Considerations for a Corporate Data Integrity Program

March 2016

A Concept Paper by the ISPE GAMP Community of Practice

Acknowledgements

This Concept Paper was written and reviewed by members of the Global ISPE Data Integrity Special Interest Group (SIG) of the ISPE GAMP Community of Practice (COP). It represents industry best practices based on the experiences and input from the individuals listed below and does not reflect the views of any one individual or company.

SIG Chairs

Lorrie Vuolo-Schuessler	GlaxoSmithKline	USA
Mark Newton	Eli Lilly and Company	USA
Nigel Price	Crucell	Switzerland
Christopher White	Alexion	USA

SIG Sponsor

Michael Rutherford	Eli Lilly and Company	USA

Document Authors

John Avellanet	Cerulean Associates LLC	USA
Eve Hitchings	Eli Lilly and Company	USA

Reviewers

Lorrie Vuolo-Schuessler	GlaxoSmithKline	USA
Mark Newton	Eli Lilly and Company	USA
Bob McDowall	R D McDowall Limited	United Kingdom

Regulatory Input and Review

David Churchward	MHRA	United Kingdom
Karen Takahashi	FDA	USA

Particular thanks go to the following for their support of this Concept Paper:

Chris Clark	TenTenTen Consulting Ltd.	United Kingdom
Arthur (Randy) Perez	Novartis Pharmaceuticals	USA
Sion Wyn	Conformity Ltd.	United Kingdom
Christopher White	Alexion	USA

Table of Contents

In 2007, the US Food and Drug Administration (FDA) indicated that the agency had begun specialized training for all investigators and submission reviewers on "uncovering data integrity, data manipulation and fraud." [1] Three years later, in July 2010, the agency announced increased data integrity rigor for all pharmaceutical inspections. Since that time, FDA has issued import alerts banning drug products because of poor integrity of the data supporting these products [2].

Data integrity is a global expectation as evidenced by the Medicines and Healthcare Products Regulatory Agency (MHRA) guidance, published in January and March of 2015 [3, 4], joining the FDA and European Medicines Agency (EMA) in prescribing expectations.

For life science companies, data integrity is both a regulatory compliance and also a financial issue. With industry's increasing reliance on technology and digital data, data integrity has begun to claim its place in the spotlight.

1 Introduction

On numerous occasions regulators have cited companies for inadequate controls on the integrity of data, raising questions as to the authenticity and reliability of the data [5, 6, 7, 8]. Therefore, implementing a successful corporate data integrity program has become a prerequisite for successful GxP compliance in the 21st century and an integral part of a company's Quality Management System (QMS).

This Concept Paper focuses on electronic records and computerized systems – a key area of emphasis for GAMP®. However, manual systems and paper based records remain a key area of data integrity failures. The risks associated with manual systems, including the risks between manual and computerized systems, should not be overlooked. The intent of this Concept Paper is to share implementation considerations based on the experiences of several companies, including successes and challenges. Although the specifics of each individual company's data integrity program will be different, the considerations described should give companies a direction for creating a successful corporate data integrity program.

2 Critical Success Factors

2.1 Executive Sponsorship

Just as an effective quality system requires the active involvement and support of senior management, so too does an effective data integrity program need executive commitment. In FDA's terminology, "senior management with executive authority" will be called upon to promote the data integrity cause, provide appropriate resource allocation, settle differences of opinion and priorities, and ensure that data integrity expectations are carried out across all levels of the organization [9].

Best practice experience dictates obtaining an officer of the company as the sponsor for the data integrity program because, at some point, sponsors will be required to:

- set a direction
- define priorities
- provide resources
- break down organizational resistance to change

The higher the level of the sponsor, the greater the force that can be leveraged to ensure alignment across the company.

Practically speaking, however, actual day-to-day sponsorship, guidance, and supervision of the data integrity program will likely be delegated to a mid-level executive. Regardless of who serves as the sponsor, management accountability, at all levels of the corporation from the Chief Executive Officer (CEO) to the operations floor supervision, plays a key role in ensuring data integrity. It is critical that they "walk the talk" and foster an environment that promotes and ensures good data integrity practices. By doing so, they demonstrate the core values of integrity in response to a failure. They do not incentivize data falsification and discourage the "wanting to please management" mentality that can lead to many data integrity issues. And of most importance, they eliminate the fear of management retribution and foster an environment where employees are empowered and encouraged to identify and report data integrity issues on the shop floor.

