PHARMACEUTICAL INSPECTION CONVENTION
PHARMACEUTICAL INSPECTION CO-OPERATION SCHEME

PI 041-1

1 July 2021

PIC/S GUIDANCE

PIC/S 指南

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

受监管 GMP/GDP 环境下数据管理和完整性优良规范

Editor: PIC/S Secretariat
e-mail: info@picscheme.org
web site: https://www.picscheme.org

TABLE OF CONTENTS 目录

1 DOCUMENT HISTORY 文件历史

Adoption by Committee of PI 041-1	1 June 2021
委员会通过，编号为 PI 041-1	2021 年 6 月 1 日
Entry into force of PI 041-1	1 July 2021
PI 041-1 生效	2021 年 7 月 1 日

2 INTRODUCTION 概述

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.

PIC/S 参与机构定期对活性药物成分 (API) 和医药产品的生产商和分销商进行检查，以确定其符合良好生产规范 (GMP) 和良好分销规范 (GDP) 原则的程度。这些检查通常在现场进行，但也可以通过远程或非现场评估文件证据来进行，在这种情况下，应考虑远程数据审核的局限性。

2.2 The effectiveness of these inspection processes is determined by the reliability 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.

这些检查过程的有效性取决于提供给检查员的证据的可靠性以及最终基础数据的完整性。检查员是否可以确定并完全依赖提供给他们的证据和记录的准确性和完整性对检查过程至关重要。

2.3 Data management refers to all those activities performed during the handling of data including but not limited to data policy, documentation, quality and security. Good data management practices influence the quality of all data generated and recorded by a manufacturer. 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.

数据管理是指在数据处理过程中进行的所有活动，包括但不限于数据政策、文件、质量和安全。良好的数据管理规范会影响制造商生成和记录的所有数据的质量。这些做法应确保数据是可归属、清晰的、同步的、原始的、准确的、完整的、一致的、持久的和可用的。虽然本文件的主要重点是与 GMP/GDP 要求有关的内容，但也应在良好数据管理的更广泛背景下考虑此处的原则，例如注册文件中包含的数据基于哪些 API 和制剂控制策略和标准设置。

2.4 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.

良好的数据管理做法适用于药品质量体系的所有要素，此处的原则等同适用于电子和纸质系统生成的数据。

2.5 Data Integrity is defined as “the degree to which data are complete, consistent, accurate, trustworthy, and reliable and that these characteristics of the data are

maintained throughout the data life cycle[1]". This is a fundamental requirement for an effective 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.

数据完整性定义为“数据完整、一致、准确、可信和可靠的程度，以及数据的这些特征在整个数据生命周期中得到维护的程度”。这是有效的药品质量体系的基本要求，可确保药品具有所需的质量。不良的数据完整性做法和漏洞会破坏记录和证据的质量，并可能最终破坏药品的质量。

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.

与数据管理和完整性的良好规范有关的责任属于接受检查的生产商或分销商。他们有全部责任和义务评估其数据管理系统的潜在漏洞，并采取措施设计和实施良好的数据治理规范，以确保维护数据完整性。

3 PURPOSE 目的

3.1 This document was written with the aim of:

本文目的在于：

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.

为检查员解释与优良数据管理有关的 GMP/GDP 要求和执行检查提供指导。

3.1.2 Providing consolidated, illustrative guidance on risk-based control strategies which enable the existing requirements for data to be valid, complete and reliable 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.

为基于风险的控制策略提供说明性综合指南，使现有的数据要求与 PIC/S 要求在现代化行业规范和全球供应链环境下实施的 GMP 和 GDP 指南中所述一样有效、完整和可靠。

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.

促进将优良数据管理要素有效实施到 GMP/GDP 检查的常规计划和实施中；提供一种工具来统一 GMP/GDP 检验，并确保与数据完整性要求相关的检查质量。

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.

本指南连同检查员备忘录等资源，应使检查员能够在检查期间最佳利用检查时间，并对数据完整性要素进行最佳评估。

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

[1] 'GXP' Data Integrity Guidance and Definitions, MHRA, March 2018 GXP 数据完整性指南和定义，MHRA，2018 年 3 月
[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 PIC/S PE 009 药品 GMP 指南，尤其是第一部分第 4、5、6 章，第二部分第 5、6&附录 11
[3] PIC/S PE 011 Guide to Good Distribution Practice for Medicinal Products, specifically sections 3, 4, 5 & 6 PIC/S PE 011 药品 GDP 指南，尤其是第 3, 4, 5 & 6 节。

此处的指南应有助于检查组规划基于风险的与良好数据管理实践有关的检查。

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.

良好的数据管理一直被认为是 GMP/GDP 的一个组成部分。因此，本指南并非旨在对受监管实体施加额外的监管负担，而是旨在就与当前行业数据管理实践相关的现有 GMP/GDP 要求的解释提供指导。

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.

数据管理和完整性原则等同适用于纸质、计算机化和混合系统，它不应限制新概念或技术的开发或采用。根据 ICH Q10 原则，本指南应通过持续改进促进创新技术的采用。

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.

本文件主要使用术语“药品质量体系”来表示用于管理和实现质量目标的质量管理体系。虽然术语“药品质量体系”主要由 GMP 监管实体使用，但就本指南而言，它应被视为可与 GDP 监管实体使用的术语“质量体系”互换。

3.7 This guide is not mandatory or enforceable under law. It is not intended to be restrictive or to replace national legislation regarding data integrity requirements for manufacturers and distributors of medicinal products and actives substances (i.e. active pharmaceutical ingredients). Data integrity deficiencies should be referenced to national legislation or relevant paragraphs of the PIC/S GMP or GDP guidance.

本指南不具有强制性，也不是法律强制执行的。它无意限制或取代关于医药产品和活性物质（即活性药物成分）的生产商和分销商的数据完整性要求的国家法律法规。数据完整性缺陷应参考国家法律法规或 PIC/S 的 GMP 或 GDP 指南的相关段落。

4 SCOPE 范围

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.

本指南适用于对进行生产 (GMP) 和分销 (GDP) 活动的场所进行现场检查。本指南中的原则适用于整个产品生命周期的所有阶段。该指南应被视为检查期间要考虑的区域的非详尽清单。

4.2 The guidance also applies to remote (desktop) inspections of sites performing manufacturing (GMP) and distribution (GDP) activities, although this will be limited to an assessment of data governance systems. On-site assessment is normally required for data verification and evidence of operational compliance with procedures.

本指南也适用于对执行生产 (GMP) 和分销 (GDP) 活动的场所进行远程（桌面）检查，虽然此类检查仅限于对数据治理系统的评估。对数据进行核查，检查其是否按程序进

行操作的证据通常需要现场评估。

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.

虽然本文件范围如上所述，但此处描述的有关良好数据管理实践的许多原则也适用于受监管的制药和卫生行业的其他领域。

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.

本指南并非用于指导在发现可能需要取证专业知识的重大数据完整性漏洞后进行的"有因"检查。

5 DATA GOVERNANCE SYSTEM 数据治理系统

5.1 What is data governance? 什么是数据治理？

5.1.1 Data governance is the sum total of arrangements which provide assurance of data integrity. 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 an attributable, legible, contemporaneous, original, accurate, complete, consistent, enduring, and available record throughout the data lifecycle. While there may be no legislative requirement to implement a 'data governance system', its establishment enables the manufacturer to define, prioritise and communicate their data integrity risk management activities in a coherent manner. Absence of a data governance system may indicate uncoordinated data integrity systems, with potential for gaps in control measures.

数据治理是保证数据完整性的安排的总和。这些安排确保数据（无论其生成、记录、处理、保留、检索和使用的过程、格式或技术如何）在记录生命周期内均是可归属的、清晰的、同步的、原始的、准确的、完整的、一致的、持久的和可用的。虽然可能没有实施"数据治理系统"的法规要求，但它的建立使生产商能够以统一的方式定义、优先考虑和沟通他们的数据完整性风险管理活动。缺乏数据治理系统可能表明数据完整性系统不协调，控制措施可能存在差距。

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).

数据生命周期是指数据如何产生、处理、报告、检查、用于决策、存储和最终在保留期结束时丢弃。与产品或工艺相关的数据可能会跨越生命周期内的各种边界。这可能包括纸质系统和计算机系统之间或不同组织边界之间的数据传输；内部（例如在生产、QC 和 QA 之间）和外部（例如在服务提供商或合同委托方与受托方之间）。

5.2 Data governance systems 数据治理系统

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.

数据治理系统应该是 PIC/S 的 GMP/GDP 中描述的药品质量系统的组成部分。它应该解决整个生命周期中的数据所有权问题，并考虑工艺和系统的设计、操作和监控，以符合数据完整性原则，包括控制有意和无意的信息更改和删除。

5.2.2 Data governance systems rely on the incorporation of suitably designed systems, the use of technologies and data security measures, combined with specific expertise to ensure that data management and integrity is effectively controlled. Regulated entities should take steps to ensure appropriate resources are available and applied in the design, development, operation and monitoring of the data governance systems, commensurate with the complexity of systems, operations, and data criticality and risk.

数据治理系统依赖于经过适当设计的系统集成、技术和数据安全措施的使用，并结合特定的专业知识来确保数据管理和完整性得到有效控制。受监管实体应采取措施，确保在数据治理系统的设计、开发、运营和监控中提供和应用适当的资源，与系统、运营以及数据关键性和风险的复杂性相称。

5.2.3 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:

数据治理体系应确保在数据生命周期内的控制与质量风险管理原则相称。这些控制可以是：

- Organisational 管理措施
  - procedures, e.g. instructions for completion of records and retention of completed records;
  - 程序，例如要求完成记录和保存已完成记录的指令；
  - training of staff and documented authorisation for data generation and approval;
  - 员工培训，数据生成和批准要求有文件记录的授权；
  - data governance system design, considering how data is generated, recorded, processed, retained and used, and risks or vulnerabilities are controlled effectively;
  - 数据治理系统设计，考虑数据如何生成、记录、处理、保存和使用，并对风险或弱点进行有效控制；
  - routine (e.g. daily, batch- or activity-related) data verification;
  - 常规（例如，每天，每批或按活动）数据核查；
  - periodic surveillance, e.g. self-inspection processes seek to verify the effectiveness of the data governance system; or
  - 定期监管，例如自检流程核查数据治理系统的有效性；或
  - the use of personnel with expertise in data management and integrity, including expertise in data security measures.
  - 使用具备数据管理和完整性专业知识，包括具备数据安全保护措施经验的人员。
- Technical 技术措施
  - computerised system validation, qualification and control;
  - 计算机化系统验证、确认和控制；
  - automation; or
  - 自动化；或
  - the use of technologies that provide greater controls for data management and integrity.
  - 使用能够提供更强的数据管理和完整性控制的技术。

5.2.4 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.

5.2.5 有效的数据治理系统能够证明高层管理人员理解并承诺有效的数据治理做法，包括将合适的组织文化与行业（节 6）组合的必要性，理解数据关键性、数据风险和数据生命周期。还应有证据证明在组织内各层级向员工就要求进行了沟通。沟通方式应确保鼓励报告失败，提供改进机会。这样可减少伪造、修改或删除数据的诱因。

5.2.6 The organisation's arrangements for data governance should be documented within their Pharmaceutical Quality System and regularly reviewed.

5.2.7 管理方面的数据治理安排应该在其药物质量体系内形成文件，并进行定期审核。

5.3 Risk management approach to data governance 数据治理的风险管理方法

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. The frequency of such reviews should be based on the criticality of the services provided by the contract acceptor, using risk management principles (refer to section 10).

高级管理层负责实施系统和程序，从而最大限度地降低数据完整性的潜在风险，并使用 ICH Q9 的原则识别残余风险。合同委托方应审查合同受托方的数据管理政策和控制策略，作为其供应商保证计划的一部分。此类审查的频率应基于合同受托方提供的服务的重要性使用风险管理原则（参见第 10 节）。

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 manufacturers, analytical laboratories, 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 documented with supporting rationale.

分配给数据治理的努力和资源应与产品质量风险相称，并应与其他质量资源需求相平衡。受 GMP/GDP 原则监管的所有实体（包括生产商、分析实验室、进口商和批发分销商）应设计和运行一个基于数据质量风险提供可接受控制状态的系统。该系统及支持理由应有记录。

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.

如果确定了长期措施以实现所需的控制状态，应实施临时措施以减轻风险，并应监测其有效性。如果需要采取临时措施或风险优先级排序，则应将剩余数据完整性风险传达给高级管理层，并不断进行审查。从自动化和计算机化系统恢复到基于纸张的系统不会消除对数据治理的需求。这种倒退的方法可能会增加管理负担和数据风险，并阻碍第 3.5 段中提到的持续改进举措。

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:

并非所有数据或处理步骤对产品质量和患者安全都具有同等重要性。应利用风险管理来确定每个数据/处理步骤的重要性。有效的数据治理风险管理方法将考虑：

- Data criticality (impact to decision making and product quality) and
- 数据关键程度（对决策和产品质量的影响）以及
- Data risk (opportunity for data alteration and deletion, and likelihood of detection / visibility of changes by the manufacturer's routine review processes).
- 数据风险（数据修改和删除的机会，生产商日常审核流程发现变化的的可能性）

From this information, risk proportionate control measures can be implemented. Subsequent sections of this guidance that refer to a risk management approach refer to 'risk' as a combination of data risk and data criticality concepts.

根据这些信息，可以实施风险比例控制措施。 本指南中涉及风险管理方法的后续部分中的“风险”指数据风险和数据关键性概念的组合。

5.4 Data criticality 数据关键程度

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:

数据影响的决策重要性可能不同，数据对决策的影响程度也可能不同。 关于数据重要性的考虑要点包括：

- Which decision does the data influence?
- 数据会影响哪个决策？

  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.

  例如：在做出批放行决定时，确定是否符合关键质量属性的数据通常比仓库清洁记录更重要。

- What is the impact of the data to product quality or safety?
- 数据对产品质量或安全有何影响？

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

  例如：对于口服片剂，API 含量数据通常比片剂脆碎度数据对产品质量和安全性的影响更大。

5.5 Data risk 数据风险

5.5.1 Whereas data integrity requirements relate to all GMP/GDP data, the assessment of data criticality will help organisations to prioritise their data governance efforts. The rationale for this prioritisation should be documented in accordance with quality risk management principles.

尽管数据完整性要求涉及所有 GMP/GDP 数据，但数据重要性评估将帮助组织确定其数据治理工作的优先级。应根据质量风险管理原则记录这种优先排序的基本原理。

5.5.2 Data risk assessments should consider the vulnerability of data to involuntary alteration, deletion, loss (either accidental or by security failure) or re-creation or deliberate falsification, and the likelihood of detection of such actions. Consideration should also be given to ensuring complete and timely 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.

