Parenteral Drug Association Points to Consider

Elements of a Code of Conduct for Data Integrity

Introduction

Data Integrity has been and currently is a major global concern of Health Authorities and the pharmaceutical industry. Although not a new issue, numerous recent Health Authority enforcement actions such as Warning Letters, Import Alerts, Product Detentions, and suspension or revocation of Marketing Authorizations has focused attention on Data Integrity. Data Integrity can result from lack of awareness of regulatory requirements, employee errors, failure to check accuracy of data, software or system malfunction, or configuration problems with electronic data handling, or malfeasance by employees. To holistically address Data Integrity, the Parenteral Drug Association (PDA) is developing a set of tools in the form of PDA Technical Reports, PDA Training Program, Data Integrity Workshops, and Points to Consider documents that can be used by industry to address this serious issue. This document presents the views of the Parenteral Drug Association (PDA) on the benefits for companies to voluntarily adopt a Code of Conduct for assuring data integrity.

How to Use this Document

This document was developed by a team with expertise in the fields of quality, regulatory affairs, auditing, and manufacturing and reviewed by attorneys specialized in food, drug and labor law. This document is written for easy adoption, in part or in its entirety, by companies, if they so choose, without the need for extensive rewriting of the document. Therefore, the terms ‘shall’ and ‘must’ have been used to permit the Code to be enforceable by a company, if adopted. This document is intended to reinforce a culture of quality and trust within the pharmaceutical industry. It is not intended to be a regulatory standard or guidance, nor is it intended to supersede any country specific or local laws and regulations governing labor, privacy and/or employee rights.

In order for the language used below to be as globally applicable as possible, the document scope has been limited to drug and biological medicinal products. The same or similar concepts could be applied for device and combination products manufacturing. PDA is providing this document and these concepts as a service to members and an example of best practices to the pharmaceutical industry. Please see Section 2 below for more details on how to use this code. Section 3 begins the code of conduct provisions.

Elements of a Code of Conduct for Data Integrity in the Pharmaceutical Industry

1.0 PURPOSE AND SCOPE

1.1 The purpose of this document is to outline the key elements necessary to help ensure the reliability and integrity of information and data throughout all aspects of a product's lifecycle. The Code of Conduct for Data Integrity is intended to apply to employees and officers and third party suppliers and others acting on behalf or at the behest of the company, such as persons that develop, test, manufacture or submit marketing authorizations for pharmaceutical and biological products. Each company will establish their own Policies, Standards, Procedures, Code of Conduct, or other quality system elements that define the requirements for data integrity (including the principles outlined in the Code of Conduct including:

- Manufacturers of finished drug products for clinical trials, bioequivalence studies, and commercial distribution
- Companies that conduct clinical trials in support of new drug applications including, but not limited to: Investigational New Drug (IND), Clinical Trial Application (CTA), Investigational Medicinal Product Dossier (IMPD), Biologics License Application (BLA), Marketing Authorization Application (MAA), New Drug Application (NDA), and Abbreviated New Drug Application (ANDA)
- Laboratories that develop methods or formulations intended to support new drug applications or laboratories that analyze samples generated from clinical trials
- Manufacturers of excipients, intermediates, or active pharmaceutical ingredients (APIs)
- Contract manufacturing organizations (CMOs)
- Contract research organizations (CROs)
- Contract testing laboratories
- Contractors, consultants, suppliers and vendors that provide services and data that support the production and control of APIs, drug or biological products

1.2 The Code of Conduct for Data Integrity is intended to apply to marketing authorization holders and pharmaceutical facilities performing services or providing products that are required to adhere to GXP practices in accordance with applicable laws, regulations and legislative directives of regulatory authorities including:

- Good Manufacturing Practice (GMP)
- Good Clinical Practice (GCP)

- Good Pharmacovigilance Practice (GVP)
- Good Laboratory Practice (GLP)
- Good Distribution Practices (GDP)
- Good Tissue Practice (GTP)

1.3 The principles outlined below are intended to identify key data integrity elements that companies may choose to incorporate into their applicable systems that define the policies, standards and requirements for the conduct of company management and each of its employees. The elements listed below may be used to create a standalone Code of Conduct that is specific to Data Integrity for GXP operations. Alternatively, the identified elements may be incorporated into a broader Code of Conduct that encompasses other aspects of business values and ethics that are beyond data integrity. The data integrity elements may be integrated with existing policies, standards or other documents that define requirements for the conduct of company management and its employees (such as Quality Agreements with supply chain partners).

