DATA INTEGRITY and DATA MANAGEMENT for GXP REGULATED FIRMS

Barbara W. Unger
Unger Consulting Inc.

PART 2

In Part 1, we reviewed the history of how we got to this point with global regulators focused on data integrity. FDA found the data integrity problems were widespread during the 2010 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 in part 2.

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*…".

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 *EudraLex 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

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

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.*	Failure to retain raw laboratory data; lack of access control over 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. This will come soon in part 3.