments.
2013	*Fresenius Kabi Oncology*	This represents the first warning letter to cite the FDASIA definition of adulteration to include products made in a facility that "delays, denies or limits" an inspection; electronic data could be altered or deleted; use of "test" or "trial" injections.
2014	*Trifarma S.p.A.*	The firm does not retain laboratory raw data; there is a lack of access control to computer systems.
2014	*Apotex Pharmachem India Pvt Ltd.*	Lack of raw data; batches were tested until they passed; OOS events were not reported nor were they investigated.
2015	*Hospira S.p.A*	Chromatography systems did not have adequate controls to prevent deletion or modification of raw data files; audit trails were not enabled for the "Test" folder and the firm was unable to verify what types of test injections were made, who made them or the date or time of deletion.
2015	*Apotex Research Private Limited*	Data used to release product did not agree with the original data; "trial" injections were identified; failure to document activities as they occurred; failure to investigate and report OOS results
2015	*GVK Biosciences*	The French Medicines Authority inspected this site in Hyderabad, India and identified apparent data manipulations conducted in

		clinical studies, particularly with EKG data. The manipulations were reported to have been ongoing for 5 years.
2015	*Quest Lifesciences Pvt. Ltd.*	This WHO Notice of Concern addressed deficiencies in documentation in the GCP clinical trials area.
2015	*Svizera Labs Private Limited*	This WHO Notice of Concern addressed deficiencies in documentation

Now that we've addressed in some detail the deficiencies that global authorities have addressed in the GMP and GCP areas, we turn to identify what you can do within your own company to identify data management and data integrity shortcomings.

E. WHAT ACTIONS COULD FIRMS TAKE?

Often, the thought of addressing computer system issues and data integrity evaluations becomes overwhelming to the Quality unit and these responsibilities are deferred to members of the IT function. I intend to simplify this topic and identify some straightforward actions that firms can take to identify and correct deficiencies in the broad area of data management. The examples we provide here are only meant to be suggestions that a firm might consider. This becomes the starting point to develop a consistent means of evaluating electronic records, and associated paper records, within a firm and for their contract manufacturers and contract laboratories. It is not, however, meant to address technical issues associated with computer system validation but rather to look at this from a Quality Unit perspective.

- Data management that ensures security and reliability of the data must be effectively incorporated into the **Pharmaceutical Quality System**. Governance should be established that ensures procedures and processes are implemented and that staff are trained appropriately. The most senior management in the firm need to support the effort and potential cost, and lead the way to ensure the data from their firm is always correct, valid, complete and secure.
- Firms must recognize that **Part 11 requirements apply whenever electronic records and/or electronic signatures are used** in GXP processes and activities. Part 11 is a regulation, just as Parts 210 and 211 are regulations. Firms that maintain they operate primarily paper-based systems should consider that their laboratories depend largely on laboratory instrument associated computer systems. A firm cannot write an SOP that exempts themselves from compliance with this regulation. It is useful to read the *Preamble* accompanying publication of the Part 11 final rule to more fully understand the intent of the rule and its applicability.
- Quality system processes may need to be revised to address use of computer systems and electronic records. **Computer systems** should be **appropriately developed, qualified, tested and periodically assessed** to ensure they remain in a validated state. A risk-based lifecycle approach should be taken from initial system development through production, decommissioning and data archiving where appropriate. Changes made to computer systems must be adequately assessed for their impact on GMP operations they support. Changes made to GMP computer systems should be reviewed and approved by the Quality unit who should have appropriate training and expertise.
- As part of system validation / re-validation, firms should **perform gap assessments for each GXP computer system** against the requirements of Part 11 using the MHRA and WHO guidelines to provide additional explanation and examples of expectations. Documented evidence supporting conclusions should be provided or referenced within the gap assessment. The simple result of "Complies" is not sufficient. Where necessary remediation activities should be identified and their progress tracked through the CAPA quality process.