1.4 Manufactures are responsible for ensuring that quality system elements have been established at each of its third party suppliers that provide products or services on behalf of or at the behest of the manufacturer. Manufacturers need to ensure that suppliers (such as contract laboratories, CROs and CMOs) that operate as an extension of the manufacturer have defined the policies, standards and requirements for the conduct of company management and each of its employees.

2.0 PREAMBLE

2.1 The pharmaceutical industry develops and manufactures drugs and biologics that help patients all over the world live longer, healthier lives. It is a privilege to work in an industry that makes a difference in the lives of patients. Every employee has a duty to engage in conduct to ensure that all stakeholders can trust employee decisions that are based on data and information that are accurate, truthful and complete.

2.2 Senior Management must establish quality standards, requirements and procedures, and is obligated to maintain and monitor the performance of the quality system that helps to ensure availability of safe and effective drugs. The company must maintain operational management oversight to demonstrate that each product has been developed, manufactured or tested under conditions that are designed to assure the reliability and integrity of information and data used to support its quality and fitness for use, and in accordance with applicable laws, regulations and legislative directives of the regulatory authorities. Ensuring data integrity means collecting, documenting, reporting, and

retaining data and information in a manner that accurately, truthfully and completely represents what actually occurred.

2.3 Every employee at each company is responsible for his/her own conduct to maintain a bond of trust between the company and its stakeholders, namely the patients, health care providers, and regulators (i.e., to prevent a broken bond due to data integrity issues). Employees have a duty to perform their GXP functions in an ethical manner that meets company requirements and industry standards as articulated in company requirements, and in accordance with all relevant laws, regulations or legislative directives of regulatory authorities.

2.4 Every employee is required to collect, analyze, report and retain information and data in a manner that accurately, truthfully and completely represents what actually occurred in either paper or electronic format in accordance with the company policies and procedures and applicable law.

2.5 By adopting a voluntary Code of Conduct for Data Integrity (Code of Conduct) senior management is committed, as required by applicable law, to notify applicable licensing/regulatory authority(s) if the company discovers that a pending or approved marketing authorization or other submission to a regulatory authority contains an untrue statement of material fact or omits material facts (e.g. information is false, misleading, inaccurate or incomplete). If data, not submitted, but used to determine whether a product batch met specifications are later found to be false, misleading, inaccurate or incomplete, a company is committed to file the appropriate notifications to health authorities (i.e. Field Alert, Biological Product Deviation Report (BPDR) or notification under the Falsified Medicines Directive(FMD)). Where warranted, management is committed to; (1) providing full disclosure, (2) verifying that a full investigation is conducted, (3) implementing corrective and preventative actions to prevent recurrence, and (4) verifying the validity and reliability of the data and information filed with regulatory agencies. This includes correcting material facts (information and data that were filed previously, if found to be incorrect, untruthful, misleading or incomplete).

3.0 ELEMENTS of a CODE OF CONDUCT FOR DATA INTEGRITY

3.1 Applicability

3.1.1 Each company that develops, tests and manufactures APIs, intermediates, or pharmaceutical and biological products or vendors/suppliers that provide supporting data may adopt a company Code of Conduct for Data Integrity which establishes standards of ethical behavior for all employees and officers of the company.

3.1.2 In support of this code companies will establish programs that: (1) promote an organizational culture that encourages ethical conduct; (2) demonstrates the

company's commitment to compliance with applicable laws; and (3) requires the prevention and detection of data integrity lapses.

