DATA INTEGRITY and DATA MANAGEMENT for GXP REGULATED FIRMS

Barbara W. Unger
Unger Consulting Inc.

PART 3

This is the final entry in the 3-part series. So far we've covered the history of how we reached the point where regulators have an intense focus in this area. We've addressed the governing regulations and guidance and some selected enforcement actions that global regulatory authorities have taken in this area. For a full collection of enforcement actions taken in 2015, see the other links included at the end of the main blog post. Now we look at actions that you can take within your firm. In conclusion I provide a list of relevant references, including links.

Here we go!

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[i]. 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.

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