The MHRA stated in their guidance that: "The data governance system should be integral to the pharmaceutical quality system." [3, 4] They also prescribe that the effort and resource assigned should be commensurate with the risk.

Executives need an awareness of four key benefits that a data integrity program can deliver, including:

1. Financial (e.g., bottom line) benefits
2. Risk reduction
3. Regulatory benefits
4. Legal product liability

Specific points to emphasize these key benefits include:

- Good data integrity practices are increasingly seen by regulators and investors as a fundamental requirement for accurate financial reporting and forecasting [10].

- More than a decade of experience combining good data integrity practices with risk-based computerized system validations has shown that this combination can reduce the overall costs of validation – and maintain such validation.

- Good data integrity requirements cross multiple regulatory health agency rules, including those of the FDA, EMA, Health Canada, MHRA, and both the harmonized International Council on Harmonisation (ICH) and Pharmaceutical Inspection Convention and Pharmaceutical Inspection Co-operation Scheme (PIC/S) guidelines, reducing the work needed to comply with each region.

- Good data integrity practices (often seen as akin to good recordkeeping practices in the legal profession) have been shown to reduce legal costs during product liability litigation and e-discovery [11].

By showing that the return on investment in an effective data integrity program outweighs the costs, the support of executive sponsors will be easier to obtain.

It is vital to obtain senior level executive sponsorship for a corporate data integrity program to ensure a holistic, thorough system that can withstand regulatory scrutiny.

2.2 Cross-Functional Steering Committee

The senior management sponsor will set the data integrity expectation and priorities; however, a steering committee consisting of the company's functional leaders and departmental supervisors will ensure their implementation. Because regulated data is created, reviewed, transformed and summarized, stored, migrated, and archived across multiple departments, an effective data integrity program requires a wide variety of functional inputs.

Data also crosses regulatory boundaries, e.g., data initially collected in clinical settings and nonclinical laboratories may fall under the Good Clinical Practice (GCP) and Good Laboratory Practice (GLP) regulations, only to be later used in assessing postmarket safety issues and fall under the Good Pharmacovigilance Practice (GPvP), Current Good Manufacturing Practice (CGMP), or even the Good Distribution Practices (GDPs). An effective data integrity program controls the integrity of regulated data across the data life cycle, all the way from its initial creation to its eventual long-term disposition and destruction. In this light, a cross-functional approach to implementing an effective data integrity program is a necessity.

To obtain accurate and helpful input, stakeholders from each of the key functional areas need to be represented in the program implementation group. Experience has shown that too large a team will be unwieldy and ineffective. Rather, consider a core steering committee supplemented on an ad hoc basis by subject matter experts and functional leaders of relevant regulated operations, as they come under the overall data integrity control framework during its implementation throughout the organization.

2.2.1 Avoid Temptation

It may be tempting to assign the responsibility for implementing the data integrity program to the Information Technology (IT) department or to the Records and Information Management (RIM) department. Avoid this! There are a number of reasons why succumbing to this temptation carries a high risk.

First, IT and RIM personnel do not have the business process knowledge to decide when a data set is "complete," or "accurate," or "original," and so on. Additionally, IT or RIM may not actively be involved in all the company's day-to-day activities of the data life cycle. Without the capability to discern data quality, they cannot identify and implement controls designed to minimize the risk to data integrity:

- How is the IT manager to assess if the chromatogram included all the results?

- When is it appropriate to drop a particular outlier from a data set?

- How should the RIM analyst view a request to catalogue and store the raw chromatography data (including sample set, injection sequence, and manual integration log) versus just the summary output graph?

- Can the RIM analyst identify raw data versus transformed data – or whether data is missing?