3.1.3 The company will establish requirements and implement programs to provide all employees with training on the fundamental principles of Data Integrity including employee conduct as a condition of performing GXP functions. Each employee shall receive annual refresher training on the Code of Conduct for Data Integrity

3.1.4 Each employee will provide annually a signed certification statement confirming that during the past year he/she has adhered to the Code of Conduct for Data Integrity including attestation that he/she has reported to company management wrongful act that raises a question about the integrity of data about which he/she became aware.

3.2 Data Collection, Analysis, Reporting and Retention

3.2.1 The company will establish procedures and documentation systems designed to assure all information and data are collected, analyzed, reported, and retained in a manner that accurately, truthfully and completely represents what actually occurred.

3.2.2 The company shall establish documentation control systems and practices to maintain data integrity as well as providing mechanisms for preventing data integrity lapses and detecting instances of non-compliance. Such systems help to ensure that all raw data from development studies and production and control activities for GXP activities are maintained in bound notebooks or controlled worksheets (pre-numbered approved forms)for paper records or in validated computer systems with appropriate security, audit trails, validation, and oversight for electronic records.

3.2.3 Employees will adhere to the requirements of the established documentation systems and shall not be permitted to record raw data on unofficial forms, writing pads or other uncontrolled media. Such procedures will describe documentation control practices and retention requirements and practices for both paper and electronic records including retention periods that comply with requirements of applicable regulatory authorities. Paper and electronic records shall be retained either as originals or as true copies (such as photocopies) or other accurate reproductions of the original record (such as electronic scanning).

3.2.4 Employees will adhere to established company procedures that describe the documentation control and retention requirements, and applicable laws, regulations and legislative directives of regulatory authorities that apply to paper and electronic documents and records. Employees shall not discard, destroy, or modify in any way raw data or original records (other than at the end of prescribed retention period as provided by approved procedures). Employees shall not delete raw data or alter original records in a manner that obscures or obliterates the original entries. If

changes are needed to correct errors, the original entries shall be retained along with entries that identify the person making the correction, and the date and reason for the correction.

3.2.5 In order to verify paper records of GXP activities, the company shall establish and maintain Signature and Initial Logs for employees that work in GXP areas that include a handwritten specimen of the signature/initials of each employee. Employees must sign or initial original records in a contemporaneous manner, and must enter the date (and time if required by procedure) to accurately reflect who performed or witnessed the activity or who entered results or verified the accuracy of entries. Employees shall never record the signature or initials of another person or pre-date or back date entries on any record (either paper or electronic).

3.2.6 The company shall maintain readily available records for an authorized inspection by regulatory authorities. The company shall provide access to all records that are required by applicable laws, regulations or legislative directives for GXP activities upon request by a duly authorized regulatory official who has the legal authority to inspect such records. Employees shall not delay, deny or limit access to records or refuse to permit inspection by duly authorized officials of regulatory authorities, except as may be specified in a written procedure [e.g., to immediately notify executive management when an inspector arrives].

3.2.7 The company will establish procedures to verify the accuracy, completeness and truthfulness of data and information used to release APIs, finished pharmaceutical products and biological products to the commercial market including verification that the supporting data and information conform to the commitments contained in marketing applications that have been approved by regulatory authorities (where applicable). Employees who perform review batch production and control records as a condition of batch release shall adhere to established procedures and shall confirm that the records supporting batch release have been second person verified for accuracy, truthfulness and completeness.

3.3 Electronic Data Acquisition Systems

3.3.1 If electronic data acquisition systems for GXP data are established, the company must ensure that the systems are configured, validated, and maintained in accordance with established industry standards intended to assure data integrity. The business processes shall include the establishment of written procedures that govern the collection, analysis, reporting and retention of electronic data including:

3.3.1.1 Procedural controls covering the use, correction, and movement of data, ensuring that data can be traced through every phase of its lifecycle. If the transfer of data is authorized, it must be controlled in a manner that

provides traceability and retention for a period of time prescribed by applicable laws, regulations or legislative directives or longer if required by company policies and procedures.

