Michael Rutherford

GAMP Global Chair, GAMP Data Integrity SIG Sponsor, ISPE 2016 Joseph X. Phillips Professional Achievement Award, ISPE 2014 Member of the Year, 2016 and 2017 ISPE Annual Meeting Education Program Chair, ISPE 2017-2018 International Board of Directors

Over the last 5-7 years, it is no surprise that data integrity has become one of the hottest regulatory and compliance topics affecting not only the pharmaceutical industry, but the scientific community. You cannot read a regulatory inspection report or warning/ untitled letter today without finding at least one, and usually more, data integrity related observations. The retraction of scientific articles in reputable scientific and medical journals has also increased due to concerns about the integrity of the data and results, raising concerns about basic research and the data associated with drug products. Data integrity is a global regulatory and compliance expectation, and actually not a new expectation. Data integrity regulations and requirements have truly existed since the 1970's and 21 CFR Part 11 actually celebrated its 20th anniversary this year. Regulatory agencies, as well as industry, rely on accurate information to ensure drug quality. If the information associated with a drug product is not accurate or reliable, there is no way a company can ensure the safety and efficacy of their products for the patient. And global regulatory agencies are becoming more aligned around these expectations. Non-compliance has resulted in recalls of products, warning or untitled letters, import alerts, injunctions, seizures, Application Integrity Policy Invocations/ legal action, and most concerning, a potential for patient harm and an impact to the pharmaceutical supply chain. It is as much a compliance issue as it is a financial issue, as seen by the impact of these regulatory actions on companies bottom lines.

It is important to note that data integrity really comes down to two key elements: data governance and data life cycle management. When we talk about management systems and governance, we are talking people, process, and technology and the associated behavioral, procedural, and technical controls. The general goals and objectives of data governance are straightforward:

- Increasing consistency and confidence in decisions
- Decreasing compliance risk
- Improving data security
- Maximizing potential business value of data
- Clarifying information ownership and accountability
- Minimizing or eliminating re-work
- Optimizing process effectiveness

For our regulated industry, the objectives are a bit more specific. We can minimize our inspectional risk by demonstrating our fitness for intended use through CSV, assessing and controlling our data integrity risk, ensuring adequate data security and access control, and effectively comply with the GxP's. But we must not lose sight of the most important objective – ensuring product quality and patient safety.

Regulatory agencies rely largely on trusting companies to do the right thing to deliver safe and effective products for their patients when the agencies are not there. Data integrity problems break that trust between industry and regulatory agencies. It should be no surprise that this trust and data integrity is heavily dependent on the company's leadership and corporate culture.

Leadership and the culture must support effective data governance processes, including effective policies and standards for data integrity, security, quality, roles and responsibilities, and use of data, as well as data integrity training and awareness for all employees. Management must lead by example and "walk-the-talk". They must promote an environment that reinforces and rewards positive action, but also take the necessary action when expectations and policies are not met. Humans make mistakes and mistakes often result in data integrity issues. Since many of our processes require human involvement, all companies have some level of data integrity issues. It is therefore critical that management drive a strategy focused on prevention, detection, and response regarding data integrity.

A company's strategy for addressing data integrity should be documented in a plan. This plan is a high-level document that defines the scope of activity, objectives, governance process (including metrics and program reporting), and action plans and initiatives. It serves as the basis for a company's data integrity program, and should be scaled based on the size and complexity of the business, the level of compliance risk, and the potential impact on product quality and patient safety. With all of the emphasis on data integrity by the regulatory agencies, you might think you should drop everything just to focus on data integrity. Regulatory agencies have made it very clear that data integrity issues should be prioritized and balanced based on criticality with your other product quality issues.

The other key element of data integrity that I mentioned earlier was data life cycle management. Data integrity is commonly defined as the degree to which data are complete, consistent, and accurate, throughout the data life cycle. I am sure all of you have heard the term ALCOA or ALCOA+ by now, which defined the attributes of data if they have integrity. (ALCOA = Attributable, Legible, Contemporaneous, Original, Accurate. + = Complete, Consistent, Enduring, Available) Just like many other life cycles, such as a system life cycle or product life cycle, it addresses data from creation to final destruction. In the ISPE/ GAMP Records and Data Integrity Guide (released in April 2017), we broke the data life cycles into the following phases: Creation; Processing; Review, reporting, and Use; Retention and Retrieval; and Destruction. Each lifecycle phase can have an impact on data integrity, and therefore should be considered as part of governance process. The best way to understand a data life cycle is to understand and define the data flow. Data associated with a product or process may cross various boundaries and interfaces throughout the life cycle. Risks associated with such transfers need to be considered and appropriately controlled to prevent data loss or modification.

As we talk about the various phases of the life cycles, there are some key takeaways and common themes. Data integrity may be, and many times is, compromised at the point of creation. All data, even if excluded, should be retained and available for review, and if excluded, a valid, documented, scientific justification is required for all excluded data. When processing, reviewing, reporting, and using data, there must be a defined and verified process (i.e. a procedure). As I mentioned earlier, procedural controls are a key element of data governance. One key review item is the audit trail, which should be based on a documented risk assessment taking into account the business process and criticality of the data, the complexity of the system and its intended use, and the potential impact on product quality. The audit trail provides one of the best means to identify potential data integrity issues. It should be performed by an individual who has an understanding of the business process and the impact on product quality and patient safety. When it comes to data retention and retrieval, it must be all of the original data and metadata required to maintain the GxP content and meaning and be stored securely to protect against deliberate or inadvertent alteration or loss throughout the retention period. This can present some real challenges, especially for data with long retention periods. Verification should occur to ensure the data can be retrieved following changes to the system. Also, when a system is retired or can no longer be supported, it is essential that you consider how the data will continue to be retained and retrieved throughout the retention period, including criticality of the data, practicality, migration options, and risks associated with maintaining the data without the metadata. When you can finally destroy the data since the retention period has expired, it also should be done in accordance with a defined and verified process, just like many other processes within the life cycle.

I have focused on just two key elements of data integrity in this brief editorial, barely touching the surface of what data integrity is all about. Hopefully this has sparked your interest enough to want to learn more about data integrity and why it continues to be such a high profile topic. ISPE, and GAMP in particular, has had a focus on data integrity for over five years. That focus really ramped up in January 2014 with the launch of the GAMP Data Integrity Special Interest Group (SIG). This SIG has played a key role in helping drive ISPE's focus on the topic, culminating in the release in April of the ISPE/ GAMP Records and Data Integrity Guide. The SIG is working on additional Good Practice Guides (GPG's) to provide practical approaches to key data integrity areas. You also have an excellent opportunity to learn more directly from industry experts at the ISPE Asia Pacific GAMP Data Integrity Conference, November 13-14, 2017, in Singapore. I will be attending and presenting at the conference along with many of my ISPE/ GAMP colleagues and industry experts in the data integrity field. I hope to see folks there.