PHARMACEUTICAL INSPECTION CONVENTION
PHARMACEUTICAL INSPECTION CO-OPERATION SCHEME

PI 041-1 (Draft 3)
30 November 2018

PIC/S GUIDANCE

GOOD PRACTICES FOR DATA MANAGEMENT AND INTEGRITY IN REGULATED GMP/GDP ENVIRONMENTS

Editor: PIC/S Secretariat

e-mail: info@picscheme.org
web site: http://www.picscheme.org

TABLE OF CONTENTS

Page

1 DOCUMENT HISTORY

Adoption by Committee of *PI 041-1*	[Date]
Entry into force of *PI 041-1*	[Date]

2 INTRODUCTION

2.1 PIC/S Participating Authorities regularly undertake inspections of manufacturers and distributors of Active Pharmaceutical Ingredient (API) and medicinal products in order to determine the level of compliance with Good Manufacturing Practice (GMP) and Good Distribution Practice (GDP) principles. These inspections are commonly performed on-site however may be performed through the remote or off-site evaluation of documentary evidence, in which case the limitations of remote review of data should be considered.

2.2 The effectiveness of these inspection processes is determined by the veracity of the evidence provided to the inspector and ultimately the integrity of the underlying data. It is critical to the inspection process that inspectors can determine and fully rely on the accuracy and completeness of evidence and records presented to them.

2.3 Good data management practices influence the quality of all data generated and recorded by a manufacturer and these practices should ensure that data is attributable, legible, contemporaneous, original, accurate, complete, consistent, enduring, and available. While the main focus of this document is in relation to GMP/GDP expectations, the principles herein should also be considered in the wider context of good data management such as, data included in the registration dossier based on which API and drug product control strategies and specifications are set.

2.4 Data Integrity is defined as "the extent to which all data are complete, consistent and accurate, throughout the data lifecycle"[1] and is fundamental in a pharmaceutical quality system which ensures that medicines are of the required quality. Poor data integrity practices and vulnerabilities undermine the quality of records and evidence, and may ultimately undermine the quality of medicinal products.

2.5 Good data management practices apply to all elements of the pharmaceutical quality system and the principles herein apply equally to data generated by electronic and paper-based systems.

[1] MHRA GMP Data Integrity Definitions and Guidance for Industry March 2015

2.6 The responsibility for good practices regarding data management and integrity lies with the manufacturer or distributor undergoing inspection. They have full responsibility and a duty to assess their data management systems for potential vulnerabilities and take steps to design and implement good data governance practices to ensure data integrity is maintained.

3 PURPOSE

3.1 This document was written with the aim of:

3.1.1 Providing guidance for inspectorates in the interpretation of GMP/GDP requirements in relation to good data management and the conduct of inspections.

3.1.2 Providing consolidated, illustrative guidance on risk-based control strategies which enable the existing requirements for data integrity and reliability as described in PIC/S Guides for GMP[2] and GDP[3] to be implemented in the context of modern industry practices and globalised supply chains.

3.1.3 Facilitating the effective implementation of good data management elements into the routine planning and conduct of GMP/GDP inspections; to provide a tool to harmonise GMP/GDP inspections and to ensure the quality of inspections with regards to data integrity expectations.

3.2 This guidance, together with inspectorate resources such as aide memoire, should enable the inspector to make an optimal use of the inspection time and an optimal evaluation of data integrity elements during an inspection.

3.3 Guidance herein should assist the inspectorate in planning a risk-based inspection relating to good data management practices.

3.4 Good data management has always been considered an integral part of GMP/GDP. Hence, this guide is not intended to impose additional regulatory burden upon regulated entities, rather it is intended to provide guidance on the interpretation of existing GMP/GDP requirements relating to current industry data management practices.

3.5 The principles of data management and integrity apply equally to paper-based, computerised and hybrid systems and should not place any restraint upon the development or adoption of new concepts or technologies. In accordance with ICH Q10 principles, this guide should facilitate the adoption of innovative technologies through continual improvement.

3.6 The term “Pharmaceutical Quality System” is predominantly used throughout this document to denote the quality management system used to manage and achieve quality objectives. While the term “Pharmaceutical Quality System” is used predominantly by GMP regulated entities, for the purposes of this guidance, it should be regarded as interchangeable with the term “Quality System” used by GDP regulated entities.

4 SCOPE

4.1 The guidance has been written to apply to on-site inspections of those sites performing manufacturing (GMP) and distribution (GDP) activities. The principles within this guide are applicable for all stages throughout the product lifecycle. The guide should be considered as a non-exhaustive list of areas to be considered during inspection.

4.2 The guidance also applies to remote (desktop) inspections of sites performing manufacturing (GMP) and distribution (GDP) activities, although this will be limited

[2] PIC/S PE 009 Guide to Good Manufacturing Practice for Medicinal Products, specifically Part I chapters 4, 5, 6, Part II chapters 5, 6 & Annex 11

[3] PIC/S PE 011 Guide to Good Distribution Practice for Medicinal Products, specifically sections 3, 4, 5 & 6

to an assessment of data governance systems. On-site assessment is normally required for data verification and evidence of operational compliance with procedures.

4.3 Whilst this document has been written with the above scope, many principles regarding good data management practices described herein have applications for other areas of the regulated pharmaceutical and healthcare industry.

4.4 This guide is not intended to provide specific guidance for “for-cause” inspections following detection of significant data integrity vulnerabilities where forensic expertise may be required.

5 DATA GOVERNANCE SYSTEM

5.1 What is data governance?

5.1.1 Data governance is the sum total of arrangements which provide assurance of data quality. These arrangements ensure that data, irrespective of the process, format or technology in which it is generated, recorded, processed, retained, retrieved and used will ensure a attributable, legible, contemporaneous, original, accurate, complete, consistent, enduring, and available record throughout the data lifecycle.

5.1.2 The data lifecycle refers to how data is generated, processed, reported, checked, used for decision-making, stored and finally discarded at the end of the retention period. Data relating to a product or process may cross various boundaries within the lifecycle. This may include data transfer between paper-based and computerised systems, or between different organisational boundaries; both internal (e.g. between production, QC and QA) and external (e.g. between service providers or contract givers and acceptors).

5.2 Data governance systems

5.2.1 Data governance systems should be integral to the pharmaceutical quality system described in PIC/S GMP/GDP. It should address data ownership throughout the lifecycle, and consider the design, operation and monitoring of processes and systems in order to comply with the principles of data integrity, including control over intentional and unintentional changes to, and deletion of information.

5.2.2 The data governance system should ensure controls over the data lifecycle which are commensurate with the principles of quality risk management. These controls may be:

- Organisational
  - procedures, e.g. instructions for completion of records and retention of completed records;
  - training of staff and documented authorisation for data generation and approval;
  - data governance system design, considering how data is generated, recorded, processed, retained and used, and risks or vulnerabilities are controlled effectively;
  - routine data verification;
  - periodic surveillance, e.g. self-inspection processes seek to verify the effectiveness of the data governance system.
- Technical
  - computerised system validation, qualification and control,
  - automation

5.2.3 An effective data governance system will demonstrate Senior management's understanding and commitment to effective data governance practices including the necessity for a combination of appropriate organisational culture and behaviours (section 6) and an understanding of data criticality, data risk and data lifecycle. There should also be evidence of communication of expectations to personnel at all levels within the organisation in a manner which ensures empowerment to report failures and opportunities for improvement. This reduces the incentive to falsify, alter or delete data.

5.2.4 The organisation's arrangements for data governance should be documented within their pharmaceutical quality system and regularly reviewed.

5.3 Risk management approach to data governance

5.3.1 Senior management is responsible for the implementation of systems and procedures to minimise the potential risk to data integrity, and for identifying the residual risk, using the principles of ICH Q9. Contract Givers should perform a review of the contract acceptor's data management policies and control strategies as part of their vendor assurance programme (refer to section 10).

5.3.2 The effort and resource assigned to data governance should be commensurate with the risk to product quality, and should also be balanced with other quality resource demands. All entities regulated in accordance with GMP/GDP principles, (including, but not limited to manufacturers, analytical laboratories, facilities, importers and wholesale distributors) should design and operate a system which provides an acceptable state of control based on the data quality risk, and which is fully documented with supporting rationale.

5.3.3 Where long term measures are identified in order to achieve the desired state of control, interim measures should be implemented to mitigate risk, and should be monitored for effectiveness. Where interim measures or risk prioritisation are required, residual data integrity risk should be communicated to senior management, and kept under review. Reverting from automated and computerised systems to paper-based systems will not remove the need for data governance. Such retrograde approaches are likely to increase administrative burden and data risk, and prevent the continuous improvement initiatives referred to in paragraph 3.5.

5.3.4 Not all data or processing steps have the same importance to product quality and patient safety. Risk management should be utilised to determine the importance of each data/processing step. An effective risk management approach to data governance will consider:

- Data criticality (impact to decision making and product quality) and
- Data risk (opportunity for data alteration and deletion, and likelihood of detection / visibility of changes by the manufacturer's routine review processes).

From this information, risk proportionate control measures can be implemented.

5.4 Data criticality

5.4.1 The decision that data influences may differ in importance and the impact of the data to a decision may also vary. Points to consider regarding data criticality include:

- Which decision does the data influence?

  For example: when making a batch release decision, data which determines compliance with critical quality attributes is normally of greater importance than warehouse cleaning records.

- What is the impact of the data to product quality or safety?

For example: for an oral tablet, API assay data is of generally greater impact to product quality and safety than tablet friability data.

5.5 Data risk

5.5.1 Data risk assessment should consider the vulnerability of data to involuntary alteration, deletion, loss or re-creation or deliberate falsification, and the likelihood of detection of such actions. Consideration should also be given to ensuring complete data recovery in the event of a disaster. Control measures which prevent unauthorised activity, and increase visibility / detectability can be used as risk mitigating actions.

5.5.2 Examples of factors which can increase risk of data failure include complex, inconsistent processes with open ended and subjective outcomes. Simple tasks which are consistent, well defined and objective lead to reduced risk.

5.5.3 Risk assessments should focus on a business process (e.g. production, QC), evaluate data flows and the methods of generating and processing data, and not just consider IT system functionality or complexity. Factors to consider include:

- Process complexity (e.g. multi-stage processes, data transfer between processes or systems, complex data processing);
- Methods of generating, processing, storing and retiring data and the ability to assure data quality and integrity;
- Process consistency (e.g. biological production processes or analytical tests may exhibit a higher degree of variability compared to small molecule chemistry);
- Degree of automation / human interaction
- Subjectivity of outcome / result (i.e. is the process open-ended vs well defined); and
- The outcome of a comparison between electronic system data and manually recorded events could be indicative for malpractices (e.g. apparent discrepancies between analytical reports and raw-data acquisition times).

5.5.4 For computerised systems, manual interfaces with IT systems should be considered in the risk assessment process. Computerised system validation in isolation may not result in low data integrity risk, in particular, if the user is able to influence the reporting of data from the validated system, and system validation does not address the basic requirements outlined in section 9 of this document. A fully automated and validated process together with a configuration that does not allow human intervention, or reduces human intervention to a minimum, is preferable as this design lowers the data integrity risk. Appropriate procedural controls should be installed and verified where integrated controls are not possible for technical reasons.

5.5.5 Critical thinking skills should be used by inspectors to determine whether control and review procedures effectively achieve their desired outcomes. An indicator of data governance maturity is an organisational understanding and acceptance of residual risk, which prioritises actions. An organisation which believes that there is ‘no risk’ of data integrity failure is unlikely to have made an adequate assessment of inherent risks in the data lifecycle. The approach to assessment of data lifecycle, criticality and risk should therefore be examined in detail. This may indicate potential failure modes which can be investigated during an inspection.