- **Internal GMP audit programs** should *always* incorporate assessments of data integrity. Internal audit staff should have documented training in assessments of data integrity. As the MHRA guidance states, these audits are not anticipated to include forensic type of audits. We provide a limited list of examples that might be addressed in internal audits, all can be found in forms 483 or in waring letters. Additional considerations should be added or modified based on newly published enforcement actions, or company specific needs. Further, when **audit functions are outsourced to a third party,** the firm should confirm that auditors have appropriate training in data integrity evaluations. This is particularly important for audits of contract laboratories, contract manufacturers and manufacturers of excipients.
- For the **QC laboratories**, specifically:
    - Laboratory instrument associated computer systems and other computer systems should be identified, assessed for their risk to the GMP area, requirements defined and validated appropriately. Periodic evaluations should be performed and documented to ensure they remain in a validated state.
    - Laboratory instrument associated computer systems and other GXP computer systems should be assessed for compliance with 21 CFR Part 11 and the MHRA guidance on data integrity. Gaps should be identified with a timeline and plan for remediation.
    - Changes to computer system software and hardware should be appropriately assessed and should not be made outside of the Quality System. For example, an out-sourced help-desk function should not make changes to GXP systems unless staff have the appropriate training and qualification. These changes should be documented within the quality system process, not exclusively in a help deck ticket.
    - The following limited list of activities to evaluate in the QC laboratory includes items from warning letters and forms 483 made available by FDA as well as those described in regulations and guidelines:
        - Is configuration of the instrument associated software qualified and tested appropriately to meet pre-defined requirements? Where is this documented?
        - Are passwords and log-ins shared or are they unique to each individual? Shared passwords prevent being able to attribute actions to a specific individual. This includes actions such as logging into the system, collection of data, processing data, modifying or deleting data.
        - Are access privileges assigned appropriately? Is there a listing of who has which privilege and actions that may be taken by each?
        - Are time/date stamps fixed or can individuals alter them?
        - Are electronic data, including audit trails, reviewed as part of laboratory result verification, lot release or OOS investigations? In the absence of audit trails and their review it is impossible for the reviewer to determine whether data have been altered or deleted. Of particular importance is whether data were modified or deleted because they were OOS results.
        - Is the review of electronic data described in an SOP and are reviewers appropriately trained in what they are to evaluate? How is the review of the electronic data documented?
        - How quickly can the audit trails be shown to an auditor? When it takes four staff member a half hour to locate the audit trail, it suggests they are not routinely evaluated.
        - Are data periodically backed up to a secure server, or are they deleted to make space on existing hard drives? Is the backup automatic or manual? If the transfer is manual, how

does the firm ensure that the transfer is complete and that data are not inadvertently deleted or altered in the process? Are these backups conducted according to a pre-defined schedule? If using automatic backup, has the process been validated and is it routinely successful?

- Equally import to the laboratory instrument associated computer systems are computerized controls applied **on-the-floor in the manufacturing** equipment. This area has received minimal attention from regulators to date, however, deficiency #6 in the December, 2015 *warning letter* to Sun Pharmaceuticals addresses such an issue.
- Finally, firms should ensure they are **informed regarding current regulations, guidance and the enforcement environment**. Enforcement actions evolve over time, and it is important to be aware of current trends. All of this information is publicly available. Enforcement actions can be monitored by review of available forms 483, warning letters, Eudra GMDP reports of non-compliance and WHO's Notice of Concern.

F. CONCLUSION: It does not take a complicated mathematical formula to show that severe financial consequences result from enforcement actions where data integrity is compromised. For example, Able Laboratories ceased doing business after receiving their form 483 in 2005, Cetero Research is no longer a business entity, Ranbaxy has been acquired by Sun Pharmaceuticals in India, and Wockhardt Ltd's sales are severely diminished in the US[iii]. All were cited in inspection forms 483 or warning letters for deficiencies in assurance of data management and data integrity.

While the Quality Control laboratory is the most frequent area where data integrity issues are identified, it is by no means the only area. Data management spans all functions within pharmaceutical and device firms. Firms are encouraged to address and provide consistent data management governance in all GXP areas, including enterprise planning systems, clinical / medical affairs and Research and Development.

Further:

- Data management and the assurance of data integrity should be effectively incorporated into the Quality Management System and should address both paper records and electronic records.
- All GxP audits should evaluate data management and data integrity.
- Computer system validation and lifecycle management should not be isolated within the IT function but rather should be shared with the Quality unit and other stakeholder functions.
- The Quality unit staff may need additional training to provide meaningful review and approval of computer system associated processes and procedures.
- Finally, governance should be established across all GxP areas and management involvement and support should be highly visible.

Data are publicly available to inform companies and their staff about changes in GMP laws, regulations, guidance, inspection focus and enforcement trends regarding data integrity. These changes can be monitored directly by reviewing regulatory agency website publications and / or a variety of both free and paid newsletter publications. Enforcement actions are made available on regulatory agency websites though the level of detail may vary among the agencies. Requirements for electronic records are not going away and failures in this area are demonstrated to be costly to remediate. It is far better to identify any deficiencies internally and remediate without intervention by a regulatory authority.