Second, data integrity requires a series of controls spanning the entire data life cycle. Often, neither IT nor RIM will have insight into the company's data that either exist at a vendor, are transferred into the company from a vendor (or vice versa), or are created and held on behalf of the company at a vendor (such as through usage of a Contract Research Organization (CRO) or Contract Manufacturing Organization (CMO). Failing to acknowledge the need for controls around data from such vendors leaves a gap in the data life cycle that allow for accusations of data integrity failure.

Finally, there is a risk of scope creep if data integrity initiatives are turned over to IT. FDA is focused on a narrow application of integrity controls intended to avoid regulated data fraud and/or regulated data loss. In contrast, IT-led data integrity initiatives can quickly upscale into broad, corporate-wide data governance initiatives leaving FDA's data integrity controls as a subset of the greater body of data governance. It is better to view the implementation of an effective data integrity program as a step toward the long-term data governance; therefore, it is recommended to let IT lead the greater data governance initiative but not the more narrow GxP data integrity effort. Leaving data integrity in the hands of IT or RIM is a recipe for confusion, frustration, and non-compliance.

2.2.2 Roles and Responsibilities

Various functions within an organization have different, but very important, roles to play in an effective data integrity program. While every company may approach the core cross-functional steering committee differently, one approach is to denote the core team using the following type of matrix.

Function	Steering Committee Role
Quality and Regulatory	Lead the committee; review and approve assessments and associated action plans; conduct periodic audits; draft policies and procedures; provide insight into regulatory analyses; conduct relevant guidance research; provide updates on recent regulatory agency expectations and activities relating to data integrity.
IT	Provide technology framework and automated controls insight; participate in system assessments; participate in vendor qualification; help draft policies and procedures as applicable; work with RIM to manage long-term data archives; implement agreed-upon automated controls, etc.
RIM	Provide archival and retention frameworks and controls inputs; details on record retention schedules; participate in vendor qualification as subject matter experts; help draft policies and procedures as applicable; work with IT to coordinate and manage long-term data archives, etc.
Purchasing/Vendor Management (if a company relies heavily on outsourcing regulated activities, e.g., virtual pharma)	Provide insight into various outsourced activities; help qualify and monitor vendors; ensure data integrity expectations are built into (or added into) vendor contracts; work with IT to ensure data integrity transference controls are built into the contracts (to maintain the data life cycle), etc.

Individual functional leaders should then be added into the mix as necessary, in which case the matrix might be supplemented with this row:

Business Functional Leaders by Department (various)	Provide operational guidance and business process knowledge for regulated data identification and data life cycle knowledge, provide insight into data obtained/transferred from vendors, business partners, other departments and sites; work with departmental staff to conduct initial assessments, etc. (in many organizations, these may be termed the "data owners").

At the outset of the initiative, consider holding a large inclusive meeting to clarify expectations and priorities, discuss common data integrity risks across the data life cycle, and then allocate work aspects on a department by department basis. Periodically, confer to:

- review the overall implementation status
- discuss open or emerging issues and risks
- review new regulatory initiatives associated with data integrity
- re-calibrate priorities based upon new business initiatives

2.3 Common Knowledge Sharing

Another crucial success factor is assuring that the executive sponsor, steering committee, and functional leaders agree about priorities and strategy. Common questions to address include:

- What does data integrity mean in day-to-day business operations?
- What is the role of computerized system validation in data integrity?
- How does data integrity integrate with 21 CFR Part 11 [12] or EU Annex 11 [13] compliance?
- Does FDA or EMA accountability differ from company accountability?
- When does the data integrity life cycle start? When does it end?

Multiple training courses will need to be held, preferably beginning with the sponsor and the steering committee, then moving to functional leaders and the organization as the program proceeds.

Experience has shown several strong best practices with significant, positive long-term impact:

1. Create a data integrity knowledge repository or knowledgebase.
2. Bring in temporary outside expertise early when required.

2.3.1 Early Outside Expertise

There are many ways in which implementing a data integrity program can go wrong. Some are obvious – focusing only on computerized system validation as the solution to data fraud and/or data loss – while some are more subtle – confusing the regulator's intent to avoid regulated data fraud and/or loss with the larger need for organizational good data governance.