5.6 Data governance system review

5.6.1 The effectiveness of data integrity control measures should be assessed periodically as part of self-inspection (internal audit) or other periodic review processes. This should ensure that controls over the data lifecycle are operating as intended.

5.6.2 In addition to routine data verification checks, self-inspection activities should be extended to a wider review of control measures, including:

- A check of continued personnel understanding of good data management practice in the context of protecting of the patient, and ensuring the maintenance of a working environment which is focussed on quality and open reporting of issues, e.g. by review of continued training in good data management principles and expectations.
- A review for consistency of reported data/outcomes against raw data entries.
- In situations where routine computerised system data is reviewed by a validated 'exception report'[4], a risk-based sample of computerised system logs / audit trails to ensure that information of relevance to GMP activity is reported accurately.

5.6.3 An effective review process will demonstrate understanding regarding importance of interaction of company behaviours with organisational and technical controls. The outcome of data governance system review should be communicated to senior management, and be used in the assessment of residual data integrity risk.

6 ORGANISATIONAL INFLUENCES ON SUCCESSFUL DATA INTEGRITY MANAGEMENT

6.1 General

6.1.1 It may not be appropriate or possible to report an inspection citation relating to organisational behaviour. An understanding of how behaviour influences (i) the incentive to amend, delete or falsify data and (ii) the effectiveness of procedural controls designed to ensure data integrity, can provide the inspector with useful indicators of risk which can be investigated further.

6.1.2 Inspectors should be sensitive to the influence of culture on organisational behaviour, and apply the principles described in this section of the guidance in an appropriate way. An effective 'quality culture' and data governance may be different in its implementation from one location to another. Depending on culture, an organisation's control measures may be:

- 'open' (where hierarchy can be challenged by subordinates, and full reporting of a systemic or individual failure is a business expectation)
- 'closed' (where reporting failure or challenging a hierarchy is culturally more difficult)

6.1.3 Good data governance in 'open' cultures may be facilitated by employee empowerment to identify and report issues through the pharmaceutical quality system. In 'closed' cultures, a greater emphasis on oversight and secondary review may be required to achieve an equivalent level of control due to the social barrier of communicating undesirable information. The availability of a confidential escalation process to senior management may also be of greater importance in this situation, and these arrangements should clearly demonstrate that reporting is actively supported and encouraged by senior management.

6.1.4 The extent of Management's knowledge and understanding of data integrity can influence the organisation's success of data integrity management. Management

[4] An 'exception report' is a validated search tool that identifies and documents predetermined 'abnormal' data or actions, which requires further attention or investigation by the data reviewer.

must know their legal and moral obligation (i.e. duty and power) to prevent data integrity lapses from occurring and to detect them, if they should occur. Management should have sufficient visibility and understanding of data integrity risks for paper and computerised (both hybrid and electronic) workflows.

6.1.5 Lapses in data integrity are not limited to fraud or falsification; they can be unintentional and still pose risk. Any potential for compromising the reliability of data is a risk that should be identified and understood in order for appropriate controls to be put in place (refer sections 5.3 - 5.5). Direct controls usually take the form of written policies and procedures, but indirect influences on employee behaviour (such as incentives for productivity in excess of process capability) should be understood and addressed as well.

6.1.6 Data integrity breaches can occur at any time, by any employee, so management needs to be vigilant in detecting issues and understand reasons behind lapses, when found, to enable investigation of the issue and implementation of corrective and preventive actions.

6.1.7 There are consequences of data integrity lapses that affect the various stakeholders (patients, regulators, customers) including directly impacting patient safety and undermining confidence in the organisation and its products. Employee awareness and understanding of these consequences can be helpful in fostering an environment in which quality is a priority.

6.1.8 Management should establish controls to prevent, detect, assess and correct data integrity breaches, as well as verify those controls are performing as intended to assure data integrity. Sections 6.2 to 6.7 outline the key items that Management should address to achieve success with data integrity.

6.2 <u>Code of ethics and policies</u>

6.2.1 A Code of Values & Ethics should reflect Management’s philosophy on quality, achieved through policies (i.e. a Code of Conduct) that are aligned to the quality culture. The Code of Values & Ethics should be written with the intent of developing an environment of trust, where all individuals are responsible and accountable for ensuring patient safety and product quality.

6.2.2 Management should make personnel aware of the importance of their role in ensuring data quality and the implication of their activities to assuring product quality and protecting patient safety.

6.2.3 Code of Conduct policies should clearly define the expectation of ethical behaviour, such as honesty. This should be communicated to and be well understood by all personnel. The communication should not be limited only to knowing the requirements, but also why they were established and the consequences of failing to fulfil the requirements.

6.2.4 Unwanted behaviours, such as deliberate data falsification, unauthorised changes, destruction of data, or other conduct that compromises data quality should be addressed promptly. Examples of unwanted behaviours and attitudes should be documented in the company Code of Conduct policies. Actions to be taken in response to unwanted behaviours should be documented. However, care should be taken to ensure that actions taken, (such as disciplinary actions) do not impede any subsequent investigation. Conforming behaviours should be recognised appropriately.

6.2.5 There should be a confidential escalation program supported by company policy and procedures whereby it encourages personnel to bring instances of possible breaches to the Code of Conduct to the attention of senior management without consequence. The potential for breaches of the Code of Conduct by senior management should be recognised and a suitable reporting mechanism for those cases should be available.

6.3 Quality culture

6.3.1 Management should aim to create a work environment (i.e. quality culture) that is transparent and open, one in which personnel are encouraged to freely communicate failures and mistakes, including potential data reliability issues, so that corrective and preventive actions can be taken. Organisational reporting structure should permit the information flow between personnel at all levels.

6.3.2 It is the collection of values, beliefs, thinking, and behaviours demonstrated consistently by management, team leaders, quality personnel and all personnel that contribute to creating a quality culture to assure data quality and integrity.

6.3.3 Management can foster quality culture by:

- Ensuring awareness and understanding of expectations (e.g. Code of Ethics and Code of Conduct);
- Leading by example, management should demonstrate the behaviours they expect to see ;
- Being accountable for actions and decisions, particularly delegated activities;
- Staying continuously and actively involved in the operations of the business;
- Setting realistic expectations, considering the limitations that place pressures on employees;
- Allocating resources to meet expectations;
- Implementing fair and just consequences and rewards that promote good cultural attitudes towards ensuring data integrity; and
- Being aware of regulatory trends to apply “lessons learned” to the organisation.

6.4 Modernising the Pharmaceutical Quality System

6.4.1 The application of modern quality risk management principles and good data management practices to the current pharmaceutical quality system serves to modernize the System to meet the challenges that come with the generation of complex data.

6.4.2 The company’s pharmaceutical quality system should be able to prevent, detect and correct weaknesses in the system or their processes that may lead to data integrity lapses. The company should know their data life cycle and integrate the appropriate controls and procedures such that the data generated will be valid, complete and reliable. Specifically, such control and procedural changes may be in the following areas:

- Quality Risk Management,
- Investigation programs,
- Data review practices (section 9),
- Computer system validation,
- IT security,
- Vendor/contractor management,
- Training program to include company’s approach to data governance and data governance SOPs ,
- Storage and retrieval of completed records, including out-sourced data storage activities,

- Appropriate oversight of the purchase of GxP critical equipment that incorporate requirements designed to meet data integrity expectations, e.g. User Requirement Specifications, (Refer section 9.2)
- Self-inspection program to include data quality and integrity, and
- Performance indicators (quality metrics) and reporting to senior management.

6.5 Regular management review of Performance indicators (including quality metrics)

6.5.1 There should be regular management reviews of performance indicators, including those related to data integrity, such that significant issues are identified, escalated and addressed in a timely manner. Caution should be taken when key performance indicators are selected so as not to inadvertently result in a culture in which data integrity is lower in priority.

6.5.2 The head of the Quality unit should have direct access to senior management in order to directly communicate risks so that senior management is aware and can allocate resources to address any issues.

6.5.3 Management can have an independent expert periodically verify the effectiveness of their systems and controls.

6.6 Resource allocation

6.6.1 Management should allocate appropriate resources to support and sustain good data integrity management such that the workload and pressures on those responsible for data generation and record keeping do not increase the likelihood of errors or the opportunity to deliberately compromise data integrity.

6.6.2 There should be sufficient number of personnel for quality and management oversight, IT support, conduct of investigations, and management of training programs that are commensurate with the operations of the organisation.

6.6.3 There should be provisions to purchase equipment, software and hardware that are appropriate for their needs, based on the criticality of the data in question. Companies should implement technical solutions that improve compliance with ALCOA+ principles and thus mitigate weaknesses in relation to data quality and integrity.

6.6.4 Personnel must be qualified and trained for their specific duties, with appropriate segregation of duties, including the importance of good documentation practices. There should be evidence of the effectiveness of training on critical procedures, such as electronic data review. The concept of good data management practices applies to all functional departments that play a role in GMP, including areas such as IT and engineering.

6.6.5 Data quality and integrity should be familiar to all, but data quality experts from various levels (SMEs, supervisors, team leaders) may be called upon to work together to conduct/support investigations, identify system gaps and drive implementation of improvements.

6.6.6 Introduction of new roles in an organisation relating to good data management such as a data custodian or Chief Compliance Officer might be considered.

6.7 Dealing with data integrity issues found internally

6.7.1 In the event that data integrity lapses are found, they should be handled as any deviation would be according to the pharmaceutical quality system. It is important to determine the extent of the problem as well as its root cause, then correcting the issue to its full extent and implement preventive measures. This may include the use of a third party for additional expertise or perspective, which may involve a gap assessment to identify weaknesses in the system.

6.7.2 When considering the impact on product, any conclusions drawn should be supported by sound scientific evidence.

6.7.3 Corrections may include product recall, client notification and reporting to regulatory authorities. Corrections and corrective action plans and their implementation should be recorded and monitored.

6.7.4 Further guidance may be found in section 12 of this guide.

7 GENERAL DATA INTEGRITY PRINCIPLES AND ENABLERS

7.1 The Pharmaceutical Quality System (PQS) should be implemented throughout the different stages of the life cycle of the APIs and medicinal products and should encourage the use of science and risk-based approaches.

7.2 To ensure that decision making is well informed and to verify that the information is reliable, the events or actions that informed those decisions should be well documented. As such, Good Documentation Practices (GDocPs) are key to ensuring data integrity, and a fundamental part of a well-designed pharmaceutical quality system (discussed in section 6).

7.3 The application of GDocPs may vary depending on the medium used to record the data (i.e. physical vs. electronic records), but the principles are applicable to both. This section will introduce those key principles and following sections (8 & 9) will explore these principles relative to documentation in both paper-based and electronic-based recordkeeping.

7.4 Some key concepts of GDocPs are summarised by the acronym ALCOA: Attributable, Legible, Contemporaneous, Original, And Accurate. The following attributes can be added to the list: Complete, Consistent, Enduring and Available (ALCOA+[5]). Together, these expectations ensure that events are properly documented and the data can be used to support informed decisions.