3.3.1.2 Security controls to prevent and detect data deletion, over-writing, manipulation and/or omission of data.

3.3.1.3 Secure date and time stamps to permit detection and to prevent manipulation of records.

3.3.1.4 Secure data retention storage locations to prevent data from being saved to unauthorized file storage locations including removable devices.

3.3.1.5 System and procedural controls to provide for the reporting and evaluation of all data generated.

3.3.2 The company shall establish appropriate security, audit trails, validation, and oversight for electronic records and signatures in compliance with applicable laws, regulations or legislative directives. Electronic records shall be attributable, legible, contemporaneous, traceable, time/date stamped and permanent.

3.3.3 The company will maintain and review audit trails for electronic GXP data that is required by company procedures or regulatory requirement. Such reviews will include periodic review of system audit trail logs against entries in transactional logs to verify that all events and data (including meta data) are being accurately and completely captured, reported and retained.

3.3.4 Employees who enter data or verify data accuracy or perform other activities involving GXP data (such as collection, analysis, reporting or retention functions) shall contemporaneously enter data in accordance with established policies and procedures. Employees shall accurately enter and completely report all required data. Employees shall not engage in any conduct that calls into question the integrity of data (such as falsifying data, making unauthorized changes, or destroying, deleting or over-writing data). Employees who review or evaluate electronic data shall follow established procedures and verify that all required data and information have been included in relevant records and reports. Employees shall always enter data and information in a manner that accurately, truthfully and completely represents what

actually occurred, and includes all testing results (if applicable).

3.4 Electronic Access Security Measures

3.4.1 Any computer data acquisition systems shall be established with secure access to prevent unauthorized changes to electronic data. The company will adopt and strictly enforce procedures that require secure access to computer systems for each computer user who enters data or has access to electronic GXP data. Security measures shall include strict controls to prevent unauthorized access to computer system including use of unique user names and passwords or other biometric means to identify authorized users such as facial recognition, fingerprint readers, and iris scanners.

3.4.2 Consistent with the Code of Conduct for Data Integrity, employees adhere to established procedures that describe requirements of security controls for accessing electronic data. Employees must not disclose and/or share their user name and /or passwords with others, or use the username or password of another person to access computer files.

3.5 Auditing of Quality System for Data Integrity

3.5.1 The company shall establish and execute as part of its internal audit program provisions to periodically evaluate the elements of the quality system used for collecting, analyzing, reporting and retaining information and data.

3.5.2 The audit program will include periodic audits to confirm adherence to established requirements for data integrity. Such shall utilize independent auditors who are qualified by education, experience and training to evaluate data integrity.

3.5.3 Employees who conduct data integrity audits will maintain a current awareness of applicable laws, regulations and legislative directives that pertain to documentation and record keeping requirements.

3.6 Investigations of Wrongful Acts

3.6.1 The company shall establish and follow procedures to investigate any alleged falsification, fabrication, or other conduct that raises a question about the integrity of data. Such investigations shall include a documented in-depth review, conducted in a fair and balanced manner, by independent personnel.

3.6.1.1 Companies may engage legal counsel to help investigators ensure that documents are properly identified and preserved, and that the company receives appropriate advice and counsel regarding the conduct of the investigation. The investigator(s) shall possess the education, experience and training to evaluate data integrity issues.

3.6.1.2 An independent investigation will serve to identify potential gaps in systems, processes, procedures and/or practices by individuals or the organization that could raise a question about data integrity. Such investigations will also serve to assess the legal implications of known or suspected wrongful acts, and possible reporting obligations to regulatory authorities.

3.6.1.3 Independent investigations into conduct that raises a question about the integrity of data shall identify all persons found during the investigation to be involved and describe in detail their actions or activities related to the conduct. Such investigation must determine the scope of the questionable conduct. For example, whether the same or similar conduct or practices may have happened in other instances or could have impacted other data. If so, the investigation needs to be extended to these events, activities, practices and/or other collected data company-wide as well.

3.6.1.4 Company procedures shall contain specific requirements for documenting the investigation, including potential impact on applications and distributed product. company procedures shall also contain specific requirements for reports to senior management and periodic checks to ensure that senior management reporting mechanisms are effective.