数据风险评估应考虑数据对非自愿更改、删除、丢失（意外或安全故障）或重新创建或故意篡改的弱点，以及检测到此类行为的可能性。还应考虑在发生灾难时确保及时完整地恢复数据。防止未经授权的活动和提高可见性/可检测性的控制措施可用作风险缓解措施。

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

可增加数据故障风险的因素例子包括复杂或不统一，具有开放式和主观结果的流程。具有统一、明确和客观任务的简单流程可降低风险。

5.5.4 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 information technology (IT) system functionality or complexity. Factors to consider include:

风险评估应侧重于业务流程（例如生产、QC）、评估数据流以及生成和处理数据的方法，而不仅仅是考虑信息技术 (IT) 系统的功能或复杂性。需要考虑的因素包括：

- process complexity (e.g. multi-stage processes, data transfer between processes or systems, complex data processing);
- 工艺复杂性（例如，多段工艺，工艺或系统之间的数据转移，数据处理的复杂性）；
- methods of generating, processing, storing and archiving data and the ability to assure data quality and integrity;
- 生成、处理、存储和归档数据的方法，以及保证数据质量和完整性的能力；
- process consistency (e.g. biological production processes or analytical tests may exhibit a higher degree of variability compared to small molecule chemistry);
- 工艺一致性（例如，相比于小分子化学，生物生产工艺或分析检测可能有较高变异性）；
- degree of automation / human interaction;
- 自动化/人工干预程度；
- subjectivity of outcome / result (i.e. is the process open-ended vs well defined);
- 结果的主观性（即工艺开放式结束 VS 良好界定）；
- outcomes of a comparison between electronic system data and manually recorded events (e.g. apparent discrepancies between analytical reports and raw-data acquisition times); and
- 电子系统数据和人工记录的事件之间的比较结果（例如分析报告和原始数据采集时间之间的明显差异）；以及
- inherent data integrity controls incorporated into the system or software.
- 集成在系统或软件中的内在数据完整性控制。

5.5.5 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.

对于计算机化系统，在风险评估过程中应考虑与 IT 系统的手动接口。计算机化系统验证单独可能不会导致低数据完整性风险，特别是如果用户能够影响已验证系统的数据报告，并且系统验证不满足本文节 9 中概述的基本要求。完全自动化和经过验证的流程以及不允许人为干预或将人为干预降至最低的配置是更可取的，因为这种设计降低了数据完整性风险。如果由于技术原因无法进行集成控制，则应安装适当的程序控制并验证。

5.5.6 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.

检查员应使用批判性思维技能来确定控制和审核程序是否有效地实现了其预期结果。数据治理成熟度的一个指标是组织对残余风险的理解和接受，这会用于指导优先安排哪些措施。认为数据完整性失败“没有风险”的组织不太可能对数据生命周期中的固有风险进行充分评估。因此，应详细检查评估数据生命周期、关键性和风险的方法。这可能表明可以在检查期间调查的潜在故障模式。

5.6 Data governance system review 数据治理系统审核

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 数据完整性控制措施的有效性应作为自检（内审）或其它定期审核流程的一部分进行定期评估。应使其确保在数据生命周期中的控制措施按预期运行。

5.6.3 In addition to routine data verification checks (e.g. daily, batch- or activity- related), self-inspection activities should be extended to a wider review of control measures, including:

5.6.4 除了常规数据核查以外（例如每日，每批或每个活动），应将自检活动扩展到更为广泛的控制措施审核，包括：

- 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).
- 检查员工是否持续理解在保护患者的背景下的优良数据管理规范，并确保维护以质量和公开报告问题为重点的工作环境（例如，对优良数据管理规范原则和要求的持续培训进行审核）。
- A review for consistency of reported data/outcomes against raw entries. This may review data not included during the routine data verification checks (where justified based on risk), and/or a sample of previously verified data to ensure the continued effectiveness of the routine process.
- 对所报告数据/结果与原始信息的一致性进行审核。这可能要审核未包括在例行数据验证检查中的数据（根据风险进行论证）和/或先前验证的数据样本，以确保例行流程的持续有效性。
- A risk-based sample of computerised system logs / audit trails to ensure that information of relevance to GMP/GDP activity is reported accurately. This is

relevant to situations where routine computerised system data is reviewed manually or by a validated 'exception report[4]'.

- 基于风险的计算机化系统日志/审计追踪样本，以确保准确报告与 GMP/GDP 活动相关的信息。这与常规计算机化系统数据审核是手动还是通过经过验证的"异常报告"审核有关。
- A review of quality system metrics (i.e. trending) that may also be indicators of data governance effectiveness.
- 对质量系统指标（即趋势）的审查，这些指标也可能是数据治理有效性的指标。

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

对数据治理系统的有效审核将可证明公司理解公司行为与管理和技术控制之间的互动的重要性。审核结果应该与高级管理层进行沟通，并用于评估残余数据完整性风险。

6 ORGANISATIONAL INFLUENCES ON SUCCESSFUL DATA INTEGRITY MANAGEMENT 组织对数据完整性管理成功与否的影响

6.1 General 概述

6.1.1 It may not be appropriate or possible to report an inspection deficiency 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.

报告与组织行为有关的检查缺陷可能不适当或不可能。了解行为如何影响 (i) 修改、删除或伪造数据的动机和 (ii) 设计用于确保数据完整性的程序控制的有效性，可以为检查员提供有用的风险指标，从而对这些风险进行深入调查。

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. However, where it is apparent that cultural approaches have led to data integrity concerns; these concerns should be effectively and objectively reported by the inspector to the organisation for rectification.

检查员应对文化对组织行为的影响保持敏感，并以适当的方式应用本指南中描述的原则。有效的"质量文化"和数据治理在不同场所的实施过程中可能会有所不同。如果文化方法很明显地导致了数据完整性问题，则检查员应该将这些问题客观有效地报告给组织进行纠正。

6.1.3 Depending on culture, an organisation's control measures may be: 根据文化，组织的控制措施可能是：

- 'open' (where hierarchy can be challenged by subordinates, and full reporting of a systemic or individual failure is a business expectation)
- "开放的"（在这种情况下，下属可以挑战等级制度，并且对系统或个人失败进行完整报告是业务要求）
- 'closed' (where reporting failure or challenging a hierarchy is culturally more difficult)

[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. "异常报告"是一种经过验证的检索工具，可发现并记录预先设定的"异常"数据或动作，它需要由数据审核人员进一步关注或调查。

- “封闭的”（报告失败或挑战等级制度在文化上更困难）

6.1.4 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.

在“开放的”文化中可以通过授权员工通过药品质量体系识别和报告问题来促进优良数据治理。在“封闭的”文化中，由于交流不想要的信息存在社会障碍，可能需要更加强调监督和二次审查，以实现等同水平的控制。在这种情况下，采用保密方式将问题升级提交至高级管理人员可能更为重要，这些安排应清楚地表明高级管理人员积极支持和鼓励报告。

6.1.5 The extent of Management’s knowledge and understanding of data integrity can influence the organisation’s success of data integrity management. Management should 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.

管理层对数据完整性的知识和理解程度会影响组织数据完整性管理的成功。管理层应该了解他们的法律和道德义务（即职责和权力），以防止发生数据完整性问题，并在发生时能够发现。管理层应该对纸质和计算机化（混合和电子）工作流的数据完整性风险有足够的可见性和理解。

6.1.6 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 undue pressure, incentives for productivity in excess of process capability, opportunities for compromising data and employee rationalisation of negative behaviours) should be understood and addressed as well.

数据完整性问题不仅限于欺诈或篡改；它们可能是无意的，但仍会带来风险。任何损害数据可靠性的可能性都是一种风险，应该识别和了解以便实施适当的控制（参见第 5.3 - 5.5 节）。直接控制通常采取书面政策和程序的形式，但亦应了解对员工行为的间接影响（例如过度压力、超过流程能力的生产力激励、破坏数据的机会和员工将负面行为合理化），并解决之。

6.1.7 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.

任何员工可能在任何时间发生数据完整性违规，因此管理层需要在发现问题时保持警惕并了解失误背后的原因，以便调查问题并实施纠正和预防措施。

6.1.8 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.

数据完整性问题会影响各种利益相关者（患者、监管机构、客户），包括直接影响患者安全和破坏对组织及其产品的信心。员工对这些后果的认识和理解有助于营造质量优先的环境。

6.1.9 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.

管理层应建立控制措施以防止、发现、评估和纠正数据完整性破坏情况，并验证是否按预期执行了这些控制措施，从而确保数据完整性。第 6.2 至 6.7 节概述了管理层应解决的关键项目，以成功实现数据完整性。

6.1.10 Senior Management should have an appropriate level of 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.

高级管理层应对有效的数据治理规范有适当的理解和承诺，包括结合适当的组织文化和行为（第 6 节）的必要性，并且理解数据关键性、数据风险和数据生命周期。应有证据证明向组织内各层级人员就相关要求进行了沟通，沟通方式可以确保鼓励报告失败，提供改进机会。这样可减少伪造、更改或删除数据的动机。

6.2 Policies related to organisational values, quality, staff conduct and ethics 与组织价值观、质量、员工行为和道德有关的政策

6.2.1 Appropriate expectations for staff conduct, commitment to quality, organisational values and ethics should clearly communicated throughout the organisation and policies should be available to support the implementation and maintenance of an appropriate quality culture. Policies should reflect Management's philosophy on quality, and 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.

应在整个组织内清楚地传达对员工行为、质量承诺、组织价值观和道德的适当期望，并应提供政策以支持实施和维护适当的质量文化。政策应反映管理层的质量理念，并应着眼于营造信任环境，让所有人对确保患者安全和产品质量负责。

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.

管理层应让员工意识到他们在确保数据质量方面的作用的重要性以及他们的活动对确保产品质量和保护患者安全的意义。

6.2.3 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.

政策应明确规定对道德行为的期望，例如诚实。应将政策传达给所有人员并让他们充分理解。沟通不应仅限于了解要求，还应了解为何建立要求以及未能满足要求的后果。

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 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 into the data integrity issues identified, e.g. severe retribution may prevent other staff members from disclosing information of value to the investigation.

应及时解决不良行为问题，例如故意篡改数据、未经授权的更改、破坏数据或其他损害数据质量的行为。不良行为和态度的例子应记录在公司政策中。应书面规定准备对不良行为采取的措施。但是，应注意确保所采取的行动（例如纪律处分）不会妨碍对已发现的数据完整性问题的任何后续调查，例如：严厉报复可能会阻止其他工作人员披露对调查有价值的信息。

6.2.5 The display of behaviours that conform to good practices for data management and integrity should be actively encouraged and recognised appropriately.

应积极鼓励和适当认可符合数据管理和完整性优良规范的行为。

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

应该有一个由公司政策和程序支持的保密升级计划，它鼓励员工将可能违反政策的情况提请高级管理人员注意，而不会对举报人/员工造成任何后果。应认识到高级管理人员违反政策的可能性，并应为这些情况提供合适的报告机制。

6.2.7 Where possible, management should implement systems with controls that by default, uphold the intent and requirements of company policies.

在可能的情况下，管理层应实施默认带有控制的系统，以支持公司政策的意图和要求。

6.3 Quality culture 质量文化

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.

管理层应致力于创建一种透明开放的工作环境（即质量文化），鼓励员工自由交流故障和错误，包括潜在的数据可靠性问题，以便采取纠正和预防措施。组织报告结构应允许各级人员之间的信息流通。

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.

质量文化是管理层、团队负责人、质量人员和所有有助于创建质量文化以确保数据质量和完整性的人员一致展示的价值观、信念、思维和行为的集合。

6.3.3 Management can foster quality culture by:

管理层可以通过以下方式培养质量文化：

- Ensuring awareness and understanding of expectations (e.g. Code of Values and Ethics and Code of Conduct),
- 确保明白和理解要求什么（例如价值观和道德准则以及行为准则），
- Leading by example, management should demonstrate the behaviours they expect to see,
- 以身作则，管理层应展示他们期望看到的行为，
- Being accountable for actions and decisions, particularly delegated activities,
- 对行动和决定负责，尤其是委派的活动，
- Staying continuously and actively involved in the operations of the business,

- 持续并积极参与业务运营，
- Setting realistic expectations, considering the limitations that place pressures on employees,
- 设定切合实际的期望，考虑给员工施加压力的局限性，
- Allocating appropriate technical and personnel resources to meet operational requirements and expectations,
- 配置适当的技术和人力资源以满足运营要求和期望，
- Implementing fair and just consequences and rewards that promote good cultural attitudes towards ensuring data integrity, and
- 实施公平公正的结果和奖励，以促进良好的文化态度，确保数据完整性，以及
- Being aware of regulatory trends to apply "lessons learned" to the organisation.
- 了解监管趋势，将"经验教训"应用于组织。

6.4 Modernising the Pharmaceutical Quality System 药物质量体系的现代化

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.

将现代质量风险管理原则和优良数据管理规范应用于现行药物质量体系可使得系统现代化，应对复杂数据产生带来的挑战。

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:

公司的药物质量体系应该能够防止、发现和纠正系统弱点或可能导致数据完整性问题的流程。公司应该知晓其数据生命周期，并结合适当的控制措施和程序，使得所生成的数据有效、完整和可靠。具体来说，此类控制和程序性变化可能反映在以下方面：

- Quality Risk Management,
- 质量风险管理，
- Investigation programs,
- 调查程序，
- Data review practices (section 9),
- 数据审核规范（节 9），
- Computerised system validation,
- 计算机化系统验证，
- IT infrastructure, services and security (physical and virtual),
- IT 设施，服务和安全保护（物理和虚拟），
- Vendor/contractor management,
- 供应商/分包方管理，
- Training program to include company's approach to data governance and data governance SOPs,

- 培训程序中包括公司的数据治理方法和数据治理 SOP，
- Storage, processing, transfer and retrieval of completed records, including decentralised/cloud-based data storage, processing and transfer activities,
- 已完成记录的存储、处理、转移和检索，包括去中心化/云端数据存贮、处理和转移活动，
- Appropriate oversight of the purchase of GMP/GDP critical equipment and IT infrastructure that incorporate requirements designed to meet data integrity expectations, e.g. User Requirement Specifications, (Refer section 9.2)
- 对 GMP/GDP 关键设备和 IT 设施的采购的适当监管，在其中包括设计用于满足数据完整性要求的需求，例如用户需求说明（见节 9.2），
- Self-inspection program to include data quality and integrity, and
- 自检程序，包括数据质量和完整性，以及
- Performance indicators (quality metrics) and reporting to senior management.
- 绩效指标（质量量度）和向高级管理层报告。

6.5 Regular management review of performance indicators (including quality metrics)
绩效指标的定期管理审评（包括质量量度）

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.