[5] EMA guidance for GCP inspections conducted in the context of the Centralised Procedure

7.5 Basic Data Integrity principles applicable to both paper and electronic systems (ALCOA +):

Data Integrity Attribute	Requirement
Attributable	It should be possible to identify the individual or computerised system that performed the recorded task. The need to document who performed the task / function, is in part to demonstrate that the function was performed by trained and qualified personnel. This applies to changes made to records as well: corrections, deletions, changes, etc.
Legible	All records must be legible – the information must be readable in order for it to be of any use. This applies to all information that would be required to be considered Complete, including all Original records or entries. Where the 'dynamic' nature of electronic data (the ability to search, query, trend, etc.) is important to the content and meaning of the record, the ability to interact with the data using a suitable application is important to the 'availability' of the record.
Contemporaneous	The evidence of actions, events or decisions should be recorded as they take place. This documentation should serve as an accurate attestation of what was done, or what was decided and why, i.e. what influenced the decision at that time.
Original	The original record can be described as the first-capture of information, whether recorded on paper (static) or electronically (usually dynamic, depending on the complexity of the system). Information that is originally captured in a dynamic state should remain available in that state.
Accurate	Ensuring results and records are accurate is achieved through many elements of a robust pharmaceutical quality system. This can be comprised of: • equipment-related factors such as qualification, calibration, maintenance and computer validation. • policies and procedures to control actions and behaviours, including data review procedures to verify adherence to procedural requirements • deviation management including root cause analysis, impact assessments and CAPA • trained and qualified personnel who understand the importance of following established procedures and documenting their actions and decisions. Together, these elements aim to ensure the accuracy of information, including scientific data that is used to make critical decisions about the quality of products.
Complete	All information that would be critical to recreating an event is important when trying to understand the event. The level of detail required for an information set to be considered

Data Integrity Attribute	Requirement
	complete would depend on the criticality of the information. (see section 5.4 Data criticality). A complete record of data generated electronically includes relevant metadata (see section 9).
Consistent	Good Documentation Practices should be applied throughout any process, without exception, including deviations that may occur during the process. This includes capturing all changes made to data.
Enduring	Records must be kept in a manner such that they exist for the entire period during which they might be needed. This means they need to remain intact and accessible as an indelible/durable record throughout the record retention period.
Available	Records must be available for review at any time during the required retention period, accessible in a readable format to all applicable personnel who are responsible for their review whether for routine release decisions, investigations, trending, annual reports, audits or inspections.

7.6 If these elements are appropriately applied to all applicable areas of GMP and GDP-related activities, along with other supporting elements of a pharmaceutical quality system, the reliability of the information used to make critical decisions regarding drug products should be adequately assured.

8 SPECIFIC DATA INTEGRITY CONSIDERATIONS FOR PAPER-BASED SYSTEMS

8.1 Structure of Pharmaceutical Quality System (PQS) and control of blank forms/templates/records

8.1.1 The effective management of paper based documents is a key element of GMP/GDP. Accordingly the documentation system should be designed to meet GMP/GDP requirements and ensure that documents and records are effectively controlled to maintain their integrity.

8.1.2 Paper records must be controlled and must remain attributable, legible, contemporaneous, original and accurate, complete, consistent enduring (indelible/durable), and available (ALCOA+) throughout the data lifecycle.

8.1.3 Procedures outlining good documentation practices and arrangements for document control should be available within the PQS. These procedures should specify how data integrity is maintained throughout the lifecycle of the data, including:

- How master documents and procedures are created, reviewed and approved for use;
- Generation, distribution and control of templates used to record data (master, logs, etc.);
- Retrieval and disaster recovery processes regarding records.

- The process for generation of working copies of documents for routine use, with specific emphasis on ensuring copies of documents, e.g. SOPs and blank forms are issued and reconciled for use in a controlled and traceable manner.
- Guidance for the completion of paper based documents, specifying how individual operators are identified, data entry formats and how amendments to documents are recorded. How completed documents are routinely reviewed for accuracy, authenticity and completeness;
- Processes for the filing, retrieval, retention, archival and disposal of records.

8.2 Importance of controlling records

8.2.1 Records are critical to GMP/GDP operations and thus control is necessary to ensure:

- Evidence of activities performed;
- Evidence of compliance with GMP/GDP requirements and company policies, procedures and work instructions;
- Effectiveness of Pharmaceutical Quality System, (PQS);
- Traceability;
- Process authenticity and consistency ;
- Evidence of the good quality attributes of the medicinal products manufactured; and
- In case of complaints or recalls, records could be used for investigational purposes.
- In case of deviations or test failures, records are critical to completing an effective investigation

8.3 Generation, distribution and control of template records

8.3.1 Managing and controlling master records is necessary to ensure that the risk of someone inappropriately using and/or falsifying a record ‘by ordinary means’ (i.e. not requiring the use of specialist fraud skills) is reduced to an acceptable level. The following expectations should be implemented using a quality risk management approach, considering the risk and criticality of data recorded (see section 5.4, 5.5).

8.4 Expectations for the generation, distribution and control of records

	Expectations	**Potential risk of not meeting expectations/items to be checked**
Item:	**Generation**	
1	All documents should have a unique identification number (including the version number) and should be checked, approved, signed and dated. The use of uncontrolled documents should be prohibited by local procedures. The use of temporary recording practices, e.g. scraps of paper should be prohibited.	Uncontrolled documents increase the potential for omission or loss of critical data as these documents may be discarded or destroyed without traceability. In addition, uncontrolled records may not be designed to correctly record critical data. It may be easier to falsify uncontrolled records.

	Expectations	Potential risk of not meeting expectations/items to be checked
		Use of temporary recording practices may lead to data omission, and these temporary original records are not specified for retention If records can be created and accessed without control, it is possible that the records may not have been recorded at the time the event occurred. Risk of using superseded forms if there is no version control or controls for issuance.
2	The document design should provide sufficient space for manual data entries.	Handwritten data may not be clear and legible if the spaces provided for data entry are not sufficiently sized. Documents should be designed to provide sufficient space for comments, e.g. in case of a transcription error, there should be sufficient space for the operator to cross out, initial and date the error, and record any explanation required. If additional pages of the documents are added to allow complete documentation, the number of, and reference to any pages added should be clearly documented on the main record page and signed. Data should not be completed on the reverse (unused side) of existing pages as this would typically be omitted when copied.
3	The document design should make it clear what data is to be provided in entries.	Ambiguous instructions may lead to inconsistent/incorrect recording of data. Ensures all critical data is recorded. Ensures clear, contemporaneous and enduring (indelible/durable) completion of entries. The document should also be structured in such a way as to record information in the same order as the operational process and related SOP, to minimize the risk of inadvertently omitting critical data.
4	Documents should be stored in a manner which ensures appropriate version control. Master copies should contain distinctive marking so to distinguish the master	Inappropriate storage conditions can allow unauthorised modification, use of expired and/or draft documents or cause the loss of master documents. The processes of implementation and the effective communication, by way of

	Expectations	**Potential risk of not meeting expectations/items to be checked**
	from a copy, e.g. use of coloured papers or inks so as to prevent inadvertent use. Master copy (in soft copy) should be prevented from unauthorised or inadvertent changes. E.g.: For the template records stored electronically, the following precautions should be in place: - Access to master templates should be controlled; - process controls for creating and updating versions should be clear and practically applied/verified; - master documents should be stored in a manner which prevents unauthorised changes;	appropriate training prior to implementation when applicable, are just as important as the document.
Item:	**Distribution and Control**	
1	Updated versions should be distributed in a timely manner. Obsolete master documents and files should be archived and their access restricted. Any issued and unused physical documents should be retrieved and reconciled. Where authorised by Quality, recovered copies of documents may be destroyed. However, master copies of authorised documents should be preserved.	There may be a risk that obsolete versions can be used by mistake if available for use.
2	Issue should be controlled by written procedures that include the following controls: - Details of who issued the copies and when they were issued. - using of a secure stamp, or paper colour code not available in the working areas or another appropriate system. - ensuring that only the current approved version is available for use. - allocating a unique identifier to each blank document issued and recording the issue of each document in a register. - Numbering every distributed copy (e.g.: copy 2 of 2) and sequential numbering of issued pages in bound books.	Without the use of security measures, there is a risk that rewriting or falsification of data may be made after photocopying or scanning the template record (which gives the user another template copy to use). Obsolete version can be used intentionally or by error. A filled record with an anomalous data entry could be replaced by a new rewritten template.

	Expectations	**Potential risk of not meeting expectations/items to be checked**
	- Where the re-issue of additional copies of the blank template is necessary, a controlled process regarding re-issue should be followed. All distributed copies should be maintained and a justification and approval for the need of an extra copy should be recorded, e.g.: "the original template record was damaged". - All issued records should be reconciled following use to ensure the accuracy and completeness of records.	All unused forms should be accounted for, and either defaced and destroyed, or returned for secure filing.

8.4.1 An index of all authorised master documents, (SOP's, forms, templates and records should be maintained within the pharmaceutical quality system. This index should mention for each type of template record at least the following information: title, reference number including version number, location (e.g., documentation data base, effective date, next review date, etc.

8.5 Use and control of records located at the point-of-use

8.5.1 Records should be available to operators at the point-of-use and appropriate controls should be in place to manage these records. These controls should be carried out to minimize the risk of damage or loss of the records and ensure data integrity. Where necessary, measures must be taken to protect records from being soiled (e.g. getting wet or stained by materials, etc.).

8.5.2 Records should be appropriately controlled in these areas by designated persons or processes in accordance with written procedures.

8.6 Filling out records

8.6.1 The items listed in the table below should be controlled to assure that a record is properly filled out.

	Expectations	**Specific elements that should be checked / Potential risk of not meeting expectations**
Item	**Completion of records**	
1.	Handwritten entries must be made by the person who executed the task[6]. Unused, blank fields within documents should be crossed-out, dated and signed.	Check that handwriting is consistent for entries made by the same person. Check the entry is legible and clear (i.e. unambiguous; and does not include the use of unknown symbols or abbreviations, e.g. use of ditto (") marks.

[6] Scribes may only be used in exceptional circumstances, refer footnote 7.

	Handwritten entries should be made in clear and legible writing. The completion of date fields should be done in the format defined for the site. E.g. dd/mm/yyyy or mm/dd/yyyy.	Check for completeness of data recorded. Check correct pagination of the records and are all pages present.
2.	Records relating to operations should be completed contemporaneously[7].	Verify that records are available within the immediate areas in which they are used, i.e. Inspectors should expect that sequential recording can be performed at the site of operations. If the form is not available at the point of use, this will not allow operators to fill in records at the time of occurrence.
3.	Records should be enduring (indelible).	Check that written entries are in ink, which is not erasable, and/or will not smudge or fade (during the retention period). Check that the records were not filled out using pencil prior to use of pen (overwriting). Note that some paper printouts from systems may fade over time, e.g. thermal paper. Indelible signed and dated copies of these should be produced and kept with the original record.
4.	Records should be signed and dated using a unique identifier that is attributable to the author.	Check that there are signature and initials logs, that are controlled and current and that demonstrate the use of unique examples, not just standardized printed letters. Ensure that all key entries are signed & dated, particularly if steps occur over time, i.e. not just signed at the end of the page and/or process. The use of personal seals is generally not encouraged; however, where used, seals

[7] The use of scribes (second person) to record activity on behalf of another operator should be considered 'exceptional', and only take place where:

- The act of recording places the product or activity at risk e.g. documenting line interventions by sterile operators.
- To accommodate cultural or staff literacy / language limitations, for instance where an activity is performed by an operator, but witnessed and recorded by a scribe. In these cases, bilingual or controlled translations of documents into local languages and dialect are advised.

In both situations, the scribe recording must be contemporaneous with the task being performed, and must identify both the person performing the observed task and the person completing the record. The person performing the observed task should countersign the record wherever possible, although it is accepted that this countersigning step will be retrospective. The process for a scribe to complete documentation should be described in an approved procedure, which should; specify the activities to which the process applies and assesses the risks associated.

		must be controlled for access. There should be a log which clearly shows traceability between an individual and their personal seal. Use of personal seals must be dated (by the owner), to be deemed acceptable.

8.7 Making corrections on records

Corrections to the records must be made in such way that full traceability is maintained.