Increasing regulatory scrutiny and the dozens of data integrity-based warning letters and enforcement actions since 2010 clearly indicate the perils of data integrity mistakes. In several recent warning letters, the FDA has noted that inexperience in data integrity controls caused serious compliance problems and recommended that companies bring in an outside "auditor/consultant with experience in…data integrity problems to assist you with coming into compliance." [14]

If a company does not have in-house experience for implementing data integrity – or has failed in past implementation attempts (whether this failure included public enforcement actions or not) – they should bring in outside expertise to help guide the initial stages of implementation. To understand current practices and issues, they should join some of the special interest groups available such as the ISPE/GAMP Data Integrity or Cloud Computing groups. LinkedIn and the ISPE and GAMP Communities also offer several 21 CFR Part 11 [12] and data integrity groups that may be able to answer specific, focused questions. Additionally, several industry associations such as ISPE, the Drug Information Association (DIA), and the Society for Clinical Data Management (SCDM) offer learning opportunities focused on specific types of data challenges.

Avoid any temptation to outsource the data integrity program; this is equal to outsourcing compliance. By outsourcing data integrity, a company is not taking ownership of its own records. The regulators will hold companies accountable for the regulated data they use, and trying to outsource the responsibility for the data integrity program is a recipe for potential contractual disputes, regulatory enforcement actions, internal non-compliance, and litigation.

If outsourcing is warranted, consider limiting their activities to training workshops, knowledge sharing, and subject matter expertise-level guidance and input. Such external expertise can also consist of helping the implementation team identify old organizational habits that may no longer be appropriate.

2.3.2 Data Integrity Repository/Knowledgebase

Knowledge sharing provides an advantage for areas within the company just preparing for the data integrity program. It is not possible to share too much information when it comes to successful data integrity.

One strong recommendation is to create a repository/knowledgebase, such as a company wiki or a SharePoint® site of, for example:

- guidance documents
- templates
- checklists
- decision-trees
- data integrity regulatory citations
- example enforcement actions relevant to the company's activities
- copies of the training program

As time goes on, experience with various data integrity questions specific to the organization will necessitate the creation of a series of frequently asked questions (FAQs) that could be posted to the knowledgebase.

A glossary of terms that is reviewed and approved by qualified personnel should be available. This can limit confusion and discussion as the program rolls out to those not initially involved. Similarly, it may be helpful to create a feedback mechanism so that individual questions can be addressed to core team members before the data integrity program is implemented at a particular department or site – this allows a lowering of the inevitable anxiety of a new compliance program. Anxiety is also generated around potential changes to business processes and controls, so it is imperative that the data integrity implementation team be clear to departmental personnel about the value added from good data integrity practices.

Another essential element of implementation success is the availability of data integrity Subject Matter Experts (SMEs) to lead, facilitate, or otherwise participate in local implementation meetings and discussions. If an outside expert is brought in to help the core team, consider using the expert to conduct train-the-trainer sessions, work through anticipated difficulties using group role-play, share experiences and best practices from other companies which have implemented data integrity programs, and show examples of positive results from improved data integrity.

Helping people become more comfortable with the intent and scope of the data integrity program, and understanding how the data integrity controls may – or may not – impact their day-to-day activities, will aid in its adoption and empower them.

2.4 Supplier Involvement

In the 21st century, life science companies increasingly outsource regulated activities that involve regulated data. Whether it is a CRO, CMO, Software-as-a-Service (SaaS), data center services, or long-term data archival storage and retrieval, suppliers inevitably play a role in an effective data integrity program. A risk-based approach to supplier data integrity controls is essential to an effective program. (ICH Q9 – Quality Risk Management – is an internationally harmonized approach to assessing risk management strategies and can provide some guidance in this area [15].)

First and foremost, suppliers that create, use, or manage data on behalf of the life science company need to be qualified. Not all such suppliers are regulated by FDA or other regulatory agencies and, therefore, avoid requiring "all vendors to have data integrity programs." This is not realistic for vendors that do not actually touch a company's data, but may instead only serve to store it – unopened and un-accessed by the supplier (such as an outsourced data center). Instead, determine if the supplier has a control framework in place that can ensure the integrity of data for the purposes of the regulated activity they perform. In other words, a CRO should have more data integrity controls than the archival storage vendor, because a typical CRO has the ability to create, edit, and manipulate individual data points, whereas a typical archival storage vendor has limited access to anything except entire datasets and/or archived media.