应该对绩效指标进行定期管理审评，包括与数据完整性有关的指标，这样可及时识别出严重问题，升级并解决。选择关键绩效指标时应谨慎，以免无意中导致数据完整性优先级较低的文化。

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.

质量部门的负责人应能直接接触高级管理人员，以便直接沟通风险，让高级管理人员了解并分配资源来解决任何问题。

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

管理层可以聘请独立专家定期查证其系统和控制的有效性。

6.6 Resource allocation 资源配置

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.

管理层应分配适当的资源来支持和维护良好的数据完整性管理，这样负责数据生成和记录保存的人员的工作量和压力不会增加出错的可能性或故意破坏数据完整性的机会。

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.

应有足够数量的人员进行质量和管理监督、IT 支持、实施调查以及与组织运营相称的培训计划管理。

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+[5] principles and thus mitigate weaknesses in relation to data quality and integrity.

应根据相关数据的关键程度，规定购买适合其需要的设备、软件和硬件。公司应实施技术解决方案，以提高对 ALCOA+ 原则的遵守情况，从而减轻与数据质量和完整性相关的弱点。

6.6.4 Personnel should be qualified and trained for their specific duties, with appropriate segregation of duties, including the importance of good documentation practices (GdocPs). 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/GDP, including areas such as IT and engineering.

人员应经过资格确认，并就其特定职责（职责分离），包括良好文档实践 (GdocP) 的重要性进行培训。应该有证据证明关键程序培训的有效性，例如电子数据审核。优良数据管理规范的概念适用于在 GMP/GDP 中发挥作用的所有职能部门，包括 IT 和工程等领域。

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.

数据质量和完整性应该为所有人所熟悉，但可能需要各级（中小企业、主管、团队领导）的数据质量专家共同开展/支持调查、确定系统差距并推动实施改进。

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

可以考虑在组织中引入与优良数据管理相关的新角色，例如数据保管人。

6.7 Dealing with data integrity issues found internally 内部发现的数据完整性问题的处理

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.

如果发现数据完整性缺失，应按照药品质量体系作为偏差进行处理。重要的是要确定问题的严重程度及其根本原因，然后全面纠正问题并实施预防措施。这可能包括使用第三方获得额外的专业知识或观点，可能涉及差距评估，以确定系统中的弱点。

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

在考虑对患者安全和产品质量的影响时，得出的任何结论都应有可靠的科学证据支持。

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.

纠正措施可能包括产品召回、客户通知和向监管机构报告。应记录和监控纠正行为和纠正行动计划及其实施。

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

更多指导参见本指南的第 12 节。

[5] EMA guidance for GCP inspections conducted in the context of the Centralised Procedure EMA 的集中程序 GCP 检查指南

7 GENERAL DATA INTEGRITY PRINCIPLES AND ENABLERS 一般数据完整性原则和推动力

7.1 The Pharmaceutical Quality System 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.

应在原料药和制剂生命周期的不同阶段实施药品质量体系，并应鼓励使用基于风险的科学方法。

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 are key to ensuring data integrity, and a fundamental part of a well-designed Pharmaceutical Quality System (discussed in section 6).

为确保决策充分知情并验证信息的可靠性，应充分记录为这些决策提供信息的事件或行动。因此，优良文件规范是确保数据完整性的关键，也是精心设计的药品质量体系的基本组成部分（在第 6 节中讨论）。

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.

GdocP 的应用可能因记录数据所用介质（即物理记录与电子记录）而异，但原则适用于两者。本节将介绍这些关键原则，随后的第 8 节和第 9 节将探讨与纸质和电子方式保存的文件相关的这些原则。

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+[6]). Together, these expectations ensure that events are properly documented and the data can be used to support informed decisions.

GdocP 的一些关键概念采用首字母概括为 ALCOA：可归属、清晰、同步、原始和准确。以下属性可以添加到列表中：完整、自洽、持久和可用 (ALCOA+)。这些要求共同确保事件得到正确记录，并且数据可用于支持知情决策。

7.5 Basic data integrity principles applicable to both paper and electronic systems (i.e. ALCOA +):

适用于纸质和电子系统（即 ALCOA+）的基本数据完整性原则：

Data Integrity Attribute **数据完整性属性**	**Requirement** **要求**
Attributable	It should be possible to identify the individual or computerised system that performed a recorded task and when the task was performed. This also applies to any changes made to records, such as corrections, deletions, and changes where it is important to know who made a change, when, and why.
可归属性	应该可以识别出实施了被记录的任务的个人身份，以及任何执行时间。这也适用于对记录所做的所有变更，如记录更正、删除和修改，此时知晓是何人何时为何做出该动作很重要。
Legible	All records should be legible – the information should be readable and unambiguous in order for it to be understandable and of 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,

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

	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.
清晰	所有记录均应清晰---信息必须可以毫不含糊地被读出，以便理解和使用。此要求适用于所有可能被认为是完整的信息，包括所有原始记录和信息。如果电子数据的“动态”属性（能够进行搜索、查询、趋势分析等）对于记录的内容和含义很重要，则使用适当的软件与数据互动的能力对于记录的“可及性”就很重要。
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.
同步	动作、事件或决策的证据应在其发生时记录。此记录应作为做了什么、决定了什么以及为什么的准确证明，即在当时是什么影响了决策。
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.
原始	原始记录可以被描述为首次捕获的信息，可以是记录在纸上（静态），也可以是电子的（通常是动态的，取决于系统的复杂性）。原始以动态状态捕获的信息应保持在该状态可及。
Accurate	Records need to be a truthful representation of facts to be accurate. Ensuring 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.
准确	记录应该真实代表准确的事实。确保记录准确是通过稳健的药物质量体系的多个要素达成的。其中可包括： • 与设备相关的因素，如确认、校正、维护和计算机验证 • 控制措施和行为的方针和程序，包括用以核查是否符合程序要求的数据审核程序 • 偏差管理，包括根本原因分析，影响分析和 CAPA • 受过培训的有资质的人员了解遵守既定程序和记录其活动和决策的重要性 这些要素一起保证信息的准确性，包括用于做出关于产品质量关键决策的科学数据。
Complete	All information that would be critical to recreating an event is important when trying to understand the event. It is important that information is not lost or deleted. The level of detail required for an

	information set to be considered 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).
完整	当试图了解一件事情时，所有在还原该事件时关键的信息都是重要的。信息未曾丢失或被删除很重要。一个数据集被认为完整而需的详细程度取决于信息的关键程度（参见节5.4数据关键程度）。以电子方式生成的数据的完整记录包括相关的元数据（参见节9）。
Consistent	Information should be created, processed, and stored in a logical manner that has a defined consistency. This includes policies or procedures that help control or standardize data (e.g. chronological sequencing, date formats, units of measurement, approaches to rounding, significant digits, etc.).
一致	信息创建、处理和存贮的方式应具有逻辑自洽性。其中包括控制或标准化数据的政策和程序（例如，时序、日期格式、测量单位、修约方法、有效数字等）。
Enduring	Records should 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.
持久	应保存记录，使其在可能需要的时间段都存在。这意味着需要在记录保存期限内将其保存为清晰持久的记录，完好无损并可访问。
Available	Records should 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.
可获得	记录必须在其所要求的保存期间随时可以获得用于审核，负责其日常放行决策、调查、趋势分析、年报、审核或检查中审核的所有适合的人员都能可读格式获得。

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.

如果这些要素恰当应用于所有 GMP 和 GDP 相关活动领域，与其它 PQMS 的支持要素一起，就能充分保证用于做出药品关键决策的信息的可靠性。

7.7 True copies 真实副本

7.7.1 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 should 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).

原始纸质记录的副本（例如分析摘要报告、验证报告等）通常在沟通中颇为有用，例如在不同地点运营的公司之间。这些记录应该在其生命周期内受控，以确保在适当时将从另一场所接受的数据保存为"真实副本"，或者如果不满足"真实副本"的要求的话，可当作"摘要报告"使用（例如，复杂分析数据的摘要）。

7.7.2 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 should

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.

可以想象电子方式生成的原始数据被保存在可接受的纸张中或以 PDF 格式保存，此时需要论证静态记录仍保存了原始数据的完整性。但是，数据保存流程应该记录所有直接或间接影响药品质量所有方面的活动（例如，分析记录可能包括有原始数据、元数据、相关审计追踪和结果文件、每项分析运行特有的软件系统参数设置，以及重建指定原始数据系列所需的所有数据处理动作（包括方法和审计追踪））的所有数据（包括元数据）。还应要求采用书面手段核查打印出的记录准确代表该活动。要得到符合 GMP/GDP 的记录，此种方法可能在管理方面任务很繁重。

7.7.3 Many electronic records are important to retain in their dynamic format, to enable interaction with the data. Data should 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.

很多电子记录要保持其动态格式，这对于与数据互动来说甚为重要。如果数据的动态形式对于其完整性或者后期的核查来说至关重要，则应以动态形式保存此类数据。应使用风险管理原则支持和论证是否要采用动态格式保存数据，以及要保存多长时间。

7.7.4 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.

在接收场所，这些记录（真实副本）有可能是采用纸质或电子格式（如 PDF）管理的。应该按批准的 QA 程序对其进行控制。

7.7.5 Care should be taken to ensure that documents are appropriately authenticated as “true copies” in a manner that allows the authenticity of the document to be readily verified, e.g. through the use of handwritten or electronic signatures or generated following a validated process for creating true copies.

应注意确保文件被恰当认证为“真实副本”，认证方式应该使得文件易于核查，例如，通过使用手书或电子签名，或使用经过验证的真实副本创建过程制作。

Item	**How should the “true copy” be issued and controlled?** **应如何发放和控制“真实副本”？**
1.	**Creating a “true copy” of a paper document.** **创建一份纸质文件的“真实副本”** At the company who issues the true copy: 公司里谁发放真实副本： - Obtain the original of the document to be copied - 获得要复制的文件原件 - Photocopy the original document ensuring that no information from the original copy is lost; - 对原始文件进行复印，确保原件中的信息不会丢失 - Verify the authenticity of the copied document and sign and date the new

hardcopy as a "true copy";

- 核查复制文件的真实性，并在新的纸质副本上签名/日期认可其为"真实副本"

The "True Copy" may now be sent to the intended recipient.

"真实副本"现在可以发给意向接收方。

Creating a "true copy" of a electronic document.

创建一份电子文件的"真实副本"

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 prohibited, where there is the potential for loss of metadata.

一份电子记录的"真实副本"应该采用电子方式创建（电子文件副本），包括所有所需的元数据。应禁止创建电子数据的 PDF 版本，这种方式可能会丢失元数据。

The "True Copy" may now be sent to the intended recipient.

"真实副本"现在可以发给意向接收方。

A distribution list of all issued "true copies" (soft/hard) should be maintained.

应保存所的已发放的"真实副本"（软/硬副本）的发放清单。

Specific elements that should be checked when reviewing records:

审核记录时要检查的特定要素

- Verify the procedure for the generation of true copies, and ensure that the generation method is controlled appropriately.
- 查证生成真实副本的程序，确保生成方法适当受控
- Check that true copies issued are identical (complete and accurate) to original records. Copied records should be checked against the original document records to make sure there is no tampering of the scanned image.
- 检查签发的真实副本与原始记录是相同的（准确完整）。复制的记录应该与原始文件记录进行比对检查，确保不是使用扫描图片进行篡改的。
- Check that scanned or saved records are protected to ensure data integrity.
- 检查扫描或保存的记录是否受到保护，确保数据完整性
- After scanning paper records and verifying creation of a 'true copy':
- 在扫描纸质记录查证创建一份"真实副本"之后

  – Where true copies are generated for distribution purposes, e.g. to be sent to a client, the original documents from which the Where true copies are generated for distribution purposes, e.g. to be sent to a client, the original documents from which the scanned images have been created should be retained for the respective retention periods by the record owner. （译注：黄色背景文原文如此，应该是制作时重复了，翻译时省去）

  – 如果制作真实副本是为了发放，例如发给客户，则记录所有者应保存创建扫描图片所用的原始文件至相应的保存时限

  – Where true copies are generated to aid document retention, it may be possible to retain the copy in place of the original records documents from which the scanned images have been created.

  – 如果制作真实副本是为了帮助保存文件，则可保存副本，取代创建扫描图片所用的原始文件

2.	At the company who receives the true copy: 接收真实副本的公司： – The paper version, scanned copy or electronic file should be reviewed and filed according to good document management practices. – 应根据优良文件管理规范审核并保存纸质版本、扫描副本或电子文件 The document should clearly indicate that it is a true copy and not an original record. 文件应清楚注明是真实副本，不是原始记录。 **Specific elements that should be checked when reviewing records:** **在审核记录时要检查的特定要素** • Check that received records are checked and retained appropriately. • 检查所收到的记录是否经过合适的检查并得到保存 • A system should be in place to verify the authenticity of "true copies" e.g. through verification of the correct signatories. • 应有系统用于查证"真实副本"的真实性，例如通过查证签名正确性

7.7.6 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.

应签有质量协议说明"真实副本"的生成和转移职责以及数据完整性控制措施。签发和控制"真实副本"的系统应该由委托方和接收方进行审计，确保该流程的稳健性，且符合数据完整性原则。

7.8 Limitations of remote review of summary reports 远程审核摘要报告的局限性

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

远程审核摘要报告中的数据通常是必须的，但是要全面了解远程数据审核的局限性，采取措施充分控制数据完整性。

7.8.2 Summary reports of data are often supplied between physically remote manufacturing sites, Market Authorisation Holders and other interested parties. However, it should 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.

数据摘要报告通常是提供给有空间距离的生产场所、上市许可持有人和其它利益方的。但是应知晓摘要报告本质上是受限的，它通常并不包括关键支持性数据和元数据，因此无法审核原始数据。

7.8.3 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.

因此摘要报告仅能看作是数据转移的一个流程，兴趣方和检查员不能仅依赖于摘要报告数据。

7.8.4 Prior to acceptance of summary data, an evaluation of the supplier's quality system and compliance with data integrity principles should be established. It is not normally acceptable nor possible to determine compliance with data integrity principles through the use of a desk-top or similar assessment.

在接受摘要数据之前，应评估供应商的质量体系及其符合数据完整性原则的程度。一般不能接受也不太可能通过使用远程或类似评估确定是否符合数据完整性原则。

7.8.4.1 For external entities, this should be determined through on-site audit when considered important in the context of quality risk management. The audit 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.