REFERENCES

- FDA *21 CFR Part 11*, *Electronic Records*; *Electronic Signatures*, 1997
- *Preamble* to the final rule, 21 CFR Part 11, March 20, 2997
- *Guidance for Industry*, General Principles of Software Validation, January, 2002
- FDA *21 CFR Part 211*. Current Good Manufacturing Practice for Finished Pharmaceuticals.
- FDA Compliance Program Guidance Manual, Chapter 46 – New Drug Evaluation, *Pre-Approval Inspections*, *Program 7346.832*
- FDA slide deck describing *GMP audits of Data Integrity and Automated Systems*. This presentation was given by Robert D. Tollefsen National Expert – Computers on April 27, 2010. He delivered the same slide deck at many industry conferences.
- FDA Guidance for Industry, Part 11*, Electronic Records; Electronic Signatures –Scope and Application*, 2003
- FDA *Guidance for Industry, Electronic Source Data in Clinical Investigations*, September 2013 formally addresses the ALCOA acronym.
- 15-page *form 483* issued to Able Laboratories in 2005.
- Rules Governing Medicinal Products in the European Union. Good Manufacturing Practice, *Annex 11*, Computerized Systems, effective 30 June 2011
- Rules Governing Medicinal Products in the European Union, Good Manufacturing Practice, *Part II*: *Basic Requirements for Active Substances Used as Starting Materials*
- MHRA *GMP Data Integrity Definitions and Guidance for Industry*, March 2015
- MHRA *expectations regarding self inspection and data integrity*, December 2013. See also the explanation from the European Compliance Academy *HERE*.
- *MHRA Inspectorate Blog on Data Integrity*, 3 parts starting June 25, 2015.
- MHRA Presentation on Data Integrity in Goa, India, September 2014. See the link to download the slides at the *bottom of the page*.
- *ICH Q7*, Good Manufacturing Practice Guide for Active Pharmaceutical Ingredients
- PIC/S Guidance, Good Practices for Computerized Systems in Regulated "GXP" Environments, 25 Sept 2007. *Guidance for Inspectors*, PI 011-3
- PIC/S Annexes to GMP Guide, Annex 11, Computerized Systems in the *GMP Guide (Annexes)*
- WHO published a 35-page draft document on their website for comment, *Guidance on Good Data and Record Management Practices* for GXP regulated activities.
- *WHO Notice of Concern* issued to Quest Life Sciences Pvt. Ltd on 30 June 2015. This site conducts clinical studies
- *WHO Notice of Concern* issued to Svizera Labs Private Limited on 2 September 2015.
- Addressing the historical issue of data integrity in FDA enforcement actions: *The Financial Value of a Comprehensive GMP Regulatory Intelligence Program*, March 25, 2015, Unger Consulting, Inc., includes links to associated warning letters, particularly those from 2000-2008.
- Notre Dame Law Review, Volume 75, Issue 1, October 1, 1999, page 312. Describes the nature and outcome the US generic drug scandal.
- *Unger Consulting Inc*. data, available upon request. Delineates the common regulations cited in FDA warning letters associated with data integrity.

- Free Guidebook from Colgin Consulting, Inc.: *"5 Questions You Should Ask Your GLP & GCP Labs – And the Answers You Need to Know."* This is available for free upon registration on the left hand side of the page to which the link takes you. The concepts are equally applicable to the GMP laboratory.
- ICHQ10, Pharmaceutical Quality System, identifies **Knowledge Management** as an "enabler" of an effective Quality System.

END NOTES:

[i] Notre Dame Law Review, Volume 75, Issue 1, October 1, 1999, page 312.

[ii] The warning letter is not available on the current FDA web site and must be requested under FOI. Following is the specific deficiency, #6 among the deficiencies listed in the warning letter:

> **6. Failure to maintain the integrity and adequacy of the laboratory's computer systems used by the Quality Control Unit in the analysis and processing of test data.** For example:
> a) There was a lack of a secure system to prevent unauthorized entry in restricted data systems. Data edit authorization rights were available to all unauthorized users, not only the system administrator.
> b) The microbiology departments original reports on sterility test failures of Penicillin G Potassium for injection, lots 9804024 and 9811016 due to environmental mold, which were sent via electronic mail to the Quality Assurance Management, differed significantly from the versions included in the Quality Assurance Management's official reports.
> c) The network (b) (4) module design limitations, which can only support up to four chromatographic data acquisition systems, had up to five chromatographic systems connected. There was no validation showing this configuration to be acceptable.
> d) System testing was not conducted to insure that each system as configured could handle high sampling rates. Validation of the systems did not include critical system tests such as volume, stress, performance, boundary and compatibility.

[iii] See article in FiercePharma from 11/3/2014