Second, contracts and quality agreements should explicitly state the particular types of controls the company expects its data handling suppliers to maintain. Thus, it is imperative that subject matter experts from the overall data integrity core team (such as Quality/Regulatory, IT, RIM, etc.) be involved. Controls should not be prescriptive (e.g., "all passwords used at a vendor must be at least eight alphanumeric characters in length") but rather reference common industry guidance such as that from ISPE or the International Organization for Standardization (ISO). Many suppliers used by life science companies are not bound to GxP regulations, so widely accepted industry best practices are important in qualifying and monitoring a supplier. Depending on the risks associated with a supplier's activities, at least one audit may need to be conducted of the supplier's controls.

2.5 Risk-Based Prioritization

An initial challenge in implementing effective data integrity is coming to terms with how to direct the limited funds and resources available. Even with an enthusiastic executive sponsor, there may not be sufficient money, time, or manpower to do everything perfectly. The executive sponsor may be called upon to decide final priorities to allow the organization to make the best use of its limited resources.

The various methods of assessing risk to data, to patients and customers, to final product, and to a firm's compliance status are beyond the scope of this Concept Paper. Traditional, system-by-system or dataset-by-dataset risk analysis methods, such as Failure Mode and Effects Analysis (FMEA) or Hazard Analysis & Critical Control Points (HACCP), may not be appropriate when trying to prioritize overall data integrity implementation activities. Instead, some form of rapid risk analysis will likely be sufficient, leaving more detailed analyses for scoping specific system validations or vendor qualifications. From a data integrity perspective, reasonable risks need to be identified, controlled, and mitigated.

Because business plans and conditions are constantly evolving, the steering committee should be prepared to periodically re-evaluate the risks and priorities for implementing data integrity controls. Data integrity cannot be implemented in a vacuum. The business and marketplace evolutions will not pause and wait for the project to complete. This is one more reason why a core cross-functional steering committee and a good executive sponsor are crucial to success.

2.5.1 Overall Data Integrity Plan

One approach to consider is a short, high-level plan with broad timescales (monthly or quarterly) that can be used by the executive sponsor and the steering committee. This can be provided to regulatory agency investigators and third-party auditors when a company is asked to provide proof of progress toward meeting improved data integrity and 21 CFR Part 11 and/or EU Annex 11 compliance [16]. To date, such overviews have been requested on a site-by-site basis.

2.6 Plan for Continuous Improvement

Another crucial success factor to implement an effective data integrity program is instilling the need for continuous improvement. Just as changing business plans and conditions drive re-evaluation of risks and priorities, so too will business evolution require implementation evolution. There are three important aspects to continuous improvement beyond simply re-evaluating and revising the implementation plan:

1. Metrics
2. Reporting
3. Auditing

Each of these is a significant topic and details are beyond the scope of this Concept Paper. However, some framing remarks and considerations for each are necessary.

Metrics are necessary for two reasons:

1. to help ensure that the promises of a positive return on investment are being fulfilled
2. to help ensure that the data integrity program itself is succeeding

For example, an effective data integrity program combined with risk-based validation should achieve reduction of computerized system validation costs. Thus, comparing the costs – including time and resources required, not just money involved – of two relatively similar system validations before and after implementation of data integrity controls is one example metric. Another metric could be the number of data integrity related internal quality audit findings prior to implementation of the data integrity program compared to findings following implementation. It should be noted that at early stages of the program, reporting of data integrity issues will increase with increased awareness and improved detection, which may skew the metrics. It is important to manage this “bad news” and continue to foster an environment of open reporting.

Reporting needs to be established both with senior management, typically through the executive sponsor, and with the overall organization. Done well, reporting can help further organizational ownership. Reporting should demonstrate the progress being made to date, identify specific open issues to be resolved, discuss next steps, and showcase current metrics as well as target numbers. Monthly or quarterly periodic meetings with the executive sponsor need to discuss implementation status and continuous improvement steps. If the rollout will take longer than a year, time needs to be set aside to revise and update the overall data integrity compliance plan referenced earlier.