对于外部实体，如果认为其在质量风险管理中很重要，则应该通过现场审核进行确认。审计应确保公司所生成数据的真实性，审计要包括对数据和报告生成和分发机制的审核。

7.8.4.2 Where summary data is distributed between different sites of the same organisation, the evaluation of the supplying site's compliance may be determined through alternative means (e.g. evidence of compliance with corporate procedures, internal audit reports, etc.).

如果摘要数据是同一组织内不同场所之间相互分发，则可以通过替代方法（例如符合公司程序的证据、内部审计报告等）来评估提供报告的场所的合规性。

7.8.5 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.

摘要数据应该根据协定的程序制作，并由出具数据的场所授权员工审核和批准。摘要应该有一份由授权人员签字的声明，声明摘要的真实性和准确性。摘要报告的制作、转移和查证方法应在质量/技术协议中进行说明。

8 SPECIFIC DATA INTEGRITY CONSIDERATIONS FOR PAPER- BASED SYSTEMS 纸质系统特有的数据完整性考量

8.1 Structure of Pharmaceutical Quality System and control of blank forms/templates/records 药物质量体系的结构和空白表格/模板/记录的控制

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.

有效的纸质文件管理是 GDMP/GDP 的一个关键要素。相应地，文件系统设计应该符合 GDMP/GDP 要求，确保文件和记录得到有效的控制，从而保证其完整性。

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

纸质记录应该受控，应该保持其在数据生命周期内的可归属性、清晰、同步、原始和准确、完整、自洽性、持久性（不易磨灭/耐用）和可及性（ALCOA+）。

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

药物质量体系内应该制订有程序，列出优良文件规范和文件控制安排。这些程序应该说明如何在数据的生命周期内维持数据完整性，包括：

- creation, review, and approval of master documents and procedures;
- 创建、审核和批准主文件和程序；

- generation, distribution and control of templates used to record data (master, logs, etc.);
- 生成、发放和控制用于记录数据的模板（主记录、日志等）；
- retrieval and disaster recovery processes regarding records;
- 记录恢复和灾难恢复过程；
- 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;
- 日常使用的工作副本文件制作，特别要强制确保文件（例如 SOP）和空白表格的副本的发放和数量平衡是受控可追溯的；
- completion of paper based documents, specifying how individual operators are identified, data entry formats, recording amendments, and routine review for accuracy, authenticity and completeness; and
- 纸质记录的填写，说明如何识别操作员身份、数据录入格式、记录修改和日常准确性、真实性和完整性审核；以及
- filing, retrieval, retention, archival and disposal of records.
- 记录填写、检索、保存、归档和处置。

8.2 Importance of controlling records 控制记录的重要性

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

记录对于 GMP/GDP 操作来说是非常关键的，因此必须加以控制从而确保：

- evidence of activities performed;
- 所实施活动的证据；
- evidence of compliance with GMP/GDP requirements and company policies, procedures and work instructions;
- 符合 GMP/GDP 要求和公司政策、程序和工作指令的证据；
- effectiveness of Pharmaceutical Quality System;
- 药物质量体系的有效性；
- traceability;
- 可追溯性；
- process authenticity and consistency;
- 工艺真实性和一致性；
- evidence of the good quality attributes of the medicinal products manufactured;
- 所生产的药品具备优良质量属性的证据；
- in case of complaints or recalls, records could be used for investigational purposes; and
- 如果有投诉或召回，可使用记录进行调查；且
- in case of deviations or test failures, records are critical to completing an effective investigation.
- 如果有偏差或检测失败，记录对于完成有效调查来说是很关键的。

8.3 Generation, distribution and control of template records 制作、分发和控制记录模板

8.3.1 Managing and controlling master documents 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).

管理和控制主文件对于确保将一些人通过“常规手段”（即不需要使用特殊的造假技巧）不当使用和/或伪造记录的风险降低至可接受程度是很有必要的。应该主使用质量风险管理方法，同时考虑所记录数据的风险和关键程度执行以下要求（参见节 5.4，5.5）。

8.4 Expectations for the generation, distribution and control of records 制作、发放和控制记录的要求

Item 项目	Generation 制作
1.	**Expectation 要求** All documents should have a unique identifier (including the version number) and should be checked, approved, signed and dated. 所有文件均应有唯一识别号（包括版本号），应该经过检查、批准、签名并签署日期。 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. 本地程序应禁止使用不受控的文件。应禁止使用临时记录，如草稿纸。 **Potential risk of not meeting expectations/items to be checked** **不符合要求的潜在风险/要检查的项目** • Uncontrolled documents increase the potential for omission or loss of critical data as these documents may be discarded or destroyed without traceablility. In addition, uncontrolled records may not be designed to correctly record critical data. • 不受控文件会增加删除或丢失关键数据的可能性，因为这些文件可能会被丢弃或销毁，且没有可追溯性。另外，不受控记录的设计可能无法正确记录关键数据。 • It might be easier to falsify uncontrolled records. • 可能更易于伪造不受控记录。 • Use of temporary recording practices may lead to data omission, and these temporary original records are not specified for retention. • 使用临时记录的做法可能会导致数据遗漏，且这些临时原始记录没有保存要求。 • 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. • 如果可以不经控制地创建和访问记录，则这些记录有可能并不是在事件发生当时所记录的。 • There is a risk of using superseded forms if there is no version control or controls for issuance. • 如果没有版本控制或者发放控制，有使用旧表格的风险。
2	**Expectation 要求** The document design should provide sufficient space for manual data entries.

	文件设计应有足够的手工填写数据空间。 **Potential risk of not meeting expectations/items to be checked** **不符合要求的潜在风险/要检查的项目** • Handwritten data may not be clear and legible if the spaces provided for data entry are not sufficiently sized. • 如果所提供的数据填写空间不够大，手写数据可能不清楚不清晰。 • 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. • 文件应设计有足够的空间填写备注，例如，如果有转抄错误，应有足够的空间让操作员划掉错误，签名日期，然后记录所需的解释。 • 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. • 如果文件有加页，应在主记录页上清楚写明所加页数和索引并签名。 • Sufficient space should be provided in the document format to add all necessary data, and data should not be recorded haphazardly on the document, for example to avoid recording on the reverse of printed recording on the reverse of printed pages which are not intended for this purpose. • 应在文件格式中提供足够的空间，使得可以添加所有必要数据。数据不应随意记录在文件上，例如，应避免记录在打印记录的打印页背面，这个背面不是用来干这个的。
3	**Expectation 要求** The document design should make it clear what data is to be provided in entries. 文件设计应该清楚，让人明白哪个栏目写哪个数据。 **Potential risks of not meeting expectations/items to be checked** **不满足要求的潜在风险/要检查的项目** • Ambiguous instructions may lead to inconsistent/incorrect recording of data. • 指令不清楚可能会导致数据记录不一致/不正确。 • Good design ensures all critical data is recorded and ensures clear, contemporaneous and enduring (indelible/durable) completion of entries. • 良好的设计能确保所有关键数据得到记录，并确保清楚录入数据填写的同步性和持久性（不易磨灭/耐用）。 • 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. • 文件结构设计应该按操作流程 P 顺序和相关 SO 记录信息，以尽可能降低无意遗漏关键数据的风险。
4	**Expectation 要求** Documents should be stored in a manner which ensures appropriate version control. 文件保存应确保合适的版本控制。 Master documents should contain distinctive marking so to distinguish the master from

	a copy, e.g. use of coloured papers or inks so as to prevent inadvertent use. 主文件应该包括有显眼的记号，使主文件和副本有明显区别，例如使用彩纸或彩墨，防止无意误用。 Master documents (in electronic form) should be prevented from unauthorised or inadvertent changes. 主文件（电子格式）应能防止未经授权或无意修改。 E.g.: For the template records stored electronically, the following precautions should be in place: 例如，以电子形式保存的记录模板，应该有以下预防措施： - access to master templates should be controlled; - 主模板的访问应受控； - process controls for creating and updating versions should be clear and practically applied/verified; and - 创建和更新版本的流程控制措施应该清楚，并易于操作/查证；且 - master documents should be stored in a manner which prevents unauthorised changes. - 主文件保存时应防止未经授权的修改。 **Potential risk of not meeting expectations/items to be checked** **不满足要求的潜在风险/要检查的项目** • Inappropriate storage conditions can allow unauthorised modification, use of expired and/or draft documents or cause the loss of master documents. • 不适合的存贮条件可能会允许未经授权的修改，使用过期的和/或草稿文件或导致主文件丢失。 • The processes of implementation and the effective communication, by way of appropriate training prior to implementation when applicable, are just as important as the document. • 实施和有效沟通（通过适用时在实施之前进行合适的培训）过程与文件一样重要。
Item 项目	**Distribution and Control 分发和控制**
1	**Expectations 要求** Updated versions should be distributed in a timely manner. 更新后的版本应该及时发放。 Obsolete master documents and files should be archived and their access restricted. 过期主文件和文件应该归档并限制其访问。 Any issued and unused physical documents should be retrieved and reconciled. 所有发放的未曾使用的实物文件均应收回并核对数量。 Where authorised by Quality, recovered copies of documents may be destroyed. However, master copies of authorised documents should be preserved. 如果经过质量批准，回收的文件副本可以销毁。但是应该保存经过批准的主文件。 **Potential risk of not meeting expectations/items to be checked** **不满足要求的潜在风险/要检查的项目**

	• There may be a risk that obsolete versions can be used by mistake if available for use. • 如果可以获得失效版本，则可能存在其被误用的风险
2	**Expectation 要求** Document issuance should be controlled by written procedures that include the following controls: 应该有书面程序控制文件发放，其中包括以下控制： - details of who issued the copies and when they were issued; - 谁发放副本以及何时发放的详细说明； - clear means of differentiating approved copies of documents, e.g. by use of a secure stamp, or paper colour code not available in the working areas or another appropriate system; - 区别已批准文件副本的明确方法，例如使用工作区域所没有的安全戳，或彩纸，或者是另一种合适的系统； - ensuring that only the current approved version is available for use; - 确保只有经过批准的现行版本才可获得并使用； - allocating a unique identifier to each blank document issued and recording the issue of each document in a register; - 在所发放的每一份空白文件上均给定一个唯一识别标识，并在登记册上记录每份文件的发放； - numbering every distributed copy (e.g.: copy 2 of 2) and sequential numbering of issued pages in bound books; - 对每份发放的副本进行编号（例如，副本 2/2），对装订成册的发放页进行连续编号； - where the re-issue of additional copies of the blank template is necessary, a controlled process regarding re-issue should be followed with all distributed copies maintained and a justification and approval for the need of an extra copy recorded, e.g.: “the original template record was damaged”; - 如果需要重新发放额外的空白记录模板，应遵守重新发放的受控流程，保存所有已发放的副本，并说明原因，书面批准对额外副本的要求，例如：“原始记录模板被损坏”。 - critical GMP/GDP blank forms (e.g.: worksheets, laboratory notebooks, batch records, control records) should be reconciled following use to ensure the accuracy and completeness of records; and - 关键的 GMP/GDP 空白表格（例如，工作表，实验室记录本，批记录，检验记录）在使用之后应该平衡数量，确保记录的准确性和完整性；且 - where copies of documents other than records, (e.g. procedures), are printed for reference only, reconciliation may not be required, providing the documents are time-stamped on generation, and their short-term validity marked on the document. - 如果是非记录的文件副本（例如程序）打印出来仅供参考，则可以不进行数量平衡，前提是这些文件有生成时间戳，文件上标有很短的有效期。 **Potential risk of not meeting expectations/items to be checked** **不满足要求的潜在风险/要检查的项目** • 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). • 如果不使用安全措施，则存在影印或扫描记录模板后进行改写或伪造数据的风险（这样给用户另一个模板副本使用）。 • Obsolete versions can be used intentionally or by error. • 过期版本可能会被有意或错误地使用。 • A filled record with an anomalous data entry could be replaced by a new rewritten template. • 已填写有异常数据的记录可能会被新的重复填写的模板替换。 • All unused forms should be accounted for, and either defaced and destroyed, or returned for secure filing. • 所有未经使用的表格应该计数，划掉或者销毁，或退回安全保存。 • Check that (where used) reference copies of documents are clearly marked with the date of generation, period of validity and clear indication that they are for reference only and not an official copy, e.g. marked 'uncontrolled when printed. • 检查文件参考副本有清楚的记号，标有生成日期、有效日期，并清楚注明其仅用于参考，不是正式副本，例如标记“打印时不受控”。

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, identifier including version number, location (e.g. documentation database, effective date, next review date, etc.).

药物质量体系内应保存有一份所有已批准主文件（SOP、表格、模板和记录）的清单。该清单应该提到每种类型的记录模板，至少有以下信息：标题、识别号包括版本号、位置（例如文件数据库，有效日期，下次审核日期等）。

8.5 Use and control of records located at the point-of-use 放在使用点的记录的使用和控制

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 should be taken to protect records from being soiled (e.g. getting wet or stained by materials, etc.).