Item	How should records be corrected?	Specific elements that should be checked when reviewing records:
1.	Cross out what is to be changed with a single line. Where appropriate, the reason for the correction must be clearly recorded and verified if critical. Initial and date the change made.	Check that the original data is readable not obscured (e.g.: not obscured by use of liquid paper; overwriting is not permitted) If changes have been made to critical data entries, verify that a valid reason for the change has been recorded and that supporting evidence for the change is available. Check for unexplained symbols or entries in records
2.	Corrections must be made in indelible ink.	Check that written entries are in ink, which is not erasable, and/or will not smudge or fade (during the retention period). Check that the records were not filled out using pencil prior to use of pen (overwriting).

8.8 Verification of records (secondary checks)

Item	When and who should verify the records?	Specific elements that should be checked when reviewing records:
1.	A- Records of critical process steps, e.g. critical steps within batch records, should be: - reviewed/witnessed by designated personnel (e.g.: production supervisor) at the time of operations occurring; and - reviewed by an authorised person within the production department	Verify the process for the handling of production records within processing areas to ensure they are readily available to the correct personnel at the time of performing the activity to which the record relates. Verify that any secondary checks performed during processing were performed by appropriately qualified

	before sending them to the Quality Assurance unit ; and - reviewed and approved by the Quality Assurance Unit (e.g. Authorised Person / Qualified Person) before release or distribution of the batch produced. B- Batch production records of non-critical process steps is generally reviewed by production personnel according to an approved procedure. C- Laboratory records for testing steps should also be reviewed by designated personnel (e.g.: second analysts) following completion of testing. Reviewers are expected to check all entries, critical calculations, and undertake appropriate assessment of the veracity of test results in accordance with data-integrity principles. This verification must be conducted after performing production-related tasks and activities. This verification must be signed or initialled and dated by the appropriate persons. Local SOPs must be in place to describe the process for review of written documents.	and independent personnel, e.g. production supervisor or QA. Check that documents were reviewed by production personnel and then quality assurance personnel following completion of operational activities.
	How should records be verified?	**Specific elements that should be checked when reviewing records:**
2.	Check that all the fields have been completed correctly using the current (approved) templates, and that the data was critically compared to the acceptance criteria. Check items 1, 2, 3, and 4 of section 8.6 and Items 1 and 2 of section 8.7.	Inspectors should review company procedures for the review of manual data to determine the adequacy of processes. The need for, and extent of a secondary check should be based on quality risk management principles, based on the criticality of the data generated. Check that the secondary reviews of data include a verification of any calculations used. View original data (where possible) to confirm that the correct data was transcribed for the calculation.

8.9 Direct print-outs from electronic systems

8.9.1 Some very simple electronic systems, e.g. balances, pH meters or simple processing equipment which do not store data, generate directly-printed paper records. These types of systems and records provide limited opportunity to influence the presentation of data by (re-)processing, changing of electronic date/time stamps. In these circumstances, the original record should be signed and dated by the person generating the record and information to ensure traceability, such as sample ID, batch number, etc. should be recorded on the record. These original records should be attached to batch processing or testing records.

8.9.2 Consideration should be given to ensuring these records are enduring, (see section 8.6.1).

8.10 True copies

8.10.1 Copies of original paper records (e.g. analytical summary reports, validation reports etc.) are generally very useful for communication purposes, e.g. between companies operating at different locations. These records must be controlled during their life cycle to ensure that the data received from another site (sister company, contractor etc.) are maintained as “true copies” where appropriate, or used as a “summary report” where the requirements of a “true copy” are not met (e.g. summary of complex analytical data).

8.10.2 It is conceivable for raw data generated by electronic means to be retained in an acceptable paper or pdf format, where it can be justified that a static record maintains the integrity of the original data. However, the data retention process must record all data, (including metadata) for all activities which directly or indirectly impact on all aspects of the quality of medicinal products, (e.g. for records of analysis this may include: raw data, metadata, relevant audit trail and result files, software / system configuration settings specific to each analytical run, and all data processing runs (including methods and audit trails) necessary for reconstruction of a given raw data set). It would also require a documented means to verify that the printed records were an accurate representation. This approach is likely to be onerous in its administration to enable a GMP/GDP compliant record.

8.10.3 Many electronic records are important to retain in their dynamic format, to enable interaction with the data. Data must be retained in a dynamic form where this is critical to its integrity or later verification. Risk management principles should be utilised to support and justify whether and how long data should be stored in a dynamic format.

8.10.4 At the receiving site, these records (true copies) may either be managed in a paper or electronic format (e.g., PDF) and should be controlled according to an approved QA procedure.

8.10.5 Care should be taken to ensure that documents are appropriately authenticated as “true copies” either through the use of handwritten or electronic signatures.

Item	How should the “true copy” be issued and controlled?	Specific elements that should be checked when reviewing records:
1.	Creating a “true copy” of a paper document. At the company who issues the true copy: - Obtain the original of the document to be copied - Photocopy the original document ensuring that no information from the original copy is lost;	Verify the procedure for the generation of true copies, and ensure that the generation method is controlled appropriately. Check that true copies issued are identical (complete and accurate) to original records. Copied records

	- Verify the authenticity of the copied document and sign and date the new hardcopy as a “true copy”; The “True Copy” may now be sent to the intended recipient. Creating a “true copy” of an electronic document. A ‘true copy’ of an electronic record should be created by electronic means (electronic file copy), including all required metadata. Creating pdf versions of electronic data should be discouraged, as this is equivalent to a printout from the electronic system, which risks loss of metadata. The “True Copy” may now be sent to the intended recipient. A distribution list of all issued “true copies” (soft/hard) should be maintained.	should be checked against the original document records to make sure there is no tampering of the scanned image. Check that scanned or saved records are protected to ensure data integrity. After scanning paper records and verifying creation of a ‘true copy’, the original documents from which the scanned images have been created should be retained for the respective retention periods by the record owner.
2.	At the company who receives the true copy: - The paper version, scanned copy or electronic file should be reviewed and filed according to good document management processes. The document should clearly indicate that it is a true copy and not an original record.	Check that received records are checked and retained appropriately. A system should be in place to verify the authenticity of “true copies” e.g. through verification of the correct signatories.

8.10.6 A quality agreement should be in place to address the responsibilities for the generation and transfer of “true copies” and data integrity controls. The system for the issuance and control of “true copies” should be audited by the contract giver and receiver to ensure the process is robust and meets data integrity principles.

8.11 Limitations of remote review of summary reports

8.11.1 The remote review of data within summary reports is a common necessity; however, the limitations of remote data review must be fully understood to enable adequate control of data integrity.

8.11.2 Summary reports of data are often supplied between physically remote manufacturing sites, Market Authorisation Holders and other interested parties. However, it must be acknowledged that summary reports are essentially limited in their nature, in that critical supporting data and metadata is often not included and therefore original data cannot be reviewed.

8.11.3 It is therefore essential that summary reports are viewed as but one element of the process for the transfer of data and that interested parties and inspectorates do not place sole reliance on summary report data.

8.11.4 Prior to acceptance of summary data, an evaluation of the supplier’s quality system and compliance with data integrity principles should be established through on-site inspection when considered important in the context of quality risk management. The inspection should assure the veracity of data generated by the company, and include a review of the mechanisms used to generate and distribute summary data and reports.

8.11.5 Summary data should be prepared in accordance with agreed procedures and reviewed and approved by authorised staff at the original site. Summaries should be accompanied with a declaration signed by the Authorised Person stating the authenticity and accuracy of the summary. The arrangements for the generation, transfer and verification of summary reports should be addressed within quality/technical agreements.

8.12 Document retention (Identifying record retention requirements and archiving records)

8.12.1 The retention period of each type of records should (at a minimum) meet those periods specified by GMP/GDP requirements. Consideration should be given to other local or national legislation that may stipulate longer storage periods.

8.12.2 The records can be retained internally or by using an outside storage service subject to quality agreements. In this case, the data centre's locations should be identified. A risk assessment should be available to demonstrate retention systems/facilities/services are suitable and that the residual risks are understood.

Item	Where and how should records be archived?	Specific elements that should be checked when reviewing records:
1.	A system should be in place describing the different steps for archiving records (identification of archive boxes, list of records by box, retention period, archiving location etc.). Instructions regarding the controls for storage, as well as access and recovery of records should be in place. Systems should ensure that all GMP/GDP relevant records are stored for periods that meet GMP/GDP requirements[8].	Check that the system implemented for retrieving archived records is effective and traceable. Check if the records are stored in an orderly manner and are easily identifiable. Check that records are in the defined location and appropriately secured. Check that access to archived documents is restricted to authorised personnel ensuring integrity of the stored records. Check for the presence of records of accessing and returning of records The storage methods used should permit efficient retrieval of documents when required.
2	All hardcopy quality records should be archived in: - secure locations to prevent damage or loss; - such a manner that it is easily traceable and retrievable. - a manner that ensures that records are durable for their archived life	Check for the outsourced archived operations if there is a quality agreement in place and if the storage location was audited. Ensure there is some assessment of ensuring that documents will still be

[8] Note that storage periods for some documents may be dictated by other local or national legislation.

		legible/available for the entire archival period. In case of printouts which are not permanent (e.g. thermal transfer paper) a verified ('true') copy should be retained, along with the non- permanent original. Verify whether the storage methods used permit efficient retrieval of documents when required.
3.	All records should be protected from damage or destruction by: - fire; - liquids (e.g. water, solvents and buffer solution); - rodents; - humidity etc. - unauthorised personnel access, who may attempt to amend, destroy or replace records	Check if there are systems in place to protect records (e.g. pest control and sprinklers). Note: Sprinkler systems can be implemented provided that they are designed to prevent damage to documents, e.g. documents are protected from water (e.g. by covering them with plastic film).
4	Strategy for disaster recovery	Check for system is in place for the recovery of records in a disaster situation

8.13 Disposal of original records

8.13.1 A documented process for the disposal of records should be in place to ensure that the correct original records are disposed of after the defined retention period. The system should ensure that current records are not destroyed by accident and that historical records do not inadvertently make their way back into the current record stream (e.g. Historical records confused/mixed with existing records.)

8.13.2 A record/register should be available to demonstrate appropriate and timely archiving or destruction of retired records in accordance with local policies.

8.13.3 Measures should be in place to reduce the risk of deleting the wrong documents. The access rights allowing deletion of records should be limited to few persons.

9 SPECIFIC DATA INTEGRITY CONSIDERATIONS FOR COMPUTERISED SYSTEMS

9.1 Structure of the QMS and control of computerised systems

9.1.1 A large variety of computerised systems are used by companies to assist in a significant number of operational activities. These range from the simple standalone to large integrated and complex systems, many of which have an impact on the quality of products manufactured. It is the responsibility of each regulated entity to fully evaluate and control all computerised systems and manage them in accordance with GMP[9] and GDP[10] requirements.

9.1.2 Organisations should be fully aware of the nature and extent of computerised systems utilised, and assessments should be in place that describe each system, its intended use and function, and any data integrity risks or vulnerabilities that may be susceptible to manipulation. Particular emphasis should be placed on determining the criticality of computerised systems and any associated data, in respect of product quality.

9.1.3 All computerised systems with potential for impact on product quality should be effectively managed under a mature pharmaceutical quality system which is designed to ensure that systems are protected from acts of accidental or deliberate manipulation, modification or any other activity that may impact on data quality and integrity.

9.1.4 The processes for the design, evaluation, and selection of computerised systems should include appropriate consideration of the data management and integrity aspects of the system. Regulated users should ensure that new systems include appropriate controls to ensure effective data management. Legacy systems are expected to meet the same basic requirements; however, full compliance may necessitate the use of additional controls, e.g. supporting administrative procedures or supplementary security hardware/software.