3.6.2 Employees shall cooperate with the company during an investigation of an incident, event or test result that does not conform to established requirements. Employees shall provide factual information about any incident/event for which that he/she may have firsthand knowledge. The information and details provided by employees during such investigations shall be accurate, truthful and complete to the best of their knowledge.

3.7 Reporting Wrongful Acts

3.7.1 The company will establish requirements for employees to notify management if they become aware of data falsification, unauthorized change, destruction, or other conduct that calls into question the integrity of data. The notification requirements including reporting mechanism shall be clearly stated in applicable written policies, standards, procedures, code of conduct, or other documents.

3.7.2 Employees shall notify responsible management of the company if they become aware of any potential issue that impacts data integrity such as those attributable to errors, omissions, or wrongful acts regardless of the cause. For example, employees shall immediately notify management if they become aware of or have reason to suspect others have falsified data, made unauthorized changes, destroyed data or other conduct that calls into question the integrity of data. The notification shall follow procedures established in applicable policies, standards, procedures, Code of Conduct, or other documents. Employees shall have the option to report such issues anonymously if they so choose and if local laws permit.

3.7.3 The company will protect from retaliation any employee who notifies responsible management about conduct of other employees that is known or suspected to involve falsification, destruction of data, unauthorized data changes, or other wrongful acts, including non-contemporaneous reporting of data.

3.8 Disciplinary Actions for Employees due to Wrongful Acts

3.8.1 The company shall establish a written policy/standard for disciplinary action when the conduct of an employee calls into question the integrity of data. The company shall inform its employees of its policies/standards for employee conduct including its policy for disciplinary action due to wrongful acts. Any deliberate data falsification, unauthorized change, destruction, or other conduct that calls into question the integrity of data shall be reviewed by responsible management, Human Resources (HR) and Legal against applicable company policies, standards, procedures, Code of Conduct, and applicable laws. Appropriate disciplinary action will be imposed for conduct that is confirmed as not conforming to the applicable written requirements or law(s). Disciplinary action will be based on the nature of the conduct and may include termination of employment when warranted. The company shall document the disciplinary action taken when the conduct of a company employee or third party employee acting on behalf or at the behest of the company is found to be in violation of the company's policy/standards or procedures related to data integrity.

3.8.2 The company shall establish requirements for employees to notify management of known or suspected data integrity problems and shall inform employees that failure to report known or suspected data integrity problems will subject the employee to disciplinary action.

3.9 Notifying Regulatory Authorities about Data Integrity Issues

3.9.1 The company will establish procedures to verify the accuracy and completeness of data and information submitted to regulatory authorities and will establish controls to verify that submissions are made in accordance with laws, regulations or legislative directives of regulatory authorities.

3.9.2 The company is committed to complying with regulatory requirements for submitting data and information to regulatory authorities. In the event that a pending or approved marketing authorization or other submission to a regulatory authority contains (or omits) an untrue statement of material fact the company will promptly notify the applicable regulatory authority(s) as required by applicable law. In such instances the company will take corrective actions needed to confirm the accuracy, completeness and truthfulness of all the data and information contained in the submission(s) and provide the regulatory authority with corrected or additional data or information as applicable. Material facts are the significant or essential evidence that is used to support conformance to the company policies, standards or procedures or conformance to applicable laws, regulations or legislative directives of regulatory authorities. Material facts means the subject matter and information are significant to decisions to be made by the company or Regulatory Authorities who rely on such data and information (as opposed to insignificant, trivial or unimportant details).

3.9.3 Employees must comply with procedures that describe reporting requirements for regulatory authorities, and must immediately notify company management if they become aware that a pending or approved marketing authorization or other submission to a regulatory authority contains an untrue statement of material fact or omits material facts (e.g., information is false, misleading, inaccurate or incomplete).