操作员在使用点应可获得记录，应该有合适的控制措施对这些记录进行管理。应执行这些控制措施以尽可能降低记录损坏或丢失风险，确保数据完整性。必要时，应该采取措施保护记录不被弄脏（例如被物料弄湿或弄脏，等）。

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

应根据书面程序指定人员或流程，对此区域的记录进行恰当控制。

8.6 Filling out records 记录填写

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

下表所列项目应该受控，确保记录的恰当填写。

Item 项目	Completion of records 记录填写
1.	**Expectation 要求** Handwritten entries should be made by the person who executed the task[7]. 手书内容应该由执行任务的人员填写。 Unused, blank fields within documents should be voided (e.g. crossed-out), dated and signed. 文件中未曾使用的空白栏应该作废（例如划掉），签名并签署日期。 Handwritten entries should be made in clear and legible writing. 手书内容的书写应该清楚明白。 The completion of date fields should be done in an unambiguous format defined for the site. E.g. dd/mm/yyyy or mm/dd/yyyy. 工厂对日期栏的填写应该有明确的格式规定，例如，2 位日/2 位月/4 位年或 2 位月/2 位日/4 位年。 **Potential risk of not meeting expectations/items to be checked** **不满足要求的潜在风险/要检查的项目** • Check that handwriting is consistent for entries made by the same person. • 检查同一人手写字迹是否一致。 • 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. （译注：此处原文有一处只有前括号，没有后括号） • 检查书写字迹是否清楚，内容是否明确（即不模糊），未使用未知符号或缩写，例如使用同上记号。 • Check for completeness of data recorded. • 检查所记录数据的完整性。 • Check correct pagination of the records and are all pages present. • 检查记录的页码是否正确，是否无缺页。
2	**Expectation 要求** Records relating to operations should be completed contemporaneously[8]. 与操作相关的记录应该同步填写完整。

[7] Scribes may only be used in exceptional circumstances, refer footnote 8. 抄写员仅可能在例外情况下使用，参见注 8。

[8] The use of scribes (second person) to record activity on behalf of another operator should be considered 'exceptional', and only take place where: 使用抄写员（第二人）代表另一操作员对活动进行记录时应该考虑“例外性”，仅可用于以下情况下：

- The act of recording places the product or activity at risk e.g. documenting line interventions by sterile operators.
- 记录动作会让产品或活动处于风险中，例如，记录无菌操作员对产线的干预。
- 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.
- 解决文化或员工文化水平/语言局限问题，例如，由一个操作员执行任务，由抄写员目击并记录。在此情况下，建议文件采用双语或将其受控翻译为本地语言和方言。

In both situations, the scribe recording should be contemporaneous with the task being performed, and should 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. 上述两种情况下，抄写员记录均应与任务执行同步，并识别执行任务的操作员和抄写员的身份。执行被观察的任务的人员应该在可能时对记录进行会签，虽然此种会签是回顾性的，但仍可以接受。抄写完整文件的流程应该有经批准的程序说明，其中要指明适用于哪些活动，并评估相关风险。

	Potential risk of not meeting expectations/items to be checked **不满足要求的潜在风险/要检查的项目** • 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. • 查证使用记录的区域可以获得记录，例如，检查员应该要求在操作现场可以进行连续记录。如果在使用点没有表格，则操作员就没法在操作时填写记录。
4	**Expectation 要求** Records should be enduring (indelible). 记录应该持久（不易磨灭）。 **Potential risk of not meeting expectations/items to be checked** **不满足要求的潜在风险/要检查的项目** • Check that written entries are in ink, which is not erasable, and/or will not smudge or fade (during the retention period). • 检查用墨水手写的内容应该不可擦除，和/或（在保存期限内）不会弄脏或褪色。 • Check that the records were not filled out using pencil prior to use of pen (overwriting). • 检查记录不是用铅笔填写然后再用钢笔书写（重写）。 • Note that some paper printouts from systems may fade over time, e.g. thermal paper. Indelible signed and dated true copies of these should be produced and kept. • 注意有些系统的打印纸随时间推移会褪色，例如热敏纸。应制备并保存此类记录的真实副本，用不褪色的笔签名并签署日期。
5	**Expectation 要求** Records should be signed and dated using a unique identifier that is attributable to the author. 记录应该使用可归属至书写人的唯一识别号签名并签署日期。 **Potential risk of not meeting expectations/items to be checked** **不满足要求的潜在风险/要检查的项目** • 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. • 检查是否有签名和首字母缩写名册，该名册应该受控和最新的，并且展示了独特示例的使用，而不仅仅是标准化的印刷字母。 • 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. • 确保所有关键书写内容均有签名&日期，尤其是如果步骤是在不同时间执行的，即不是在每页和/或工艺结束时才签名。 • The use of personal seals is generally not encouraged; however, where used, seals should be controlled for access. There should be a log which clearly shows traceability between an individual and their personal seal. Use of personal seals should be dated (by the owner), to be deemed acceptable.

	• 通常不鼓励使用个人印鉴，但如果使用，则印鉴应该受控。应该有登记册清楚表明人员与其个人印鉴之间的可追溯性。使用个人印鉴应该有日期（由所有人签署），这样是可以接受的。

8.7 Making corrections on records 在记录在做更正

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

更正记录应该保持可全面追溯。

Item 项目	How should records be corrected? 记录要如何更正？
1	**Expectation 要求** Cross out what is to be changed with a single line. 将要修改的内容用单线划掉。 Where appropriate, the reason for the correction should be clearly recorded and verified if critical. 适当时，应该清楚记录更正原因，并查证是否关键。 Initial and date the change made. 对所做修改签署首字母和日期。 **Specific elements that should be checked when reviewing records:** **在审核记录时应检查的特定要素** • Check that the original data is readable not obscured (e.g. not obscured by use of liquid paper; overwriting is not permitted). • 检查原始数据应该可读，没有遮挡（例如，不得使用修正液遮盖，不允许覆写） • 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. • 如果对关键数据内容进行了修改，则要查证记录了有效的修改原因，并有修改的支持性证据。 • Check for unexplained symbols or entries in records. • 检查记录中没有解释的符号或内容。
2	**Expectation 要求** Corrections should be made in indelible ink. 应该使用不可擦除的墨水进行更正。 **Specific elements that should be checked when reviewing records:** **在审核记录时应检查的特定要素** • Check that written entries are in ink, which is not erasable, and/or will not smudge or fade (during the retention period). • 检查书写所用墨水是不可擦除的，和/或（在保存期限内）不会弄脏或褪色。 • Check that the records were not filled out using pencil prior to use of pen (overwriting). • 检查记录填写未使用铅笔，然后再用钢笔覆写。

8.8 Verification of records (secondary checks) 记录核查（第二人检查）

Item 项目	When and who should verify the records? 记录由何人在何时进行核查？
1.	**Expectation 要求** Records of critical process steps, e.g. critical steps within batch records, should be: 关键工艺步骤的记录例如批记录内的关键步骤，应该： - reviewed/witnessed by independent and designated personnel at the time of operations occurring; and - 由另一人或指定的人员在操作发生时进行核查/现场验看；且 - reviewed by an approved person within the production department before sending them to the Quality unit ; and - 由生产部内部经过批准的人员进行审核，然后再发给质量部门；且 - reviewed and approved by the Quality Unit (e.g. Authorised Person / Qualified Person) before release or distribution of the batch produced. - 由质量部门（例如受权人/QP）审核批准后放行或销售所生产的批次。 Batch production records of non-critical process steps is generally reviewed by production personnel according to an approved procedure. 非关键工艺步骤的批生产记录一般由生产部人员根据已批准的程序进行审核。 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 reliability of test results in accordance with data-integrity principles. 实验室检测步骤记录亦应在检测完成之后由指定人员进行审核（例如第二个化验员）。审核人员应检查所有书写内容、关键计算，并根据数据完整性原则对检测结果可靠性进行合适的评估。 Additional controls should be considered when critical test interpretations are made by a single individual (e.g. recording of microbial colonies on agar plates). A secondary review may be required in accordance with risk management principles. In some cases this review may need to be performed in real-time. Suitable electronic means of verifying critical data may be an acceptable alternative, e.g. taking photograph images of the data for retention. 如果由单人对关键检测进行解释（例如，记录琼脂碟上的微生物菌落），则应考虑进行额外控制。可能要根据风险管理原则要求第二人审核。有些情况下，可能需要实时执行此类审核。可以接受采用合适的电子手段核查关键数据，例如对数据拍摄照片用于保存。 This verification should be conducted after performing production-related tasks and activities and be signed or initialled and dated by the appropriate persons. 此类核查应该在执行完生产相关任务和活动之后执行，并由合适的人员签字或签首字母并签署日期。 Local SOPs should be in place to describe the process for review of written documents. 应该有本地 SOP 描述书面文件审核的流程。 **Specific elements that should be checked when reviewing records:** **在审核记录时应检查的特定要素** • 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. • 查证生产区域内生产记录处理的流程，确保正确的人员在执行与记录有关的活动时易于获得这些记录。 • Verify that any secondary checks performed during processing were performed by appropriately qualified and independent personnel, e.g. production supervisor or QA. • 查证在生产期间所执行的第二人检查是否是由经过合适确认的独立人员（例如生产主管或 QA）执行的。 • Check that documents were reviewed by production personnel and then quality assurance personnel following completion of operational activities. • 检查文件是否在操作活动完成之后由生产人员审核，然后由质量保证人员审核。
Item 项目	**When and who should verify the records? 由谁何时对记录进行核查？**
1	**Expectation 要求** 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. 检查是否使用最新（批准的）模板，所有空格均正确填写完成，数据与可接受标准进行了严格比较。 Check items 1, 2, 3, and 4 of section 8.6 and Items 1 and 2 of section 8.7 检查节 8.6 的第 1、2、3 和 4 项与节 8.7 的第 1 和 2 项。 **Specific elements that should be checked when reviewing records:** **在审核记录时应检查的特定要素** • Inspectors should review company procedures for the review of manual data to determine the adequacy of processes. • 检查员应该审核公司程序中对手写数据的审核，确定流程是否充分。 • 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. • 是否需要第二人检查，以及第二人检查的程度应该依据质量风险管理原则，依据所生成数据的关键程度。 • Check that the secondary reviews of data include a verification of any calculations used. • 检查第二人数据审核中是否包括有对所用所有计算的核查。 • View original data (where possible) to confirm that the correct data was transcribed for the calculation. • 查看原始数据（如可能），确认转录用于计算的数据是否正确。

8.9 Direct print-outs from electronic systems 电子系统直接打印件

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.

有些非常简单的电子系统如天平、pH 计或简单的处理设备不能存贮数据，只是直接打印出纸质记录。这类设备和记录留下有限的机会通过处理（再处理）、修改电子日期/时间戳影响数据呈现。在此种情况，生成记录和信息的人应在原始记录上签名/日期，确保可追溯性，例如样品 ID、批号等应记录在记录上。这些原始记录应该附入批生产或检测记录。

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

应该考虑确保这些记录持久（参见节 8.6.1）。

8.10 Document retention (Identifying record retention requirements and archiving records)
文件保存（规定记录保存要求和记录归档）

8.10.1 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.

每种类型的记录的保存时长均应（至少）满足 GMP/GDP 要求中所指定的时长。应考虑其它本地或国家法律中指定更长保存期限的要求。

8.10.2 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.

记录应由内部保存，或使用签有质量协议的外部存储服务。在此情况下，数据中心的位置应该有写明。应该有一份风险评估证明存储系统/设施/服务是适用的，且已了解残留风险。

Item 项目	**Where and how should records be archived?** **记录应归档在何处？如何归档？**
1	**Expectation 要求** 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.). 应有系统描述记录归档步骤（档案盒标识、档案盒内记录清单、保存时限、档案放置位置等）。 Instructions regarding the controls for storage, as well as access and recovery of records should be in place. 应有关于记录存贮、获取和检索的控制指导。 Systems should ensure that all GMP/GDP relevant records are stored for periods that meet GMP/GDP requirements[9]. 系统应该确保所有 GMP/GDP 相关记录存贮时间符合 GMP/GDP 要求。 **Specific elements that should be checked when reviewing records:** **在审核记录时应检查的特定要素** • Check that the system implemented for retrieving archived records is effective and traceable. • 检查已归档记录的检索系统是否有效和可追溯 • Check if the records are stored in an orderly manner and are easily identifiable. • 检查记录存贮是否有序，易于识别

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

	• Check that records are in the defined location and appropriately secured. • 检查记录是否放在指定位置，并受到恰当的安全保护 • Check that access to archived documents is restricted to authorised personnel ensuring integrity of the stored records. • 检查是否仅限于经过授权的人员获取已归档文件，确保已存贮记录的完整性 • Check for the presence of records of accessing and returning of records. • 检查是否有记录调阅和归还记录 • The storage methods used should permit efficient retrieval of documents when required. • 所用的存贮方法应该允许在需要时有效检索文件
2	**Expectation 要求** All hardcopy quality records should be archived in: 所有纸质质量记录均应归档于： • secure locations to prevent damage or loss, • 可防止受损或丢失的安全位置； • such a manner that it is easily traceable and retrievable, and • 易于追溯和检索，且 • a manner that ensures that records are durable for their archived life. • 保证记录在其存档周期内的持久性 **Specific elements that should be checked when reviewing records:** **在审核记录时应检查的特定要素** • Check for the outsourced archived operations if there is a quality agreement in place and if the storage location was audited. • 检查外包归档操作，是否签有质量协议，存贮位置是否经过审计 • Ensure there is some assessment of ensuring that documents will still be legible/available for the entire archival period. • 确保进行了评估，保证文件在整个归档期内清晰可及 • In case of printouts which are not permanent (e.g. thermal transfer paper) a verified ('true') copy should be retained. • 不能永久保存的打印件（例如，热敏纸）应保存经过确认的（真实）副本 • Verify whether the storage methods used permit efficient retrieval of documents when required. • 确认所用存贮方法能在需要时快速检索文件
3	**Expectation 要求** All records should be protected from damage or destruction by: 所有记录均应保护免受以下损坏或毁坏： • fire; • 火灾 • liquids (e.g. water, solvents and buffer solution);

- 液体（例如水、溶剂和缓冲液）
- rodents;
- 虫鼠
- humidity etc; and.
- 潮湿等，以及
- unauthorised personnel access, who may attempt to amend, destroy or replace records.
- 无授权人员的进出，有人可能会企图修改、销毁或替换记录

Specific elements that should be checked when reviewing records:

在审核记录时应检查的特定要素

- Check if there are systems in place to protect records (e.g. pest control and sprinklers).
- 检查是否有系统保护记录（例如，虫鼠控制和喷淋装置）
- Note: Sprinkler systems should be implemented according to local safety requirements; however, they should be designed to prevent damage to documents, e.g. documents are protected from water.
- 注：喷淋系统可根据当地安全要求使用，但其设计应该防止对文件的损坏，例如需要防水的文件
- Check for appropriate access controls for records.
- 检查接触记录是否有适当的控制

8.11 Disposal of original records or true copies 原始记录或真实副本的处置

8.11.1 A documented process for the disposal of records should be in place to ensure that the correct original records or true copies 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.)

应制订记录处理文件 流程，以确保在规定的保存期限后处理正确的原始记录或真实副本。系统应确保现行记录未被意外销毁，并且历史记录不会无意中回到现行记录流（例如，历史记录与现行记录混淆/混合）。

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

应有记录/登记本证明根据当地政策对退役记录进行了及时恰当的归档或销毁。

8.11.3 Measures should be in place to reduce the risk of deleting the wrong documents. The access rights allowing disposal of records should be controlled and limited to few persons.

应采取措施降低删除错误文件的风险。处理记录的权限应受控，并仅限于少数人。

9 SPECIFIC DATA INTEGRITY CONSIDERATIONS FOR COMPUTERISED SYSTEMS 计算机化系统的特殊数据完整性考量

9.1 Structure of the Pharmaceutical Quality System and control of computerised systems 药物质量体系的结构和计算机化系统的控制

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[10] and GDP[11] requirements.

有很多种不同的的计算机化系统被公司用来协助进行大量的运营活动。其范围从简单的单机系统到复杂的大型集成系统，其中许多对所生产的产品质量产生影响。每个受监管实体都有责任全面评估和控制所有计算机化系统，并根据 GMP 和 GDP 要求对其进行管理。

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.

组织应充分了解所用计算机化系统的性质和范围，并应进行评估以描述每个系统、其预期用途和功能，以及可能容易受到操纵的任何数据完整性风险或漏洞。应特别强调确定计算机化系统和任何相关数据在产品质量方面的重要性。

9.1.3 All computerised systems with potential for impact on product quality should be effectively managed under a 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.