9.1.5 When determining data vulnerability and risk, it is important that the computerised system is considered in the context of its use within the business process. For example, the integrity of results generated by an analytical method, utilising an integrated computer interface is affected by sample preparation, entry of sample weights into the system, use of the system to generate data, and processing / recording of the final result using that data. The creation and assessment of a data flow map may be useful in understanding the risks and vulnerabilities of computerised systems, particularly interfaced systems.

9.1.6 The guidance herein is intended to provide specific considerations for data integrity in the context of computerised systems. Further guidance regarding good practices for computerised systems may be found in the PIC/S Good Practices for Computerised Systems in Regulated "GxP" Environments (PI 011).

9.2 Qualification and validation of computerised systems

9.2.1 The qualification and validation of computerised systems should be performed in accordance with the relevant GMP/GDP guidelines; the tables below provide clarification regarding specific expectations for ensuring good data governance practices for computerised systems.

9.2.2 Users should be aware that validation alone does not necessarily guarantee that records generated are necessarily adequately protected and validated systems may be vulnerable to loss and alteration by accidental or malicious means. Thus, validation should be supplemented by appropriate administrative and physical controls, as wells as training and education of users.

[9] PIC/S PE 009 Guide to Good Manufacturing Practice for Medicinal Products, specifically Part I chapters 4, Part II chapters 5, & Annex 11

[10] PIC/S PE 011 GDP Guide to Good Distribution Practice for Medicinal Products, specifically section 3.5

	Expectations	Potential risk of not meeting expectations/items to be checked
Item:	**System Validation & Maintenance**	
1	Regulated companies should implement appropriate systems to ensure that data management and integrity requirements are considered in the initial stages of system procurement and throughout system and data lifecycle. For GMP regulated users, Annex 15 requirements such as Functional Specifications (FS) and/or User Requirement Specifications (URS) should adequately address data management and integrity. Specific attention should be paid to the purchase of GxP critical equipment to ensure that systems are appropriately evaluated for data integrity controls prior to purchase. Legacy systems in use should be evaluated to determine whether existing system configuration and functionality permits the appropriate control of data in accordance with good data management and integrity practices. Where system functionality or design of these systems does not provide an appropriate level of control, additional controls should be considered and implemented.	Inadequate consideration of DI requirements may result in the purchase of software systems that do not include the basic functionality required to meet data management and integrity expectations. Inspectors should verify that the implementation of new systems followed a process that gave adequate consideration to DI principles. Some legacy systems may not include appropriate controls for data management, which may allow the manipulation of data with a low probability of detection. Assessments of existing systems should be available and provide an overview of any vulnerabilities and list any additional controls implemented to assure data integrity. Additional controls should be appropriately validated.
2	Regulated users should have an inventory of all computerised systems in use. This list should include reference to: - The name, location and primary function of each computerised system; - Assessments of the function and criticality of the system and associated data; (e.g. direct GMP/GDP impact, indirect impact, none) - The current validation status of each system and reference to existing validation documents. Risk assessments should be in place for each system, specifically assessing the necessary controls to ensure data integrity. The level and extent of validation of controls for data integrity should be determined based on the criticality of the system and process and potential risk to product quality, e.g. processes or systems that generate or control batch release data would generally require greater control than	Companies that do not have adequate visibility of all computerised systems in place may overlook the criticality of systems and may thus create vulnerabilities within the data lifecycle. An inventory list serves to clearly communicate all systems in place and their criticality, ensuring that any changes or modifications to these systems are controlled. Verify that risk assessments are in place for critical processing equipment and data acquisition systems. A lack of thorough assessment of system impact may lead to a lack of appropriate validation and system control. Examples of critical systems to review include: Systems used to control the purchasing and status of products and materials;

	Expectations	Potential risk of not meeting expectations/items to be checked
	those systems managing less critical data or processes. Consideration should also be given to those systems with higher potential for disaster, malfunction or situations in which the system becomes inoperative. Assessments should also review the vulnerability of the system to inadvertent or unauthorised changes to critical configuration settings or manipulation of data. All controls should be documented and their effectiveness verified.	Systems for the control and data acquisition for critical manufacturing processes; Systems that generate, store or process data that is used to determine batch quality; Systems that generate data that is included in the Batch processing or packaging records; Systems used in the decision process for the release of products.
3	A Validation Summary Report for each computerised system (written and approved in accordance with Annex 15 requirements) should be in place and state (or provide reference to) at least the following items: - Critical system configuration details and controls for restricting access to configuration and any changes (change management). - A list of all currently approved normal and administrative users specifying the username and the role of the user. - Frequency of review of audit trails and system logs. - Procedures for: o how a new system user is created; o the process for the modification (change of privileges) for an existing user; o defining the combination/format of passwords for each system the process of reviewing and deleting users; o arrangements for back-up and frequency; o A reference to the disaster recovery procedure; o Process and responsibilities for data archiving, including procedures for accessing and reading archived data; o Approved locations for data storage. - The report should explain how the original data are retained with relevant metadata in a form that permits the reconstruction of the	Check that validation systems and reports specifically address data integrity requirements following GMP/GDP requirements and considering ALCOA principles. System configuration and segregation of duties (e.g. authorisation to generate data should be separate to authorisation to verify data) should be defined prior to validation, and verified as effective during testing. Check the procedures for system access to ensure modifications or changes to systems are restricted and subject to change control management. Ensure that system administrator access is restricted to authorised persons and is not used for routine operations. Check the procedures for granting, modifying and removing access to computerised systems to ensure these activities are controlled. Check the currency of user access logs and privilege levels, there should be no unauthorised users to the system and access accounts should be kept up to date. There should also be restrictions to prevent users from amending audit trail functions.

	Expectations	Potential risk of not meeting expectations/items to be checked
	manufacturing process or the analytical activity.	
4	Companies should have a Validation Master Plan in place that includes specific policies and validation requirements for computerised systems and the integrity of such systems and associated data. The extent of validation for computerised systems should be determined based on risk. Further guidance regarding assessing validation requirements for computerised systems may be found in PI 011. Before a system is put into routine use, it should be challenged with defined tests for conformance with the acceptance criteria. It would be expected that a prospective validation for computerised systems is conducted. Appropriate validation data must be available for systems already in-use. Computer system validation should be designed according to GMP Annex 15 with URS, FAT, SAT, IQ, OQ and PQ tests. Qualification testing includes Design Qualification (DQ); Installation qualification (IQ); Operational Qualification (OQ); and Performance Qualification (PQ). In particular, specific tests should be designed in order to challenge those areas where data quality or integrity is at risk. Companies should ensure that computerised systems are qualified for their intended use. Companies should therefore not place sole reliance on vendor qualification packages; validation exercises should include specific tests to ensure data integrity is maintained during operations that reflect normal and intended use. The number of tests should be guided by a risk assessment but the critical	Check that validation documents include specific provisions for data integrity; validation reports should specifically address data integrity principles and demonstrate through design and testing that adequate controls are in place. Unvalidated systems may present a significant vulnerability regarding data integrity as user access and system configuration may allow data amendment. Check that end-user testing includes test-scripts designed to demonstrate that software not only meets the requirements of the vendor, but is fit for its intended use.

	Expectations	Potential risk of not meeting expectations/items to be checked
	functionalities should be at least identified and tested, e.g., certain PLCs and systems based on basic algorithms or logic sets, the functional testing may provide adequate assurance of reliability of the computerised system. For critical and/or more complex systems, detailed verification testing is required during IQ, OQ & PQ stages.	
5	Periodic System Evaluation Computerised systems should be evaluated periodically in order to ensure continued compliance with respect to Data Integrity controls. The evaluation should include deviations, changes (including any cumulative effect of changes), upgrade history, performance and maintenance, and assess whether these changes have had any detrimental effect on data management and integrity controls. The frequency of the re-evaluation should be based on a risk assessment depending on the criticality of the computerised systems considering the cumulative effect of changes to the system since last review. The assessment performed should be documented.	Check that re-validation reviews for computerised systems are outlined within validation schedules. Verify that systems have been subject to periodic review, particularly with respect to any potential vulnerabilities regarding data integrity. Any issues identified, such as limitations of current software/hardware should be addressed in a timely manner and corrective and preventive actions, and interim controls should be available and implemented to manage any identified risks.
6	Operating systems and network components should be updated in a timely manner according to vendor recommendations and migration of applications from older to newer platforms should be planned and conduced in advance of the time before the platforms reach an unsupported state which may affect the management and integrity of data generated by the system. Security patches for operating systems and network components should be applied in a controlled and timely manner according to vendor recommendations in order to maintain data security. Where unsupported operating systems are maintained, i.e. old operating systems are used even after they run out of support by the vendor or supported versions are not security patched, the systems (servers) should be isolated as	Verify that system updates are performed in a controlled and timely manner. Older systems should be reviewed critically to determine whether appropriate data integrity controls are integrated, or, (where integrated controls are not possible) that appropriate administrative controls have been implemented and are effective.

	Expectations	Potential risk of not meeting expectations/items to be checked
	much as possible from the rest of the network. Remaining interfaces and data transfer to/from other equipment should be carefully designed, configured and qualified to prevent exploitation of the vulnerabilities caused by the unsupported operating system. Due to their inherent vulnerability, unsupported systems should not be accessible remotely.	

	Expectations	Potential risk of not meeting expectations/items to be checked
Item:	**Data transfer between systems**	
1	Interfaces should be assessed and addressed during validation to ensure the correct and complete transfer of data. Interfaces should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimise data integrity risks. Verification methods may include the use of: ○ Secure transfer ○ Encryption ○ Check sums Where applicable, interfaces between systems should be designed and qualified to include an automated transfer of GxP data.	Interfaces between computerised systems present a risk whereby data may be inadvertently lost, amended or transcribed incorrectly during the transfer process. Ensure data is transferred directly to the secure location/database and not simply copied from the local drive (where it may have the potential to be altered). Temporary data storage on local computerised systems (e.g. instrument computer) before transfer to final storage or data processing location creates an opportunity for data to be deleted or manipulated. This is a particular risk in the case of 'standalone' (non-networked) systems. Ensure the environment that initially stores the data has appropriate DI controls in place. Well designed and qualified automated data transfer is much more reliable than any manual data transfer conducted by humans.
2	Where system software is installed or updated, the user should ensure that archived data can be read by the new software. Where necessary this may require conversion of existing archived data to the new format. Where conversion to the new data format of the new software is not possible, the old software should be maintained installed in one computer and also available as a backup media in order to have the opportunity to read the archived data in case of an investigation.	It is important that data is readable in its original form throughout the data lifecycle, and therefore users must maintain the readability of data, which may require maintaining access to superseded software.