3.9.4 The company will consult with legal counsel in the event that data integrity lapses are detected but do not involve untrue statements of material fact having been omitted from a pending or approved marketing authorization or other submission to a regulatory authority. Counsel should be experienced with laws, regulations or legislative directives of regulatory authorities. The company, with advice of Counsel, will decide whether self-disclosure of data integrity lapses to regulatory authorities is

prudent for those situations where the laws, regulations or legislative directives of the regulatory authorities do not require notification.

3.10 Data Integrity of Outsourced Services & Purchased Raw Materials

3.10.1 The company shall establish agreements with affiliates, CMOs, service providers or suppliers that define the data integrity requirements that are applicable to the specific raw material supplied or to the activity or services that are provided.

3.10.2 The company will, as part of it Vendor/Supplier Qualification program, confirm that, contractors, vendors or other third party suppliers of products or services who act on behalf or at the behest of the company have established Policies, Standards, Procedures, Code of Conduct, or other documents that define the requirements for data integrity (including the principles outlined in this Code of Conduct for Data Integrity. Employees of Third Party suppliers shall adhere to their own data integrity requirements and take appropriate action to verify the accuracy, truthfulness, and completeness of the data and information provided to its customers.

3.11 Employee Training

3.11.1The company shall establish and maintain an employee learning management system that includes the fundamental training requirements that pertain to documentation of GXP activities including concepts and principles of data integrity such as those contained in the Elements of Code of Conduct for Data Integrity, and how employees are to report suspected data integrity issues to company management. The company must provide all employees with the information and learning needed for employees to understand company requirements for data integrity as well as the requirements of regulatory agencies that relate to their respective GXP job functions.

3.11.2 The company shall establish procedures that require all employees to have received the required training on fundamentals of documentation and data integrity before being permitted to perform GXP activities, and that each employee must receive annual refresher training.

3.11.3 Management shall review at least annually the records of training on fundamentals of documentation and data integrity to confirm that employees received required training before being permitted to perform GXP activities, and to verify that each employee has received annual refresher training.

4.0 GLOSSARY

Data Information derived or obtained from raw data, for example a reported analytical result (MHRA, 2015)

Data Integrity The extent to which all data are complete, consistent and accurate throughout the data lifecycle.

Senior Management are person(s) who direct and control a company or site at the highest levels with the authority and responsibility to mobilise resources within the company or site. (ICH Q10 based in part on ISO 9000:2005)

GXP is a general term to describe any number of good quality practices that are covered by guidelines or regulations where G means "Good", X is a descriptor, and P means "Practice," such as GMP means Good Manufacturing Practices.

Material Facts are crucial to the interpretation of a phenomenon or a subject matter, or to the determination of an issue at hand this is a specific type of confirmed or validated event, item of information, or state of affairs (Black's Law Dictionary, 2nd Ed.)

Meta Data are data used to describe other data. It can be used to describe information such as file type, format, author, user rights, etc. and is usually attached to files, but invisible to the user. (ISPE, GAMP 5)

Quality System is the sum of all aspects of a system that implements quality policy and ensures that quality objectives are met.(ICH Q9)

Raw Data Original records and documentation, retained in the format in which they were originally generated (i.e. paper or electronic), or as a 'true copy'. Raw data must be contemporaneously and accurately recorded by permanent means. In the case of basic electronic equipment which does not store electronic data, or provides only a printed data output (e.g. balance or pH meter), the printout constitutes the raw data. (MHRA, 2015)

Wrongful Act - is any act that may subvert the integrity of the review process. A wrongful act includes, but is not limited to, submitting a fraudulent application, offering or promising a bribe or illegal gratuity, or making an untrue statement of material fact. A wrongful act also includes submitting data that are otherwise unreliable due to, for example, a pattern of errors whether caused by incompetence, negligence, or a practice such as inadequate standard operating procedures or a system-wide failure to ensure the integrity of data submissions. A wrongful act may be evidenced in a document, including informal documents such as correspondence or memoranda, or verbally, such as in telephone conversations or in one-on-one meetings. Regardless of the means, each suspected incident of a wrongful act should be reported and investigated to determine whether they raise significant questions regarding data integrity and

reliability with respect to a regulated product. **[**FDA, "Application Integrity Policy," Mar 5, 1998]