所有可能影响产品质量的计算机化系统都应在药品质量系统下进行有效管理，该系统旨在确保系统免受意外或故意操纵、修改或任何其他可能影响数据质量的活动的影响和完整性。

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 vendors of systems have an adequate understanding of GMP/GDP and data integrity requirements, and 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.

计算机化系统的设计、评估和选择过程应包括对系统数据管理和完整性方面的适当考虑。受监管的用户应确保系统供应商充分了解 GMP/GDP 和数据完整性要求，并且新系统包括适当的控制以确保有效的数据管理。遗留系统应满足相同的基本要求；然而，要完全合规可能需要使用额外的控制措施，例如支持性管理程序或补充安全硬件/软件。

9.1.5 Regulated users should fully understand the extent and nature of data generated by computerised systems, and a risk based approach should be taken to determining the data risk and criticality of data (including metadata) and the subsequent controls required to manage the data generated. For example:

受监管用户应充分了解计算机化系统生成的数据的范围和性质，并应采取基于风险的方法来确定数据（包括元数据）的数据风险和重要性以及管理生成的数据所需的后续控制。例如：

9.1.5.1 In dealing with raw data, the complete capture and retention of raw data would normally be required in order to reconstruct the manufacturing event or analysis.

在处理原始数据时，通常需要完整捕获并保留原始数据，以还原生产事件或分析。

[10] PIC/S PE 009 Guide to Good Manufacturing Practice for Medicinal Products, specifically Part I chapters 4, Part II chapters 5, & Annex 11 PIC/S PE 009 药品 GMP 指南，尤其是第一部分第 4 章，第二部分第 5 章和附录 11.
[11] PIC/S PE 011 GDP Guide to Good Distribution Practice for Medicinal Products, specifically section 3.5 PIC/S PE 011 药品 GDP 指南，尤其是第 3.5 节。

9.1.5.2 In dealing with metadata, some metadata is critical in reconstruction of events, (e.g. user identification, times, critical process parameters, units of measure), and would be considered as 'relevant metadata' that should be fully captured and managed. However, non-critical meta-data such as system error logs or non-critical system checks may not require full capture and management where justified using risk management.

在处理元数据时，一些元数据对事件的重构至关重要（例如用户身份、时间、关键过程参数、度量单位），将被视为“相关元数据”，应被完全捕获和管理。如采用风险管理进行了论证，则非关键元数据（例如系统错误日志或非关键系统检查）可能不需要完全捕获和管理。

9.1.6 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 are 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.

在确定数据弱点和风险时，强调要在业务流程中考虑计算机化系统的使用环境。例如，使用集成计算机接口的分析方法生成的结果的完整性受样品制备、将样品重量输入系统、使用系统生成数据以及使用该数据处理/记录最终结果的影响。创建和评估数据流向图的可能有助于了解计算机化系统，尤其是接口系统的风险和弱点。

9.1.7 Consideration should be given to the inherent data integrity controls incorporated into the system and/or software, especially those that may be more vulnerable to exploits than more modern systems that have been designed to meet contemporary data management requirements. Examples of systems that may have vulnerabilities include: manual recording systems, older electronic systems with obsolete security measures, non-networked electronic systems and those that require additional network security protection e.g. using firewalls and intrusion detection or prevention systems.

应考虑集成在系统和/或软件中的固有数据完整性控制，尤其是那些可能比为满足当代数据管理要求而设计的现代系统更容易受到攻击的控制。可能存在漏洞的系统例子包括：手动记录系统、安全措施过时的旧电子系统、未联网的电子系统以及需要额外网络安全保护的系统，例如使用防火墙和入侵检测或预防系统。

9.1.8 During inspection of computerised systems, inspectors are recommended to utilise the company's expertise during assessment. Asking and instructing the company's representatives to facilitate access and navigation can aid in the inspection of the system.

在检查计算机化系统时，建议检查员在评估过程中利用公司的专业知识。询问和指导公司代表有利于系统访问，而导航可有助于对系统的检查。

9.1.9 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).

本指南旨在为计算机化系统环境中的数据完整性提供具体考虑。有关计算机化系统优良规范的进一步指导，请参见 PIC/S【受监管的“GxP”环境中的计算机化系统优良规范】(PI 011)。

9.1.10 The principles herein apply equally to circumstances where the provision of computerised systems is outsourced. In these cases, the regulated entity retains the responsibility to ensure that outsourced services are managed and assessed in accordance with GMP/GDP requirements, and that appropriate data

management and integrity controls are understood by both parties and effectively implemented.

此处的原则同样适用于由外包公司提供计算机化系统的情况。 在这些情况下，受监管实体有责任确保根据 GMP/GDP 要求管理和评估外包服务，并确保双方理解并有效实施适当的数据管理和完整性控制。

9.2 Qualification and validation of computerised systems 计算机化系统的确认与验证

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.

计算机化系统的确认和验证应按照相关的 GMP/GDP 指南进行； 下表阐明了对确保计算机化系统的良好数据治理做法的具体要求。

9.2.2 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 of users.

验证本身并不一定能够保证生成的记录得到充分保护，经过验证的系统亦可能存在弱点，能够被意外或恶意修改或丢失数据。因此，验证应辅以适当的管理和物理控制以及用户培训。

9.2 Validation and Maintenance 验证和维护

Item 项目	**System Validation & Maintenance 系统验证&维护**
1	**Expectation 要求** Regulated companies should document and implement appropriate controls to ensure that data management and integrity requirements are considered in the initial stages of system procurement and throughout system and data lifecycle. For regulated users, Functional Specifications (FS) and/or User Requirement Specifications (URS) should adequately address data management and integrity requirements. 受监管公司应该记录和执行适合的控制，确保在系统采购的初期和整个系统与数据生命周期中考虑了数据管理和完整性要求。对于受监管用户，功能标准（FS）和/或用户需求说明（URS）应该充分解决数据管理和完整性要求。 Specific attention should be paid to the purchase of GMP/GDP critical equipment to ensure that systems are appropriately evaluated for data integrity controls prior to purchase. 要特别注意 GMP/GDP 关键设备的采购，确保这些系统在采购之前经过合适的数据完整性控制评估。 Legacy systems (existing 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. 应该对遗留系统（现有在用系统）进行评估，确定现有系统参数设置和功能是否能够根据优良数据管理和完整性规范对数据进行合适的控制。如果这些系统的系统功能或设计不能提供适当水平的控制，则应考虑和实施其它的控制措施。 **Potential risk of not meeting expectations/items to be checked** **潜在不符合要求风险/需检查的项目**

	• 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. • 对 DI 要求考虑不足可能会导致软件系统的采购中未包括满足数据管理和完整性要求所需的基本功能。 • Inspectors should verify that the implementation of new systems followed a process that gave adequate consideration to DI principles. • 检查员应该核查是否在充分考虑 DI 原则之后使用了新的系统。 • Some legacy systems may not include appropriate controls for data management, which may allow the manipulation of data with a low probability of detection. • 一些遗留系统可能对数据管理没有合适的控制措施，这样可能会允许对数据进行篡改，却不易发现。 • 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 and may include: • 应该有对现有系统所做的评估，评估中应有所有弱点的概述，所有为确保数据完整性而实施的其它控制措施的清单。其它控制措施应该经过适当的验证，可包括： • Using operating system functionality (e.g. Windows Active Directory groups) to assign users and their access privileges where system software does not include administrative controls to control user privileges; • 如果系统软件没有管理控制措施控制用户权限，是否使用操作系统功能（例如 WINDOWNS 活动目录组）设置用户及其访问权限 • Configuring operating system file/folder permissions to prevent modification/deletion of files when the modification/deletion of data files cannot be controlled by system software; or • 如果系统软件不能控制数据文件的修改/删除，为操作系统文件/文件夹许可权限进行设置，防止对文件进行修改/删除；或者 • Implementation of hybrid or manual systems to provide control of data generated. • 实施混合或手动系统，为所生成的数据提供控制。
2	**Expectation 要求** Regulated users should have an inventory of all computerised systems in use. The list should include reference to: 受监管用户应该有所有在用计算机化系统的清单。清单应包括以下： - The name, location and primary function of each computerised system; - 每个计算机化系统的名称、位置和基本功能； - Assessments of the function and criticality of the system and associated data; (e.g. direct GMP/GDP impact, indirect impact, none) - 对系统和相关数据的功能和关键程度的评估（例如，直接 GMP/GDP 影响，间接影响，无影响）； - The current validation status of each system and reference to existing validation documents.

- 每个系统的当前验证状态，现有验证文件的索引

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 those systems managing less critical data or processes.

每个系统应有风险评估，要具体评估确保数据完整性所需的控制。应根据系统和工艺及其对产品质量的潜在风险的关键程序确定数据完整性控制的验证水平和程度，例如生成或控制批放行数据的工艺或系统的控制一般要严于管理不怎么关键的数据或流程的系统。

Consideration should also be given to those systems with higher potential for disaster, malfunction or situations in which the system becomes inoperative.

还要考虑发生灾难、故障或系统无法运行情况可能性较大的系统。

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.

评估亦要审核系统在无意或未经授权修改关键参数设置或数据篡改方面的弱点。应记录所有控制措施，并核查其有效性。

Potential risk of not meeting expectations/items to be checked

潜在不符合要求风险/需检查的项目

- 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.
- 所有计算机化系统没有足够可视性的公司可能会忽略系统的关键程度，从而在数据生命周期内产生薄弱点。
- 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.
- 查看是否有一份清楚写明所有系统及其关键程度的清单，是否能确保对这些系统的所有变更或修改均受控
- 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:
- 核查所有关键工艺设备和数据采集系统均有风险评估。缺乏彻底的系统影响性评估可能会导致缺乏适当的验证和系统控制。需审核的关键系统例子包括：
  - systems used to control the purchasing and status of products and materials;
  - 用于控制产品和物料采购和状态的系统；
  - systems for the control and data acquisition for critical manufacturing processes;
  - 关键生产工艺控制和数据采集系统；
  - systems that generate, store or process data that is used to determine batch quality;
  - 生成、存贮或处理用于决定批质量的数据的系统；

	• systems that generate data that is included in the batch processing or packaging records; and • 生成批生产或包装记录中所含数据的系统；以及 • systems used in the decision process for the release of products. • 产品放行决策流程所用系统；
3	**Expectation 要求** For new systems, 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: 新系统均应有每个计算机化系统的验证摘要报告（根据附录 15 要求起草和批准），至少说明（或提供索引）以下项目： - Critical system configuration details and controls for restricting access to configuration and any changes (change management). - 关键系统参数设置详细信息，和限制访问参数设置和所有变更的控制（变更管理）。 - A list of all currently approved normal and administrative users specifying the username and the role of the user. - 一份所有当前已批准的普通和管理用户的清单，写明用户名和用户角色。 - Frequency of review of audit trails and system logs. - 审计追踪和系统日志审核频次。 - Procedures for: - 以下程序： o creating new system user; o 创建新的系统用户； o modifying or changing privileges for an existing user; o 修改或变更现有用户的权限； o defining the combination or format of passwords for each system o 规定每个系统密码组合或格式； o reviewing and deleting users; o 用户审核和删除； o back-up processes and frequency; o 备份流程和频次； o disaster recovery; o 灾难恢复； o data archiving (processes and responsibilities), including procedures for accessing and reading archived data; o 数据归档（流程和职责），包括访问和读取已归档数据的程序； o approving locations for data storage. o 批准数据存贮位置。 - The report should explain how the original data are retained with relevant metadata in a form that permits the reconstruction of the manufacturing

	process or the analytical activity. - 报告应该解释原始数据及其相关元数据如何以一种允许重建生产工艺或分析活动的形式保存 For existing systems, documents specifying the above requirements should be available; however, need not be compiled into the Validation Summary report. These documents should be maintained and updated as necessary by the regulated user. 对于现有系统，应有文件说明上述要求，但不需要编制到验证摘要报告中。必要时，受监管用户应该保存并更新这些文件。 **Potential risk of not meeting expectations/items to be checked** 潜在不符合要求风险/需检查的项目 • Check that validation systems and reports specifically address data integrity requirements following GMP/GDP requirements and considering ALCOA principles. • 检查验证系统和报告，尤其要解决 GMP/GDP 的数据完整性要求，同时考虑 ALCOA 原则。 • 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. • 验证之前应规定系统参数设置和职责分离（例如生成数据的授权应该与核查数据的授权分开），在测试时核查其有效性。 • Check the procedures for system access to ensure modifications or changes to systems are restricted and subject to change control management. • 检查系统访问程序，确保对系统的修改或变更受到限制，并进行变更控制管理。 • Ensure that system administrator access is restricted to authorised persons and is not used for routine operations. • 确保系统管理员访问仅限于经过授权的人员，且不会被用于日常操作。 • 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. • 检查计算机化系统的权限批准、修改和删除程序，确保此类活动受控。检查用户访问日志和权限层次是否最新，系统不应有未经授权的用户，访问账号应该保持更新。 • There should also be restrictions to prevent users from amending audit trail functions and from changing any pre-defined directory paths where data files are to be stored. • 还应该有限制防止用户修改审计追踪功能，防止修改预定的数据文件保存的目录路径。
4	**Expectation 要求** 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. 公司应该有验证主计划，其中应包括具体的计算机化系统政策和验证要求，和此类系统与相关数据的完整性。

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.

应该基于风险确定计算机化系统的验证程度。关于评估计算机化系统验证需求的更多指导参见 PI 011。

Before a system is put into routine use, it should be challenged with defined tests for conformance with the acceptance criteria.

在将系统用于日常操作之前，应采用规定的测试挑战其是否符合可接受标准。

It would be expected that a prospective validation for computerised systems is conducted. Appropriate validation data should be available for systems already in-use.

要求对计算机化系统进行前验证。已在用的系统应有适当的验证数据。

Computerised system validation should be designed according to GMP Annex 15 with URS, DQ, FAT, SAT, IQ, OQ and PQ tests as necessary.

计算机化系统验证应根据 GMP 附录 15 进行设计，必要时应有 URS、DQ、FAT、SAT、IQ、OQ 和 PQ 测试。

The qualification testing approach should be tailored for the specific system under validation, and should be justified by the regulated user. Qualification may include 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.

确认测试方法应该为准备验证的具体系统量身定制，应该由受监管用户进行论证。确认可包括设计确认（DQ）、安装确认（IQ）、运行确认（OQ）和性能确认（PQ）。特别要设计具体的测试挑战数据质量或完整性有风险的领域。

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.