9.3 System security for computerised systems

	Expectations	Potential risk of not meeting expectations / items to be checked
Item:	System security	
1	User access controls shall be configured and enforced to prohibit unauthorised access to, changes to and deletion of data. The extent of security controls is dependent on the criticality of the computerised system. For example: - Individual Login IDs and passwords should be set up and assigned for all staff needing to access and utilise the specific electronic system. Shared login credentials do not allow for traceability to the individual who performed the activity. For this reason, shared passwords, even for reasons of financial savings, must be prohibited. - Input of data and changes to computerised records must be made only by authorised personnel. Companies should maintain a list of authorised individuals and their access privileges for each electronic system in use. - Appropriate controls should be in place regarding the format and use of passwords, to ensure that systems are effectively secured. - Upon initially having been granted system access, a system should allow the user to create a new password, following the normal password rules. - Systems should support different user access roles (levels) and assignment of a role should follow the least-privilege rule, i.e. assigning the minimum necessary access level for any job function. As a minimum, simple systems should have normal and admin users, but more for complex systems will typically requires more levels of users (a hierarchy) to effectively support access control.	Check that the company has taken all reasonable steps to ensure that the computerised system in use is secured, and protected from deliberate or inadvertent changes. Systems that are not physically and administratively secured are vulnerable to data integrity issues. Inspectorates should confirm that verified procedures exist that manage system security, ensuring that computerised systems are maintained in their validated state and protected from manipulation. It is acknowledged that some computerised systems support only a single user login or limited numbers of user logins. Where no suitable alternative computerised system is available, equivalent control may be provided by third party software, or a paper based method of providing traceability (with version control). The suitability of alternative systems should be justified and documented. Increased data review is likely to be required for hybrid systems. Inspectors should verify that a password policy is in place to ensure that systems enforce good password rules and require strong passwords. Consideration should be made to using stronger passwords for systems generating or processing critical data. Systems where a new password cannot be changed by the user, but can only be created by the admin, are incompatible with data integrity, as the confidentiality of passwords cannot be maintained. Check that user access levels are appropriately defined, documented and controlled. The use of a single user access level on a system and assigning all users this role, which per definition will be the admin role, is not acceptable. Verify that the system uses authority checks to ensure that only authorized

	Expectations	Potential risk of not meeting expectations / items to be checked
	- Granting of administrator access rights to computer systems and infrastructure used to run GxP critical applications should be strictly controlled. Administrator access rights should not be given to normal users on the system (i.e. segregation of duties). - Normal users should not have access to critical aspects of the computer system, e.g. system clocks, file deletion functions, etc. - Systems should be able to generate a list of users with actual access to the system, including user names and roles. The list should be used during periodic user reviews. - Systems should be able to generate a list of successful and unsuccessful login attempts, including: o User name o User role o Date and time of the attempt o Session length (successful attempts) - User access controls should ensure strict segregation of duties, i.e. that all users on a system, who are conducting normal work tasks, should have only normal access rights. Normally, users with elevated access rights (e.g. admin) should not conduct normal work tasks on the system. - System administrators should normally be independent from users performing the task, and have no involvement or interest in the outcome of the data generated or available in the electronic system. For example, QC supervisors and managers should not be assigned as the system administrators for electronic systems in their laboratories (e.g., HPLC, GC, UV-Vis). Typically, individuals outside of the quality and production organisations (e.g., Information Technology administrators) should serve as	individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

	Expectations	Potential risk of not meeting expectations / items to be checked
	the system administrators and have enhanced permission levels. - For smaller organisations, it may be permissible for a nominated person in the quality unit or production department to hold access as the system administrator; however, in these cases the administrator access should not be used for performing routine operations and the user should hold a second and restricted access for performing routine operations. In these cases all administrator activities conducted should be recorded and approved within the quality system. - Any request for new users, new privileges of users should be authorised by appropriate personnel (e.g. line manager and system owner) and forwarded to the system administrator in a traceable way in accordance with a standard procedure. - Computer systems giving access to GxP critical data or operations should have an inactivity logout, which, either at the application or the operating system level, logs out a user who has been inactive longer than a predefined time. The time should be shorter, rather than longer and should typically be set to prevent unauthorised access to systems. Upon activation of the inactivity logout, the system should require the user to go through the normal authentication procedure to login again.	
2	Computerised systems must be protected from accidental changes or deliberate manipulation. Companies should assess systems and their design to prevent unauthorised changes to validated settings that may ultimately affect data integrity. Consideration should be given to: - The physical security of computerised system hardware:	Check that access to hardware and software is appropriately secured, and restricted to authorised personnel. Verify that suitable authentication methods are implemented. These methods should include user IDs and passwords but other methods are possible and may be required. However, it is essential that users are positively identifiable.

	Expectations	Potential risk of not meeting expectations / items to be checked
	o Location of and access to servers; o Restricting access to PLC modules, e.g. by locking access panels. o Physical access to computers, servers and media should be restricted to authorized individuals. Users on a system should not normally have access to servers and media. - Vulnerability of networked systems from local and external attack; - Remote network updates, e.g. automated updating of networked systems by the vendor. - Security of system settings, configurations and key data. Access to critical data/operating parameters of systems must be appropriately restricted and any changes to settings/configuration controlled through change management processes by authorised personnel. - The system clock should be synchronized with the clock of connected systems and access restricted to authorised personnel. - Firewalls should be setup to protect critical data and operations. Port openings (firewall rules) should be based on the least privilege policy, making the firewall rules as tight as possible and thereby allowing only permitting traffic.	For remote authentication to systems containing critical data available via the internet (e.g. cloud solutions); verify that additional authentication are employed such as the use of pass code tokens or biometrics. Verify that access to key operational parameters for systems is appropriately controlled and that, where appropriate, systems enforce the correct order of events and parameters in critical sequences of GxP steps.
	Firewall Review Firewall rules should be subject to periodic reviews against specifications in order to ensure that they are set as restrictive as necessary, allowing only permitted traffic. The reviews should be documented.	Firewall rules are typically subject to changes over time, e.g. temporary opening of ports due to maintenance on servers etc. If never reviewed, firewall rules may become obsolete permitting unwanted traffic or intrusions.

	Expectations	**Potential risk of not meeting expectations / items to be checked**
3	Electronic signatures used in the place of handwritten signatures must have appropriate controls to ensure their authenticity and traceability to the specific person who electronically signed the record(s). Electronic signatures must be permanently linked to their respective record, i.e. if a later change is made to a signed record; the record must indicate the amendment and appear as unsigned. Where used, electronic signature functionality must automatically log the date and time when a signature was applied. The use of advanced forms of electronic signatures is becoming more common, e.g., the use of biometrics is becoming more prevalent by firms. The use of advanced forms of electronic signatures should be encouraged.	Check that electronic signatures are appropriately validated, their issue to staff is controlled and that at all times, electronic signatures are readily attributable to an individual. Any changes to data after an electronic signature has been assigned should invalidate the signature until the data has been reviewed again and re-signed.
4	Restrictions on use of USB devices For reasons of system security, USB ports should be default disabled on computer clients and servers hosting GxP critical data. If necessary, ports should only be opened for approved purposes and all USB devices should be properly scanned before use. The use of private USB devices (flash drives, cameras, smartphones, keyboards etc) on company computer clients and servers hosting GxP data, or the use of company USB devices on private computers, should not be allowed.	This is especially important for Windows environments where system vulnerabilities are known that allow USB devices to trick the computer, by pretending to to be another external device, e.g. keyboard, and can contain and start executable code.

783 9.4 Audit trails for computerised systems

784

	Expectations	**Potential risk of not meeting expectations / items to be checked**
Item:	**Audit Trails**	
1	Consideration should be given to data management and integrity requirements when purchasing and implementing computerised systems. Companies should select software that includes appropriate electronic audit trail functionality. Companies should endeavour to purchase and upgrade older systems to implement software that includes electronic audit trail functionality. It is acknowledged that some very simple systems lack appropriate audit trails; however, alternative arrangements to verify the veracity of data must be implemented, e.g. administrative procedures, secondary checks and controls. Additional guidance may be found under section 9.9 regarding Hybrid Systems. Audit trail functionality should be verified during validation of the system to ensure that all changes and deletions of critical data associated with each manual activity are recorded and meet ALCOA+ principles. Audit trail functionalities must be enabled and locked at all times and it must not be possible to deactivate the functionality. If it is possible for administrative users to deactivate the audit trail functionality, an automatic entry should be made in the audit trail indicating that the functionality has been deactivated. Companies should implement procedures that outline their policy and processes for the review of audit trails in accordance with risk management principles. Critical audit trails related to each operation should be independently reviewed with all other records related to the operation and prior to the review of the completion of the operation, e.g. prior to batch release, so as to ensure that critical data and changes to it are acceptable. This review should be	Validation documentation should demonstrate that audit trails are functional, and that all activities, changes and other transactions within the systems are recorded, together with all metadata. Verify that audit trails are regularly reviewed (in accordance with quality risk management principles) and that discrepancies are investigated. If no electronic audit trail system exists a paper based record to demonstrate changes to data may be acceptable until a fully audit trailed (integrated system or independent audit software using a validated interface) system becomes available. These hybrid systems are permitted, where they achieve equivalence to integrated audit trail, such as described in Annex 11 of the PIC/S GMP Guide. Failure to adequately review audit trails may allow manipulated or erroneous data to be inadvertently accepted by the Quality Unit and/or Authorised Person. Clear details of which data are critical, and which changes and deletions must be recorded (audit trail) should be documented.

	Expectations	**Potential risk of not meeting expectations / items to be checked**
	performed by the originating department, and where necessary verified by the quality unit, e.g. during self-inspection or investigative activities.	
2	Where available, audit trail functionalities for electronic-based systems should be assessed and configured properly to capture any critical activities relating to the acquisition, deletion, overwriting of and changes to data for audit purposes. Audit trails should be configured to record all manually initiated processes related to critical data. The system should provide a secure, computer generated, time stamped audit trail to independently record the date and time of entries and actions that create, modify, or delete electronic records. The audit trail should include the following parameters: - Who made the change - What was changed, incl. old and new values - When the change was made, incl. date and time - Why the change was made (reason) - Name of any person authorising the change. The audit trail should allow for reconstruction of the course of events relating to the creation, modification, or deletion of an electronic record. The system must be able to print and provide an electronic copy of the audit trail, and whether looked at in the system or in a copy, the audit trail should be available in a meaningful format. If possible, the audit trail should retain the dynamic functionalities found in the computer system, e.g. search functionality and export to e.g. Excel	Verify the format of audit trails to ensure that all critical and relevant information is captured. The audit trail must include all previous values and record changes must not obscure previously recorded information. Audit trail entries should be recorded in true time and reflect the actual time of activities. Systems recording the same time for a number of sequential interactions, or which only make an entry in the audit trail, once all interactions have been completed, may not in compliance with expectations to data integrity, particularly where each discrete interaction or sequence is critical, e.g. for the electronic recording of addition of 4 raw materials to a mixing vessel. If the order of addition is a CPP, then each addition should be recorded individually, with time stamps. If the order of addition is not a CCP then the addition of all 4 materials could be recored as a single timestamped activity.

9.5 Data capture/entry for computerised systems

	Expectations	Potential risk of not meeting expectations / items to be checked
Item:	**Data capture/entry**	
1	Systems should be designed for the correct capture of data whether acquired through manual or automated means. For manual entry: - The entry of critical data should only be made by authorised individuals and the system should record details of the entry, the individual making the entry and when the entry was made. - Data should be entered in a specified format that is controlled by the software, validation activities should verify that invalid data formats are not accepted by the system. - All manual data entries of critical data should be verified, either by a second operator, or by a validated computerised means. - Changes to entries should be captured in the audit trail and reviewed by an appropriately authorised and independent person. For automated data capture: - The interface between the originating system, data acquisition and recording systems should be validated to ensure the accuracy of data. - Data captured by the system should be saved into memory in a format that is not vulnerable to manipulation, loss or change. - The system software should incorporate validated checks to ensure the completeness of data acquired, as well as any metadata associated with the data.	Ensure that manual entries made into computerised systems are subject to an appropriate secondary check. Validation records should be reviewed for systems using automated data capture to ensure that data verification and integrity measures are implemented and effective.
2	Any necessary changes to data must be authorised and controlled in accordance with approved procedures. For example, manual integrations and reprocessing of laboratory results must be performed in an approved and controlled manner. The firm's quality unit	Verify that appropriate procedures exist to control any amendments or re-processing of data. Evidence should demonstrate an appropriate process of formal approval for the proposed change, controlled/restricted/defined changes and formal review of the changes made.