Two elements that are critical to ensuring the success of the program and continuous improvement are training and auditing. General staff training should not be overlooked since it provides the critical foundation to achieve a state of understanding for doing the right things rather than policing and implementing IT barriers to prevent the wrong things. Both training and auditing are important because both are only effective up to a point. Auditing for data integrity goes beyond the typical internal quality auditing necessary for an effective quality system. There are multiple types of audits required in an effective data integrity program:

- Initial gap assessment or audit of non-conformance to data integrity control requirements and best practices
- Ongoing internal quality audits of established data integrity controls to ensure continuing effectiveness and compliance
- Periodic audits of long-term data archives to verify the controls for data deterioration and media migration are being followed and are effective
- Supplier qualification audits for suppliers creating, modifying, reviewing, analyzing, transmitting, storing, and/or archiving data on behalf of the company
- Closeout gap assessment or full audit following (or close to) completion of data integrity program implementation

Auditing plans should be made and audits conducted as the data integrity program proceeds. In this way the company can be certain that progress made is retained and built upon.
For the initial gap assessment and closeout assessment, consider an independent auditor. This does not necessarily mean an outside expert, but rather use someone independent of the core team. An auditor from another of the company's sites that has already completed a successful data integrity program, an internal subject matter expert recently hired into the company who was not involved in the initial project, etc., are possible independent sets of eyes through which to identify and evaluate potential data integrity gaps.

2.7 Organizational Communication and Reinforcement

Communicating to the organization – and reinforcing – the need for good data integrity practices is a crucial requirement for success. Periodic meetings with the sponsor and reporting various metrics are one means to this end.

In the repository/knowledgebase section, building a set of Frequently Asked Questions (FAQs) can be one helpful means to communicate. The FAQs should be publicized as the project proceeds to each new area of the company. Hold informal "lunch-and-learn" sessions to lower anxiety, answer questions, address concerns, and keep people informed and aware.

Consider creating one-page "guides" that address specific topics such as "What to do when you need to scan records and data from paper to electronic format" (which might point out a particular Standard Operating Procedure (SOP) to follow, perhaps several FAQs to read, the company's resident subject matter expert on scanning, etc.) or "How to ensure data from your vendor has integrity" (which may point out the need for a qualification audit to ensure the contract has specific data integrity controls, a specific SOP on sampling and verifying incoming data, the company's resident subject matter expert on supplier data integrity and 21 CFR Part 11 [12] compliance, EU Annex 11 [13] compliance, etc.)

Techniques such as these will help sustain and build momentum and then serve to buttress a growing culture of data integrity for long-term success.

2.8 Mix Procedural, Physical, and Logical Controls

Effective data integrity necessitates a mix of controls. From auditing vendors to system validation, automated data creator identification (e.g., user accounts and passcodes) to automated disaster recovery backups, physical security of stored data can be complicated without significant thought given during implementation.

The core steering committee needs to identify the controls and best practices the company may already have in place and those the company need to strengthen and/or create. Both the initial training of the core team as well as an independent “as is” gap analysis can help in this identification process.

The executive sponsor and the core team need to fully acknowledge that there are no one-size-fits-all types of controls that work in every situation where the company needs to control regulated data integrity. Automation can only go so far and procedural and policy controls, along with appropriate training on them, are necessary, as are physical controls. Written contracts with vendors are required, as are some type of audit. Log reviews may be audited to some extent, but trained personnel are still required to act upon any findings. Physical security controls, such as perimeter security and data center security, are also important to implement, maintain, and verify as part of good data integrity; it has long been a principle of industry data security standards and hacker culture that if physical access to just one company system can be obtained, access to all the organization’s electronic data is inevitable. Thus, effective data integrity controls should mix the procedural, the physical, and the logical.