公司应该确保计算机化系统经过确认，满足其既定用途。因此公司不应该仅依赖于供应商的确认包，验证工作应该包括具体的测试，确保在能反映既定的正常使用的运行期间维护数据完整性。

The number of tests should be guided by a risk assessment but the critical 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.

测试数目应该由风险评估指导，但应该至少识别并测试关键功能，例如一些基于基本算法 或逻辑设置的 PLC 和系统，功能性测试就能提供足够的计算机化系统可靠性保证。对于关键的和/或更为复杂的系统，在 IQ、OQ&PQ 阶段需要有详细的核查。

Potential risk of not meeting expectations/items to be checked

潜在不符合要求风险/需检查的项目

- 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.
- 检查验证文件是否包括有数据完整性条款；验证报告应该特别说明数据完整性原则，通过设计和测试证明具备足够的控制。
- Unvalidated systems may present a significant vulnerability regarding data integrity as user access and system configuration may allow data amendment.

	• 未经验证的系统可能在数据完整性方面有重大缺点，因为用户访问和系统参数设置可能允许对数据进行修改。 • 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. • 检查最终用户测试中是否包括有测试脚本，设计用于证明软件不仅满足供应商要求，而且适合其既定用途。
5	**Expectation 要求** Periodic System Evaluation 定期系统评估 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. 计算机化系统应该经过定期评估，确保持续符合数据完整性控制要求。评估应该包括偏差、变更（包括所有变更累积效应）、更新历史、性能和维护，并评估这些变更是否已经对数据管理和完整性控制产生了有害影响。 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. 重新评估的频次应依据风险评估。风险评估取决于计算机化系统的关键程度，同时考虑上次审核以来系统变更的累积效应。应记录所执行的评估。 **Potential risk of not meeting expectations/items to be checked** **潜在不符合要求风险/需检查的项目** • Check that re-validation reviews for computerised systems are outlined within validation schedules. • 检查计算机化系统的再验证审核是否列在验证计划中。 • Verify that systems have been subject to periodic review, particularly with respect to any potential vulnerabilities regarding data integrity. • 核查系统是否进行了定期审核，尤其是在潜在的数据完整性潜在弱点方面。 • 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. • 所有已发现的问题，例如应及时解决当前软件/硬件的局限性，应制订并实施 CAPA 和临时措施管理已发现的风险。
6	**Expectation 要求** Operating systems and network components (including hardware) should be updated in a timely manner according to vendor recommendations and migration of applications from older to newer platforms should be planned and conducted 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. 应该根据供应商的建议及时更新操作系统和网络组件（包括硬件）。应在平台达到不受支持的状态之前就提前规划和执行应用程序从旧平台向新平台的迁移，否则可能会影响系统生成的数据的管理和完整性。

	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. The application of security patches should be performed in accordance with change management principles. 为维护数据安全性，应根据供应商的建议及时以受控方式安装操作系统和网络组件的安全补丁。应用安全补丁应该遵守变更管理原则。 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 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. 如果保留着不受支持的操作系统，也就是说即使在供应商不再支持之后仍使用旧版本，或受支持的版本未打安全补丁，则应尽可能将该系统（服务器）与网络的其余部分隔离。剩余的接口和与其他设备之间的数据传输应仔细设计、配置和验证，以防止不受支持的操作系统造成的漏洞被利用。 Remote access to unsupported systems should be carefully evaluated due to inherent vulnerability risks. 由于固有的漏洞风险，应仔细评估对不受支持的系统的远程访问。 **Potential risk of not meeting expectations/items to be checked** **潜在不符合要求风险/需检查的项目** • 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. • 查证系统更新是否及时受控。 应严格审查旧系统以确定是否集成了适当的数据完整性控制，或者（在无法进行集成控制的情况下）是否已实施适当的管理控制，控制是否有效。

9.3 Data Transfer 数据转移

Item 项目	Data transfer and migration 数据转移和迁移
1	**Expectation 要求** Interfaces should be assessed and addressed during validation to ensure the correct and complete transfer of data. 在验证期间应该对接口进行评估和说明，确保数据转移正确完整。 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: 接口应包括有合适的输入和数据处理正确性和安全性的内置检查，以最大程度降低数据完整性风险。查证方法可包括使用： ○ Secure transfer ○ 安全转移 ○ Encryption

	○ 加密 ○ Checksums ○ 校验 Where applicable, interfaces between systems should be designed and qualified to include an automated transfer of GMP/GDP data. 适用时，系统之间的接口设计和确认应该包括 GMP/GDP 数据的自动转移。 **Potential risk of not meeting expectations/items to be checked** **潜在不符合要求风险/需检查的项目** • Interfaces between computerised systems present a risk whereby data may be inadvertently lost, amended or transcribed incorrectly during the transfer process. • 计算机化系统之间的接口存在风险，数据可能会在传输过程中意外丢失、被修改或错误转录 • 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). • 确保数据直接传输到安全位置/数据库，而不是简单地从本地驱动器复制（在那里可能会被更改）。 • 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. • 在传输到最终存储或数据处理位置之前在本地计算机化系统（例如仪器计算机）上的临时数据存储为数据被删除或操纵创造了机会。 在“单机”（未联网）系统的情况下，这是一个特殊的风险。 确保最初存储数据的环境具有适当的 DI 控制。 • Well designed and qualified automated data transfer is much more reliable than any manual data transfer conducted by humans. • 精心设计且合格的自动数据传输比任何人工进行的数据传输可靠得多。
2	**Expectation 要求** Where system software (including operating system) is installed or updated, the user should ensure that existing and archived data can be read by the new software. Where necessary this may require conversion of existing archived data to the new format. 在安装或更新系统软件（包括操作系统）时，用户应确保新软件可以读取现有和存档数据。 如有必要，可能需要将现有存档数据转换为新格式。 Where conversion to the new data format of the new software is not possible, the old software should be maintained, e.g. installed in one computer or other technical solution, and also available as a backup media in order to have the opportunity to read the archived data in case of an investigation. 如果无法转换为新软件的新数据格式，则应维护旧软件，例如 安装在一台计算机或采用其他技术解决方案，同时作为备份介质，在调查时有机会读取存档数据。 **Potential risk of not meeting expectations/items to be checked** **潜在不符合要求风险/需检查的项目** • It is important that data is readable in its original form throughout the data lifecycle, and therefore users should maintain the readability of data, which may require

	maintaining access to superseded software. • 数据在整个数据生命周期中以其原始形式可读非常重要，因此用户应保持数据的可读性，这可能需要保持对被取代软件的访问。 • The migration of data from one system to another should be performed in a controlled manner, in accordance with documented protocols, and should include appropriate verification of the complete migration of data. • 数据从一个系统到另一个系统的迁移应按照书面方案以受控方式进行，并应包括对数据完整迁移的适当查证。
3	**Expectation 要求** When legacy systems software can no longer be supported, consideration should be given to maintaining the software for data accessibility purposes (for as long possible depending upon the specific retention requirements). This may be achieved by maintaining software in a virtual environment. 当遗留系统软件不再受支持时，应考虑出于数据可访问性目的对软件进行维护（尽可能长，取决于特定的保留要求）。可以在虚拟环境中维护软件。 Migration to an alternative file format that retains as much as possible of the 'true copy' attributes of the data may be necessary with increasing age of the legacy data. 随着旧数据放置时长的增加，可能需要迁移到尽可能多地保留数据“真实副本”属性的替代文件格式。 Where migration with full original data functionality is not technically possible, options should be assessed based on risk and the importance of the data over time. The migration file format should be selected considering the balance of risk between long-term accessibility versus the possibility of reduced dynamic data functionality (e.g. data interrogation, trending, re- processing, etc.) The risk assessment should also review the vulnerability of the system to inadvertent or unauthorised changes to critical configuration settings or manipulation of data. All controls to mitigate risk should be documented and their effectiveness verified. It is recognised that the need to maintain accessibility may require migration to a file format that loses some attributes and/or dynamic data functionality. 如果在技术上无法使用完整的原始数据功能进行迁移，则应根据风险和数据随时间的重要性评估选项。迁移文件格式的选择应考虑长期可访问性与动态数据功能降低的可能性（例如数据查询、趋势分析、再处理等）之间的风险平衡。风险评估还应审查系统无意或未经授权的更改关键配置设置或数据篡改的薄弱点。应记录所有降低风险的控制措施，并验证其有效性。众所周知，为保持可访问性，可能需要转化为一种文件格式而丢失某些属性和/或动态数据功能。 **Potential risk of not meeting expectations/items to be checked** **潜在不符合要求风险/需检查的项目** • When the software is maintained in a virtual environment, check that appropriate measures to control the software (e.g. validation status, access control by authorised persons, etc.) are in place. All controls should be documented and their effectiveness verified. • 如果在虚拟环境下维护软件，则要检查是否有适当的措施对软件进行控制（例如，验证状态、授权人员访问控制等）。所有控制措施均应有文件记录，其有效性均应经过查证。

9.4 System security for computerised systems 计算机化系统的系统安全性

Item: 项目	System security 系统安全性
1.	**Expectation 要求** 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: 应配置和实施用户访问控制，以禁止未经授权访问、更改和删除数据。安全控制的程度取决于计算机化系统的重要性。例如： - 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, should be prohibited. Login parameters should be verified during validation of the electronic system to ensure that login profiles, configuration and password format are clearly defined and function as intended. - 应为所有需要访问和使用特定电子系统的员工设置和分配个人登录 ID 和密码。共享登录凭据无法跟踪执行活动的个人。因此，即使出于节省资金的原因，也应该禁止共享密码。应在电子系统验证期间查证登录参数，以确保明确定义登录配置文件、配置和密码格式并按预期运行。 - Input of data and changes to computerised records should be made only by authorised personnel. Companies should maintain a list of authorised individuals and their access privileges for each electronic system in use. - 数据输入和计算机化记录的更改只能由授权人员进行。公司应为每个使用中的电子系统保留一份授权人员及其访问权限的列表。 - Appropriate controls should be in place regarding the format and use of passwords, to ensure that systems are effectively secured. - 应该对密码的格式和使用进行适当的控制，以确保系统得到有效保护。 - Upon initially having been granted system access, a system should allow the user to create a new password, following the normal password rules. - 在最初被授予系统访问权限后，系统应允许用户按照正常的密码规则创建新密码。 - 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 complex systems will typically requires more levels of users (e.g. a hierarchy) to effectively support access control. - 系统应支持不同的用户访问角色（级别），角色的分配应遵循最低权限规则，即为任何工作职能分配必要的最低访问级别。简单系统至少应该有普通用户和管理员用户，但复杂系统通常需要更多级别的用户（例如层次结构）来有效支持访问控制。 - Granting of administrator access rights to computerised systems and infrastructure used to run GMP/GDP critical applications should be strictly controlled. Administrator access rights should not be given to normal users on the system (i.e. segregation of duties). - 应严格控制授予管理员访问用于运行 GMP/GDP 关键应用程序的计算机化系统

和基础设施的权限。不应将管理员访问权限授予系统上的普通用户（即职责分离）。

- Normal users should not have access to critical aspects of the computerised system, e.g. system clocks, file deletion functions, etc.
- 普通用户不应访问计算机化系统的关键领域，例如系统时钟、文件删除功能等。
- Systems should be able to generate a list of users with actual access to the system, including user identification and roles. User lists should include the names or unique identifiers that permit identification of specific individuals. The list should be used during periodic user reviews.
- 系统应该能够生成对系统具有实际访问权限的用户列表，包括用户 ID 和角色。用户列表应包括允许识别特定个人的姓名或唯一标识符。对用户进行定期审核时应使用该列表。
- Systems should be able to generate a list of successful and unsuccessful login attempts, including:
- 系统应该能够生成成功和失败的登录尝试列表，包括：
    - User identification
    - 用户身份
    - User access role
    - 用户访问角色
    - Date and time of the attempted login, either in local time or traceable to local time
    - 尝试登录的日期和时间，可以是本地时间或可追溯至本地时间
    - Session length, in the case of successful logins
    - 任务长度，如果是成功登录的话
- 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.
- 用户访问控制应确保严格的职责分离（即系统上执行正常工作任务的所有用户应仅具有正常访问权限）。通常，具有较高访问权限的用户（例如管理员）不应在系统上执行正常的工作任务。
- 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 the system administrators and have enhanced permission levels.
- 系统管理员通常应该独立于执行任务的用户，并且不参与或不关心电子系统中生成或可用数据的结果。例如，不应将 QC 主管和经理指定为其实验室电子系统（例如 HPLC、GC、UV-Vis）的系统管理员。通常，应由质量和生产组织之外的个人（例如信息技术管理员）担任系统管理员并具有更高的权限级别。
- 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.

- 对于较小的组织，可能允许质量部门或生产部门的指定人员作为系统管理员持有访问权限；但是，在这些情况下，不应使用管理员访问权限来执行日常操作，并且用户应该持有第二个受限访问权限来执行日常操作。在这些情况下，所有管理人员进行的活动都应在质量体系内进行记录和批准。
- 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.
- 任何对新用户、用户新权限的请求应由相关人员（例如直线经理和系统所有者）授权，并按照标准程序以可追溯的方式转交给系统管理员。
- Computerised systems giving access to GMP/GDP 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.
- 允许访问 GMP/GDP 关键数据或操作的计算机化系统应具有不活动注销功能，无论是在应用程序还是操作系统级别，都会将不活动时间超过预定义时间的用户注销。时间应该更短，而不是更长，并且通常应该设置为防止对系统的未授权访问。激活非活动注销后，系统应要求用户通过正常的身份验证程序再次登录。

Potential risk of not meeting expectations/items to be checked

潜在不符合要求风险/需检查的项目

- 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.
- 检查公司是否采取了所有合理的步骤来确保使用中的计算机化系统是安全的，并且不会受到有意或无意的更改。
- 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.
- 没有物理和管理安全的系统容易受到数据完整性问题的影响。检查员应确认存在管理系统安全的经过验证的程序，确保计算机化系统保持在其经过验证的状态并防止被操纵。
- Check that individual user log-in IDs are in use. Where the system configuration allows the use of individual user log-in IDs, these should be used.
- 检查个人用户登录 ID 是否正在使用中。如果系统配置允许使用个人用户登录 ID，则应使用这些 ID。
- It is acknowledged that some legacy 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. • 众所周知，一些旧的计算机化系统仅支持单个用户登录或有限数量的用户登录。在没有合适的替代计算机化系统可用的情况下，可以通过第三方软件或纸质方法追溯（带版本控制）提供等效控制。应证明并记录替代系统的适用性。混合系统可能需要更多的数据审查。 • 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. • 检查员应验证密码策略是否到位，以确保系统执行良好的密码规则并要求强密码。应考虑对生成或处理关键数据的系统使用更强的密码。 • 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. • 用户无法更改新密码而只能由管理员创建的系统不符合数据完整性要求，因为无法维护密码的机密性。 • 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. • 检查用户访问级别是否得到适当定义、记录和控制。在系统上使用单个用户访问级别并为所有用户分配此角色（根据定义将是管理员角色）是不可接受的。 • Verify that the system uses authority checks to ensure that only authorised individuals can use the system, electronically sign a record, access the operation or computerised system input or output device, alter a record, or perform the operation at hand. • 查证系统是否使用权限检查以确保只有经过授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机化系统输入或输出设备、更改记录或执行手头的操作。

2	**Expectation 要求**
	Computerised systems should 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:
	应保护计算机化系统免受意外更改或故意操纵。公司应评估系统及其设计，以防止未经授权更改可能最终影响数据完整性的已验证设置。应考虑：
	- The physical security of computerised system hardware:
	- 计算机化系统硬件的物理安全：
	  ○ Location of and access to servers;
	  ○ 服务器的位置和访问权限；
	  ○ Restricting access to PLC modules, e.g. by locking access panels.
	  ○ 限制对 PLC 模块的访问，例如通过锁定检修面板。
	  ○ Physical access to computers, servers and media should be restricted to authorised individuals. Users on a system should not normally have access to servers and media.