	Expectations	Potential risk of not meeting expectations / items to be checked
	must establish measures to ensure that changes to data are performed only when necessary and by designated individuals. Original (unchanged) data should be retained in its original form. Any and all changes and modifications to original data must be fully documented and should be reviewed and approved by at least one appropriately trained and qualified individual.	

9.6 Review of data within computerised systems

	Expectations	Potential risk of not meeting expectations / items to be checked
Item:	**Review of electronic data**	
1	The regulated user should perform a risk assessment in order to identify all the GMP/GDP relevant electronic data generated by the computerised systems, and the criticality of the data. Once identified, critical data should be audited by the regulated user and verified to determine that operations were performed correctly and whether any change (modification, deletion or overwriting) have been made to original information in electronic records. All changes must be duly authorised. An SOP should describe the process by which data is checked by a second operator. These SOPs should outline the critical raw data that is reviewed, a review of data summaries, review of any associated log-books and hard-copy records, and explain how the review is performed, recorded and authorised. The review of audit trails should be part of the routine data review within the approval process. The frequency, roles and responsibilities of audit trail review should be based on a risk assessment according to the GMP/GDP relevant value of the data recorded in the computerised system. For example, for changes of electronic data that can have a direct impact on the quality of the medicinal products, it would be expected to review audit trails	Check local procedures to ensure that electronica data is reviewed based on its criticality (impact to product quality and/or decision making). Evidence of each review should be recorded and available to the inspector. Where data summaries are used for internal or external reporting, evidence should be available to demonstrate that such summaries have been verified in accordance with raw data. Check that regulated party has a detailed SOP outlining the steps on how to perform secondary reviews and audit trail reviews and what steps to take if issues are found during the course of the review. Where global systems are used, it may be necessary for date and time records to include a record of the time zone to demonstrate contemporaneous recording. Check that known changes, modifications or deletions of data are actually recorded by the audit trail functionality.

	Expectations	Potential risk of not meeting expectations / items to be checked
	prior to the point that the data is relied upon to make a critical decision, e.g. batch release. The regulated user should establish an SOP that describes in detail how to review audit trails, what to look for and how to perform searches etc. The procedure should determine in detail the process that the person in charge of the audit trail review should follow. The audit trail activity should be documented and recorded. Any significant variation from the expected outcome found during the audit trail review should be fully investigated and recorded. A procedure should describe the actions to be taken if a review of audit trails identifies serious issues that can impact the quality of the medicinal products or the integrity of data.	
2	The company's quality unit should establish a program and schedule to conduct ongoing reviews of audit trails based upon their criticality and the system's complexity. These reviews should be incorporated into the company's self-inspection programme. Procedures should be in place to address and investigate any audit trail discrepancies, including escalation processes for the notification of senior management and national authorities where necessary.	Verify that self-inspection programs incorporate checks of audit trails, with the intent to verify the effectiveness of existing controls and compliance with internal procedures regarding the review of data. Audit trail checks should be both random, (selected based on chance) and targeted (selected based on criticality or risk).

9.7 Storage, archival and disposal of electronic data

	Expectations	Potential risk of not meeting expectations / items to be checked
Item:	**Storage, archival and disposal of electronica data**	
1	Storage of data must include the entire original data and metadata, including audit trails, using a secure and validated process. If the data is backed up, or copies of it are made, then the backup and copies must also have the same appropriate levels of controls so as to prohibit	Check that data storage, back-up and archival systems are designed to capture all data and metadata. There should be documented evidence that these systems have been validated and verified. Check that data associated with superseded or upgraded systems is managed appropriately and is accessible.

	Expectations	Potential risk of not meeting expectations / items to be checked
	unauthorised access to, changes to and deletion of data or their alteration. For example, a firm that backs up data onto portable hard drives must prohibit the ability to delete data from the hard drive. Some additional considerations for the storage and backup of data include: - True copies of dynamic electronic records can be made, with the expectation that the entire content (i.e., all data and metadata is included) and meaning of the original records are preserved. - Stored data should be accessible in a fully readable format. Companies may need to maintain suitable software and hardware to access electronically stored data backups or copies during the retention period - Routine backup copies should be stored in a remote location (physically separated) in the event of disasters. - Back-up data should be readable for all the period of the defined regulatory retention period, even if a new version of the software has been updated or substituted for one with better performance. - Systems should allow backup and restoration of all data, including meta-data and audit trails.	
2	The record retention procedures must include provisions for retaining the metadata. This allows for future queries or investigations to reconstruct the activities that occurred related to a batch.	
3	Data should be archived periodically in accordance with written procedures. Archive copies should be physically secured in a separate and remote location from where back up and original data are stored. The data should be accessible and readable and its integrity maintained for all the period of archiving.	There is a risk with archived data that access and readability of the data may be lost due to software application updates or superseded equipment. Verify that the company has access to archived data, and that they maintain access to the necessary software to enable review of the archived data. Where external or third party facilities are utilised for the archiving of data, these service providers should be subject to

	Expectations	Potential risk of not meeting expectations / items to be checked
	There should be in place a procedure for restoring archived data in case an investigation is needed. The procedure in place for restoring archived data should be regularly tested. If a facility is needed for the archiving process then specific environmental controls and only authorised personnel access should be implemented in order to ensure the protection of records from deliberate or inadvertent alteration or loss. When a system in the facility has to be retired because problems with long term access to data are envisaged, procedures should assure the continued readability of the data archived. For example, it could be established to transfer the data to another system.	assessment, and all responsibilities recorded in a quality technical agreement. Check agreements and assessment records to verify that due consideration has been given to ensuring the integrity of archived records.
4	It should be possible to print out a legible and meaningful record of all the data generated by a computerised system (including metadata). If a change is performed to records, it should be possible to also print out the change of the record, indicating when and how the original data was changed.	Check validation documentation for systems to ensure that systems have been validated for the generation of legible and complete records. Samples of print-outs may be verified.
5	Procedures should be in place that describe the process for the disposal of electronically stored data. These procedures should provide guidance for the assessment of data and allocation of retention periods, and describe the manner in which data that is no longer required is disposed of.	Check that the procedures clearly stipulate the conditions for the disposal of data, and that care is taken to avoid the inadvertent disposal of required data during its lifecycle.

9.8 Management of Hybrid Systems

	Expectations	Potential risk of not meeting expectations / items to be checked
Item:	**Management of Hybrid Systems**	
1	Hybrid systems require specific and additional controls in reflection of their complexity and potential increased vulnerability to manipulation of data. Each element of the hybrid system should be qualified and controlled in accordance with the guidance relating to manual and computerised systems as specified above.	Check that hybrid systems are clearly defined and identified, and that each contributing element of the system is validated. Attention should be paid to the interface between the manual and computerised system. Inspectors should verify that adequate controls and secondary checks

	Appropriate quality risk management principles should be followed when assessing, defining, and demonstrating the effectiveness of control measures applied to the system. A detailed system description of the entire system should be available that outlines all major components of the system, the function of each component, controls for data management and integrity, and the manner in which system components interact. Procedures and records should be available to manage and appropriately control the interface between manual and automated systems, particularly steps associated with: - Manual input of manually generated data into computerised systems; - Transcription (including manual) of data generated by automated systems onto paper records; - Automated detection and transcription of printed data into computerised systems.	are in place where manual transcription between systems takes place. Original data should be retained following transcription and processing. Hybrid systems commonly consist of a combination of computerised and manual systems. Particular attention should be paid to verifying: - The extent of qualification and/or validation of the computerised system; and, - The robustness of controls applied to the management of the manual element of the hybrid system due to the difficulties in consistent application of a manual process.

10 DATA INTEGRITY CONSIDERATIONS FOR OUTSOURCED ACTIVITIES

10.1 General supply chain considerations

10.1.1 Data integrity plays a key part in ensuring the security and integrity of supply chains. Data governance measures by a contract giver may be significantly weakened by unreliable or falsified data or materials provided by supply chain partners. This principle applies to all outsourced activities, including suppliers of raw materials, contract manufacturers, analytical services, wholesalers and contracted consultation service providers.

10.1.2 Initial and periodic re-qualification of supply chain partners and outsourced activities should include consideration of data integrity risks and appropriate control measures.

10.1.3 It is important for an organisation to understand the data integrity limitations of information obtained from the supply chain (e.g. summary records and copies / printouts), and the challenges of remote supervision. These limitations are similar to those discussed in section 8.11 of this guidance This will help to focus resources towards data integrity verification and supervision using a quality risk management approach.

10.2 Routine document verification

10.2.1 The supply chain relies upon the use of documentation and data passed from one organisation to another. It is often not practical for the contract giver to review all raw data relating to reported results. Emphasis should be placed upon robust supplier and contractor qualification, using the principles of quality risk management.

10.3 Strategies for assessing data integrity in the supply chain

10.3.1 Companies should conduct regular risk reviews of supply chains and outsourced activity that evaluate the extent of data integrity controls required. Information considered during risk reviews may include:

- The outcome of site audits, with focus on data governance measures
- Review of data submitted in routine reports, for example:

Area for review	**Rationale**
Comparison of analytical data reported by the contractor or supplier vs in-house data from analysis of the same material	To look for discrepant data which may be an indicator of falsification

10.3.2 Quality agreements should be in place between manufacturers and suppliers/contract manufacturing organisations (CMOs) with specific provisions for ensuring data integrity across the supply chain. This may be achieved by setting out expectations for data governance, and transparent error/deviation reporting by the contract acceptor to the contract giver. There should also be a requirement to notify the contract giver of any data integrity failures identified at the contract acceptor site.

10.3.3 Audits of suppliers and manufacturers of APIs, critical intermediate suppliers, primary and printed packaging materials suppliers, contract manufacturers and service providers conducted by the manufacturer (or by a third party on their behalf) should include a verification of data integrity measures at the contract organisation.

10.3.4 Audits and routine surveillance should include adequate verification of the source electronic data and metadata by the Quality Unit of the contract giver using a quality risk management approach. This may be achieved by measures such as:

Site audit	Review the contract acceptors organisational behaviour, and understanding of data governance, data lifecycle, risk and criticality.
Material testing vs CoA	Compare the results of analytical testing vs suppliers reported CoA. Examine discrepancies in accuracy, precision or purity results. This may be performed on a routine basis, periodically, or unannounced, depending on material and supplier risks.
Remote data review	The contract giver may consider offering the Contracted Facility/Supplier use of their own hardware and software system (deployed over a Wide Area Network) to use in batch manufacture and testing. The contract giver may monitor the quality and integrity of the data generated by the Contracted Facility personnel in real time. In this situation, there should be segregation of duties to ensure that contract giver monitoring of data does not give provision for amendment of data generated by the contract acceptor.
Quality monitoring	Quality and performance monitoring may indicate incentive for data falsification (e.g. raw materials which marginally comply with specification on a frequent basis.

10.3.5 Contract givers may work with the contract acceptor to ensure that all client-confidential information is encoded to de-identify clients. This would facilitate review of source electronic data and metadata at the contract giver's site, without breaking confidentiality obligations to other clients. By reviewing a larger data set, this enables a more robust assessment of the contract givers data governance measures. It also permits a search for indicators of data integrity failure, such as repeated data sets or data which does not demonstrate the expected variability.

10.3.6 Care should be taken to ensure the authenticity and accuracy of supplied documentation, (refer section 8.11). The difference in data integrity and traceability risks between 'true copy' and 'summary report' data should be considered when making contractor and supply chain qualification decisions.