2.9 Keep the Data Integrity Lifecycle Focus

Personnel involved in the implementation of the data integrity program should understand and rely upon data integrity controls that span the entire data life cycle, from initial data creation and/or collection all the way through to eventual data long-term archival and disposition. As the MHRA guidance notes, data integrity is defined as “The extent to which all data are complete, consistent and accurate through the data lifecycle” and the data life cycle is defined as “All phases in the life of the data (including raw data) from initial generation and recording through processing (including transformation or migration), use, data retention, archive/retrieval and destruction.” [3] The data life cycle requires controls from different departments and organizations along its entire length, from creation to eventual disposition. At each stage of its existence – and each point in the life cycle-data needs to have integrity. Once integrity is lost anywhere along this life cycle, integrity is extremely difficult and costly to regain.

Just as a single point of data may cross regulatory and departmental boundaries, so too will the single data point live across multiple systems. A single record required to be retained for ten years is likely to exist on at least two different computerized systems in its lifespan, sit on several different media formats, and be viewed and used by multiple departments (and even multiple companies considering sponsors and business partners). Thus, allowing a data integrity program to spend excessive time on system by system controls is unlikely to serve the purpose of ensuring integrity for regulated data across business processes, across regulation compliance, and across time.

Failing to understand and incorporate data integrity controls across the life cycle of data is like failing to understand and incorporate quality controls across the life cycle of a product. Keeping the focus on the overall data integrity life cycle allows a company to identify and implement appropriate controls. This has the added benefit of minimizing any risk of going overboard in one area only to have insufficient controls elsewhere.

The data integrity life cycle and the need for continuous controls clearly demonstrates why system validation by itself is never enough, why cross-functional action is necessary, why any single group such as IT or RIM cannot be held accountable for the organization’s data integrity, why controls need to be a mix of the procedural, physical and logical (e.g., automated), and why controls at one stage of the data are not sufficient in and of themselves without controls on all the other stages of the data’s life cycle. Assurance of data integrity should be present from beginning to end of the data’s existence in an organization.

3 Sustainability

Corporate programs do not last forever, so building data integrity controls across the company culture is essential. Just as good documentation practices have spread beyond quality systems, companies also need to sustain those practices and routines that result in high quality data. Good data integrity habits engender good data integrity cultures.

While building specific good data integrity routines and processes is beyond the scope of this Concept Paper, it is imperative that data integrity be built into processes and organizational routines. Continued awareness through sharing of current data integrity related information and refresher training involving data integrity concepts would help reinforce the expectations. Keeping data integrity in the forefront will ultimately help achieve a sustainable quality culture where actions and behaviors that support trustworthy and reliable data become second nature to all employees.

4 Conclusion

Although a successfully implemented corporate data integrity program will not create a data integrity paradise, it will go a long way to assure data trustworthiness and reliability, enhance product safety and efficacy, improve business processes, and protect the life science company's compliance status and bottom line. Implementing a successful corporate data integrity program takes forethought, persistence, and insight. This Concept Paper helps to frame the discussion for life sciences companies exploring how to establish data integrity controls across their product life cycle from initial data creation to long-term data disposition. And while there is no one "right way" to implement the many data integrity controls needed, learning from – and building upon – the successes and challenges of others, is a strong way to help assure success.

Note: This Concept Paper touches on only the data integrity requirements and elements that are a part of QMS processes (e.g., policies, standards, procedures, related tools, management review, audits, and validation). These requirements and elements are part of a broader data governance framework that is addressed in a future ISPE/GAMP Good Practice Guide on Electronic Records and Data Integrity under development. The data governance system should be integral to the pharmaceutical quality system. More information associated with this guide will be made available in the coming months.

5 References

1. Deborah Autor, *How to Avoid Warning Letters and Other Troubles with the FDA,* speech at the Joint FDA/FDLI Enforcement and Litigation Conference, Washington, DC, February 2007.

2. Reuters, Ipca hit by FDA ban over Ratlam plant production violations, 23 January 2015, accessed 9 February 2015, http://in.reuters.com/article/2015/01/23/ipca-labs-fda-idINKBN0KW0AP20150123.

3. MHRA, GMP Data Integrity Definitions and Guidance for Industry, Revision 1, January 2015.

4. MHRA, GMP Data Integrity Definitions and Guidance for Industry, Revision 1.1, March 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/412735/Data_integrity_definitions_and_guidance_v2.pdf.

5. FDA, Warning Letter to Novacyl Wuxi Pharmaceutical Co., Ltd., 19 December 2014, accessed 15 January 2015, http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/ucm427976.htm.

6. MHRA, Statement of Non-Compliance with GMP to Wockhardt Limited, 16 January 2015, http://eudragmdp.ema.europa.eu/inspections/gmpc/searchGMPNonCompliance.do.

7. EMA, Italian Medicines Agency Statement of Non-Compliance with GMP to SRI KRISHNA Pharmaceuticals Ltd., 23 December 2014, http://eudragmdp.ema.europa.eu/inspections/gmpc/index.do, http://www.pharmacompass.com/assets/pdf/news/N1.pdf.

8. WHO Prequalification Team – Inspection Services Notice of Concern to Micro Labs Limited, 30 May 2014, http://apps.who.int/prequal/info_applicants/NOC/MicroLabs_NoC_30May2014.pdf

9. FDA, Inspection Guide, Management Controls Subsystem, accessed 15 January 2015, http://www.fda.gov/ICECI/Inspections/InspectionGuides/ucm170207.htm.

10. Jason Finley, "Data Integrity: A Necessity, Not an Option," *InformationWeek: Wall Street & Technology,* July 2014, http://www.wallstreetandtech.com/data-management/data-integrity-a-necessity-not-an-option/a/d-id/1297577.

11. Norton Rose Fulbright LLP, *8th Annual Litigation Trends Survey and Report,* November 2011, http://www.nortonrosefulbright.com/files/us/images/publications/201111018thAnnualLitigationTrendsReportWhatsTrending3.pdf.

12. 21 CFR Part 11 – Electronic Records; Electronic Signatures, US Code of Federal Regulations, U.S. Food and Drug Administration (FDA), www.fda.gov.

13. EudraLex Volume 4 – Guidelines for Good Manufacturing Practices for Medicinal Products for Human and Veterinary Use, Annex 11 – Computerized Systems, June 2011, ec.europa.eu.

14. FDA, Warning Letter to Novacyl Wuxi Pharmaceutical Co., Ltd., 19 December 2014 accessed 15 January 2015, http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/ucm427976.htm.

15. International Council for Harmonisation (ICH), ICH Harmonised Tripartite Guideline, *Quality Risk Management – Q9,* Step 4, 9 November 2005, www.ich.org.

16. See FDA's instructions to its investigators in FDA in its enforcement manuals, specifically the BIMO Attachment A: Computerized Systems, accessed 18 December 2014, http://www.fda.gov/ICECI/EnforcementActions/BioresearchMonitoring/ucm133927.htm.

6 Acronyms and Abbreviations

CEO	Chief Executive Officer
COP	Community of Practice
CGMP	Current Good Manufacturing Practice
CMO	Contract Manufacturing Organization
CRO	Contract Research Organization
DIA	Drug Information Association
EMA	European Medicines Agency
FAQ	Frequently Asked Question
FDA	Food and Drug Administration (US)
FMEA	Failure Mode and Effects Analysis
GCP	Good Clinical Practice
GDP	Good Distribution Practice
GLP	Good Laboratory Practice
GPvP	Good Pharmacovigilance Practice
GxP	Good X Practice (X can mean: Clinical, Laboratory, Manufacturing, Pharmaceutical, etc.)
HACCP	Hazard Analysis and Critical Control Points
ICH	International Council for Harmonisation
ISO	International Organization for Standardization
IT	Information Technology
MHRA	Medicines and Healthcare products Regulatory Agency (UK)
PIC/S	Pharmaceutical Inspection Convention and Pharmaceutical Inspection Co-operation Scheme
RIM	Records and Information Management
SaaS	Software as a Service
SCDM	Society for Clinical Data Management

SIG	Special Interest Group
SME	Subject Matter Expert
SOP	Standard Operating Procedure
QMS	Quality Management System

600 N. Westshore Blvd., Suite 900, Tampa, Florida 33609 USA
Tel: +1-813-960-2105, Fax: +1-813-264-2816

www.ispe.org