11 REGULATORY ACTIONS IN RESPONSE TO DATA INTEGRITY FINDINGS

11.1 Deficiency references

11.1.1 The integrity of data is fundamental to good manufacturing practice and the requirements for good data management are embedded in the current PIC/S Guides to GMP/GDP for Medicinal products. The following table provides a reference point highlighting some of these existing requirements.

ALCOA principle	PIC/S Guide to Good Manufacturing Practice for Medicinal products, PE009 (Part I):	PIC/S Guide to Good Manufacturing Practice for Medicinal products, PE009 (Part II):	Annex 11 (Computerised Systems)	PIC/S Guide to Good Distribution Practice for Medicinal products, PE011:
Attributable	[4.20, c & f], [4.21, c & i], [4.29 point 5]	[5.43], [6.14], [6.18], [6.52]	[2], [12.1], [12.4], [15]	[4.2.4], [4.2.5]
Legible	[4.1], [4.2], [4.7], [4.8], [4.9], [4.10]	[6.11], [6.14], [6.15], [6.50]	[4.8], [7.1], [7.2] [8.1], [9], [10], [17]	[4.2.3], [4.2.9]
Contemporaneous	[4.8]	[6.14]	[12.4], [14]	[4.1], [4.2.9]
Original	[4.9], [4.27], [Paragraph "Record"]	[6.14], [6.15], [6.16]	[8.2], [9]	[4.2.5]
Accurate	[4.1], [6.17]	[5.40], [5.42], [5.45], [5.46], [5.47], [6.6]	[Paragraph "Principles"] [4.8], [5], [6], [7.2], [10], [11]	[4.2.3]
Complete	[4.8]	[6.16], [6.50], [6.60], [6.61]	[4.8], [7.1], [7.2], [9]	[4.2.3], [4.2.5]
Consistent	[4.2]	[6.15], [6.50]	[4.8], [5]	[4.2.3]
Enduring	[4.1], [4.10]	[6.11], [6.12], [6.14]	[7.1], [17]	[4.2.6]
Available	[Paragraph "Principle"], [4.1]	[6.12], [6.15], [6.16]	[3.4], [7.1], [16], [17]	[4.2.1]

11.2 Classification of deficiencies

Note: The following guidance is intended to aid consistency in reporting and classification of data integrity deficiencies, and is not intended to affect the inspecting authority's ability to act according to its internal policies or national regulatory frameworks.

11.2.1 Deficiencies relating to data integrity failure may have varying impact to product quality. Prevalence of the failure may also vary between the action of a single employee to an endemic failure throughout the inspected organisation.

11.2.2 The draft PIC/S guidance[11] on classification of deficiencies states:

"A critical deficiency is a practice or process that has produced, or leads to a significant risk of producing either a product which is harmful to the human or veterinary patient or a product which could result in a harmful residue in a food producing animal. *A critical deficiency also occurs when it is observed that the manufacturer has engaged in fraud, misrepresentation or falsification of products or data".*

11.2.3 Notwithstanding the "critical" classification of deficiencies relating to fraud, misrepresentation or falsification, it is understood that data integrity deficiencies can also relate to:

- Data integrity failure resulting from bad practice,
- Opportunity for failure (without evidence of actual failure) due to absence of the required data control measures.

11.2.4 In these cases, it may be appropriate to assign classification of deficiencies by taking into account the following (indicative list only):

Impact to product with actual or potential risk to patient health: Critical deficiency:

- Product failing to meet specification at release or within shelf life.
- Reporting of a 'desired' result rather than an actual out of specification result when reporting of QC tests, critical product or process parameters.
- Wide-ranging and intentional manipulation or falsification of data, with or without the knowledge and assistance of senior management, the extent of which critically undermines the reliability of the pharmaceutical quality system and erodes all confidence in the quality and safety of medicines manufactured or handled by the site.

Impact to product with no risk to patient health: Major deficiency:

- Data being mis-reported, e.g. original results 'in specification', but altered to give a more favourable trend.
- Reporting of a 'desired' result rather than an actual out of specification result when reporting of data which does not relate to QC tests, critical product or process parameters.
- Failures arising from poorly designed data capture systems (e.g. using scraps of paper to record info for later transcription).

No impact to product; evidence of moderate failure: Major deficiency:

- Bad practices and poorly designed systems which may result in opportunities for data integrity issues or loss of traceability across a limited

[11] This draft guidance has not been published yet.

number of functional areas (QA, production, QC etc.). Each in its own right has no direct impact to product quality.

No impact to product; limited evidence of failure: Other deficiency:

- Bad practice or poorly designed system which result in opportunities for data integrity issues or loss of traceability in a discrete area.
- Limited failure in an otherwise acceptable system, e.g. manipulation of non-critical data by an individual.

11.2.5 It is important to build an overall picture of the adequacy of the key elements (data governance process, design of systems to facilitate compliant data recording, use and verification of audit trails and IT user access etc.) to make a robust assessment as to whether there is a company-wide failure, or a deficiency of limited scope/ impact.

11.2.6 Individual circumstances (exacerbating / mitigating factors) may also affect final classification or regulatory action. Further guidance on the classification of deficiencies and intra-authority reporting of compliance issues will be available in the PIC/S guidance on the classification of deficiencies, once it has been published.

12 REMEDIATION OF DATA INTEGRITY FAILURES

12.1 Responding to Significant Data Integrity issues

12.1.1 Consideration should be primarily given to resolving the immediate issues identified and assessing the risks associated with the data integrity issues. The response by the company in question should outline the actions taken. Responses from implicated manufacturers should include:

12.1.1.1 A comprehensive investigation into the extent of the inaccuracies in data records and reporting, to include:

- A detailed investigation protocol and methodology; a summary of all laboratories, manufacturing operations, and systems to be covered by the assessment; and a justification for any part of the operation that the regulated user proposes to exclude[12];
- Interviews of current and former employees to identify the nature, scope, and root cause of data inaccuracies. These interviews may be conducted by a qualified third party;
- An assessment of the extent of data integrity deficiencies at the facility. Identify omissions, alterations, deletions, record destruction, non-contemporaneous record completion, and other deficiencies;
- Determination of the scope (Data, products, processes and specific batches), and timeframe for the incident, with justification for the time-boundaries applied;
- A description of all parts of the operations in which data integrity lapses occur, additional consideration should be given to global corrective actions for multinational companies or those that operate across multiple differing sites;
- A comprehensive retrospective evaluation of the nature of the testing and manufacturing data integrity deficiencies, and the potential root cause(s).

[12] The scope of the investigation should include an assessment of the extent of data integrity at the corporate level, including all facilities, sites and departments that could potentially be affected.

The services of a qualified third-party consultant with specific expertise in the areas where potential breaches were identified may be necessary;

- A risk assessment of the potential effects of the observed failures on the quality of the drugs involved. The assessment should include analyses of the potential risks to patients caused by the release/distribution of products affected by a lapse of data integrity, risks posed by ongoing operations, and any impact on the veracity of data submitted to regulatory agencies, including data related to product registration dossiers.

12.1.1.2 Corrective and preventive actions taken to address the data integrity vulnerabilities and timeframe for implementation, and including:

- Interim measures describing the actions to protect patients and to ensure the quality of the medicinal products, such as notifying customers, recalling product, conducting additional testing, adding lots to the stability program to assure stability, drug application actions, and enhanced complaint monitoring.
- Long-term measures describing any remediation efforts and enhancements to procedures, processes, methods, controls, systems, management oversight, and human resources (e.g., training, staffing improvements) designed to ensure the data integrity.

12.1.2 Whenever possible, inspectorates should meet with senior representatives from the implicated companies to convey the nature of the deficiencies identified and seek written confirmation that the company commits to full disclosure of issues and their prompt resolution. A management strategy should be submitted to the regulatory authority that includes the details of the global corrective action and preventive action plan. The strategy should include:

- A detailed corrective action plan that describes how the regulated user intends to ensure the 'ALOCA+' attributes (see section 7.4) of all of the data generated, including analytical data, manufacturing records, and all data submitted or presented to the Competent Authority.
- A comprehensive description of the root causes of the data integrity lapses, including evidence that the scope and depth of the current action plan is commensurate with the findings of the investigation and risk assessment. This must indicate if individuals responsible for data integrity lapses remain able to influence GMP/GDP-related or drug application data.

12.1.3 Inspectorates should implement policies for the management of significant data integrity issues identified at inspection in order to manage and contain risks associated with the data integrity breach.

12.2 Indicators of improvement

12.2.1 An on-site inspection is required to verify the effectiveness of actions taken to address serious data integrity issues. Some indicators of improvement are:

12.2.1.1 Evidence of a thorough and open evaluation of the identified issue and timely implementation of effective corrective and preventive actions, including appropriate implementation of corrective and preventive actions at an organisational level;

12.2.1.2 Evidence of open communication of issues with clients and other regulators. Transparent communication should be maintained throughout the investigation and remediation stages. Regulators should be aware that further data integrity failures may be reported as a result of the detailed investigation. Any additional reaction to these notifications should be proportionate to public health risks, to encourage continued reporting;

12.2.1.3 Evidence of communication of data integrity expectations across the organisation, incorporating processes for open reporting of potential issues and opportunities for improvement without repercussions;

12.2.1.4 The regulated user should ensure that an appropriate evaluation of the vulnerability of any sophisticated electronic systems to data manipulation takes place to ensure that follow-up actions have fully resolved all the violations, third party expertise may be required;

12.2.1.5 Implementation of data integrity policies in line with the principles of this guide;

12.2.1.6 Implementation of routine data verification practices.

13 DEFINITIONS

13.1 Archiving

Long term, permanent retention of completed data and relevant metadata in its final form for the purposes of reconstruction of the process or activity.

13.2 Audit Trail

GMP/GDP audit trails are metadata that are a record of GMP/GDP critical information (for example the change or deletion of GMP/GDP relevant data), which permit the reconstruction of GMP/GDP activities.

13.3 Back-up

A copy of current (editable) data, metadata and system configuration settings (e.g. variable settings which relate to an analytical run) maintained for the purpose of disaster recovery.

13.4 Computerised system

A system including the input of data, electronic processing and the output of information to be used either for reporting or automatic control.

13.5 Data

Facts, figures and statistics collected together for reference or analysis.

13.6 Data Flow Map

A graphical representation of the "flow" of data through an information system

13.7 Data Governance

The sum total of arrangements to ensure that data, irrespective of the format in which it is generated, recorded, processed, retained and used to ensure a complete, consistent and accurate record throughout the data lifecycle.

13.8 Data Integrity

The extent to which all data are complete, consistent and accurate throughout the data lifecycle. The data should comply with ALCOA+ principles.

13.9 Data Lifecycle

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.

13.10 Exception report

A validated search tool that identifies and documents predetermined 'abnormal' data or actions, which require further attention or investigation by the data reviewer.

13.11 Hybrid Systems

A system for the management and control of data that typically consists of an electronic system, supplemented by a defined manual system. Hybrid systems rely on the effective management of both sub-systems for correct operation.

13.12 Metadata

Data that describes the attributes of other data, and provides context and meaning.

13.13 Quality Unit

The department within the regulated entity responsible for oversight of quality including in particular the design, effective implementation, monitoring and maintenance of the pharmaceutical quality system.

13.14 System Administrator

A person who manages the operation of a computer system or particular electronic communication service.

14 REVISION HISTORY

Date	Version Number	Reasons for revision
18 July 2016	Draft 1	Consultation of PIC/S Participating Authorities on publication of the Good Practices as a draft.
10 August 2016	Draft 2	Publication of Draft 2 on the PIC/S website Implementation of the draft on a trial basis and comment period for PIC/S Participating Authorities.
30 November 2018	Draft 3	Updated version to include feedback from PIC/S Participating Authorities