- 对计算机、服务器和媒体的物理访问应仅限于获得授权的个人。系统上的用户通常不应访问服务器和媒体。

- Vulnerability of networked systems from local and external attack;
- 网络系统受到本地和外部攻击的脆弱性；
- Remote network updates, e.g. automated updating of networked systems by the vendor.
- 远程网络更新，例如供应商自动更新联网系统。
- Security of system settings, configurations and key data. Access to critical data/operating parameters of systems should be appropriately restricted and any changes to settings/configuration controlled through change management processes by authorised personnel.
- 系统设置、配置和关键数据的安全性。应适当限制对系统关键数据/操作参数的访问，并由授权人员通过变更管理流程控制对设置/配置的任何更改。
- The operating system clock should be synchronized with the clock of connected systems and access to all clocks restricted to authorised personnel.
- 操作系统时钟应与连接系统的时钟同步，并且仅限授权人员访问所有时钟。
- Appropriate network security measures should be applied, including intrusion prevention and detection systems.
- 应采用适当的网络安全措施，包括入侵防御和检测系统。
- 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.
- 应设置防火墙以保护关键数据和操作。端口开放（防火墙规则）应基于最低权限策略，使防火墙规则尽可能严密，从而只接受所允许流量。

Regulated users should conduct periodic reviews of the continued appropriateness and effectiveness of network security measures, (e.g. by the use of network vulnerability scans of the IT infrastructure to identify potential security weaknesses) and ensure operating systems are maintained with current security measures.

受监管的用户应定期审查网络安全措施的持续适当性和有效性（例如，通过使用 IT 基础设施的网络漏洞扫描来识别潜在的安全弱点），并确保使用当前的安全措施维护操作系统。

Potential risk of not meeting expectations/items to be checked

潜在不符合要求风险/需检查的项目

- Check that access to hardware and software is appropriately secured, and restricted to authorised personnel.
- 检查对硬件和软件的访问是否得到适当保护，并且仅限于授权人员。
- 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.
- 查证是否实施了合适的身份验证方法。这些方法应包括用户 ID 和密码，但其他方法也是可能的，并且可能是必需的。 但是，用户的可识别性至关重要。
- For remote authentication to systems containing critical data available via the internet; verify that additional authentication techniques are employed such as

	the use of pass code tokens or biometrics. • 用于对包含可通过互联网获得的关键数据的系统进行远程身份验证； 查证是否采用了其他身份验证技术，例如使用密码令牌或生物识别技术。 • 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 GMP/GDP steps. • 查证对系统关键操作参数的访问是否得到适当控制，并且在适当的情况下，系统在 GMP/GDP 步骤的关键序列中强制执行正确的事件和参数顺序。
3	**Expectation 要求** Network protection 网络保护 Network system security should include appropriate methods to detect and prevent potential threats to data. 网络系统安全应该包括适当的方法用于检测和防止对数据的潜在威胁。 The level of network protection implemented should be based on an assessment of data risk. 所实施的网络保护级别应基于对数据风险的评估。 Firewalls should be used to prevent unauthorised access, and their 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. 应使用防火墙防止未经授权的访问，应根据规范定期审查其规则，以确保将其设置为必要的限制，只接受允许的流量。 审查应记录在案。 Firewalls should be supplemented with appropriate virus-protection or intrusion prevention/detection systems to protect data and computerised systems from attempted attacks and malware. 防火墙应辅以适当的病毒保护或入侵防御/检测系统，以保护数据和计算机化系统免受企图攻击和恶意软件的侵害。 **Potential risk of not meeting expectations/items to be checked** **潜在不符合要求风险/需检查的项目** • Inadequate network security presents risks associated with vulnerability of systems from unauthorised access, misuse or modification. • 网络安全不足会带来与系统因无授权访问、误用或修改而易受攻击相关的风险。 • Check that appropriate measures to control network access are in place. Processes should be in place for the authorisation, monitoring and removal of access. • 检查控制网络访问的适当措施是否到位。 应该有适当的授权、监控和取消访问流程。 • Systems should be designed to prevent threats and detect attempted intrusions to the network and these measures should be installed, monitored and maintained. • 系统的设计应该能够防止威胁并检测对网络的入侵企图，并且应该安装、监控和维护这些措施。 • 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.

	• 防火墙规则通常会随时间发生变化，例如 由于服务器维护等原因暂时开放端口。如果从未审查，防火墙规则可能会过时，允许不需要的流量或入侵。
4	Electronic signatures used in the place of handwritten signatures should have appropriate controls to ensure their authenticity and traceability to the specific person who electronically signed the record(s). 代替手写签名使用的电子签名应有适当的控制，以确保其真实性和可追溯至电子签名记录的具体个人。 Electronic signatures should be permanently linked to their respective record, i.e. if a later change is made to a signed record; the record should indicate the amendment and appear as unsigned. 电子签名应与其各自的记录永久链接，即如果以后对签名记录进行了更改， 记录应指明修订并显示为未签名。 Where used, electronic signature functionality should automatically log the date and time when a signature was applied. 在使用时，电子签名功能应自动记录应用签名的日期和时间。 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. 使用高级形式的电子签名正变得越来越普遍（例如，公司越来越普遍地使用生物识别技术）。 应鼓励使用高级形式的电子签名。 **Potential risk of not meeting expectations/items to be checked** **潜在不符合要求风险/需检查的项目** • 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. • 检查电子签名是否经过适当验证，发放给员工时是否受控，所有时间、电子签名是否易于追溯至具体个人。 • 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. • 在电子签名完成之后对数据所做的任何变更均应让签名无效，除非该数据被重新审核和重新签名。
5	Restrictions on use of USB devices USB 设备的限制 For reasons of system security, computerised systems should be configured to prevent vulnerabilities from the use of USB memory sticks and storage devices on computer clients and servers hosting GMP/GDP critical data. If necessary, ports should only be opened for approved purposes and all USB devices should be properly scanned before use. 为系统安全起见，应对计算机化系统进行配置，以防止在托管 GMP/GDP 关键数据的计算机客户端和服务器上使用 U 盘和存储设备造成漏洞。如有必要，应仅出于已批准的目的打开端口，并且在使用前应正确扫描所有 USB 设备。 The use of private USB devices (flash drives, cameras, smartphones, keyboards, etc.) on company computer clients and servers hosting GMP/GDP data, or the use of company USB devices on private computers, should be controlled in order to prevent security breaches. 应控制在托管 GMP/GDP 数据的公司计算机客户端和服务器上使用私人 USB 设备（闪存驱动器、相机、智能手机、键盘等），或在私人计算机上使用公司 USB 设备，以防

	止安全 违反。 **Potential risk of not meeting expectations/items to be checked** **潜在不符合要求风险/需检查的项目** • This is especially important where operating system vulnerabilities are known that allow USB devices to trick the computer, by pretending to be another external device, e.g. keyboard, and can contain and start executable code. • 如果已知操作系统有弱点可让 USP 设备假装是另一个外部设备，如键盘，并可能含有可执行代码且开始运行，从而操纵计算机，则此点尤为重要。 • Controls should be in place to restrict the use of such devices to authorised users and measures to screen USB devices before use should be in place. • 应有控制措施限制仅允许授权人员使用此类设备，在使用前有措施筛选 USP 设备。

9.5 Audit trails for computerised systems 计算机化系统的审计追踪

Item: **项目**	**Audit Trails 审计追踪**
1.	**Expectation 要求** 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. 在采购和使用计算机化系统时，应考虑数据管理和完整性要求。公司应该选择具备合适的电子审计追踪功能的软件。 Companies should endeavour to purchase and upgrade older systems to implement software that includes electronic audit trail functionality. 公司应该尽量购买，并将旧的系统升级，从而使用含有电子审计追踪功能的软件。 It is acknowledged that some very simple systems lack appropriate audit trails; however, alternative arrangements to verify the veracity of data should be implemented, e.g. administrative procedures, secondary checks and controls. Additional guidance may be found under section 9.10 regarding hybrid systems. 已知有些非常简单的系统缺少合适的审计追踪，但应该采用替代手段核查数据的真实性，例如管理程序、第二人检查和控制。更多关于混合系统的指南可在节 9.10 中找到。 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. 系统验证期间应核查审计追踪功能，确保每个人工活动有关的关键数据的修改和删除均被记录，并符合 ALCOA+原则。 Regulated users should understand the nature and function of audit trails within systems, and should perform an assessment of the different audit trails during qualification to determine the GMP/GDP relevance of each audit trail, and to ensure the correct management and configuration of audit trails for critical and GMP/GDP relevant data. This exercise is important in determining which specific trails and which entries within trails are of significance for review with a defined frequency established. For example, following such an assessment audit trail reviews may focus on: 受监管的用户应该了解系统内审计追踪的属性和功能，并在确认期间对不同审计追踪

进行评估，确定每个审计追踪的 GMP/GDP 相关性，确保对关键的 GMP/GDP 相关数据的审计追踪进行正确管理和参数设置。这种做法在确定哪种特定的追踪和审计追踪内哪条信息对于规定审核频次有重大影响时很重要。例如，遵守此类评估，审计追踪审核可能会关注：

- Identifying and reviewing entries/data that relate to changes or modification of data.
- 识别并审核与数据变更或修改有关的信息/数据。
- Review by exception – focusing on anomalous or unauthoried activities.
- 异常审核—关注异常或未经授权的活动。
- Systems with limitations that allow change of parameters/data or where activities are left open to modification
- 有局限性的系统允许修改参数/数据，或允许修改活动
- Note: Well-designed systems with permission settings that prevent change of parameters/data or have access restrictions that prevent changes to configuration settings may negate the need to examine related audit trails in detail
- 注：经过良好设计具备许可设置的系统可防止参数/数据变更，或有访问限制可防止对参数设置的修改，这样就不需要详细检查相关审计追踪

Audit trail functionalities should be enabled and locked at all times and it should not be possible to deactivate, delete or modify the functionality. If it is possible for administrative users to deactivate, delete or modify the audit trail functionality, an automatic entry should be made in the audit trail indicating that this has occurred.

所有时间均应激活并锁定审计追踪功能，该功能应不可关闭、删除或修改。如果管理员用户可关闭、删除或修改审计追踪功能，则审计追踪中应该自动生成信息显示发生过此类事件。

Companies should implement procedures that outline their policy and processes to determine the data that is required in audit trails, and 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 performed by the originating department, and where necessary verified by the quality unit, e.g. during self-inspection or investigative activities.

公司应该执行程序列出其政策和流程，确定审计里所需的数据，并根据风险管理原则对审订追踪进行审核。与每项操作有关的关键审计追踪应在操作完成审核之前（例如在批放行之前）与其它相关记录一起审核，从而确保关键数据及其修改是可接受的。此类审核应该由发起部门执行，必要时由质量部门核查，例如在自检期间或调查性活动期间。

Non-critical audit trails reviews can be conducted during system reviews at a pre-defined frequency. This review should be performed by the originating department, and where necessary verified by the quality unit (e.g. during batch release, self-inspection or investigative activities).

非关键审计追踪的审核可按预定的频次在系统审核期间执行。此类审核应该由发起部门执行，必要时由质量部门进行核查 （例如，在批放行、自检或调查性活动期间）。

Potential risk of not meeting expectations/items to be checked

潜在不符合要求风险/需检查的项目

	• 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 relevant metadata. • 验证文件应该证明审计追踪功能正常，系统内部的所有活动、修改和其它转录均和所有相关元数据一起被记录。 • Verify that audit trails are regularly reviewed (in accordance with quality risk management principles) and that discrepancies are investigated. • 查证审计追踪是否经过定期审核（根据质量风险管理原则），偏差是否经过调查。 • 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. • 如果没有电子审计追踪系统，在使用全面审计追踪的系统（集成系统，或使用经过验证的接口的独立审计软件）之前是否有纸质记录证明数据修改是可接受的。此类混合系统是允许使用的，前提是其可达到集成审计追踪的等同功能，例如 PIC/S GMP 指南附录 11 中所述的要求。 • Failure to adequately review audit trails may allow manipulated or erroneous data to be inadvertently accepted by the Quality Unit and/or Authorised Person. • 未能充分审核审计追踪可能会允许篡改数据或产生错误数据，而质量部门和/或授权人无意中接受了此类数据 • Clear details of which data are critical, and which changes and deletions should be recorded (audit trail) should be documented. • 应详细清楚地记录哪些数据是关键的，哪些修改和删除应该有记录（审计追踪）
2	**Expectation 要求** 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. 如果电子系统有审计追踪功能，应该对其进行评估，其参数设置应适合捕获与数据获取、删除、改写和变更有关的所有关键活动，用于审计。 Audit trails should be configured to record all manually initiated processes related to critical data. 审计追踪应设置为记录与关键数据有关的所有手动启动的流程。 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. 系统提供由计算机生成的有时间戳的安全审计追踪，独立记录录入数据的和电子记录创建、修改或删除动作的时间和日期。 The audit trail should include the following parameters: 审计追踪应该包括以下参数： - details of the user that undertook the action;

- 执行动作的用户详细信息；
- what action occurred, was changed, incl. old and new values;
- 发生了什么动作，修改了什么，包括修改前后 的值；
- when the action was taken, incl. date and time ;
- 何时执行的动作，包括时间和日期；
- why the action was taken (reason); and
- 为何执行该动作（原因），以及
- in the case of changes or modifications to data, the name of any person authorising the change.
- 如果数据有变化或修改，被授权进行修改的人的姓名。

The audit trail should allow for reconstruction of the course of events relating to the creation, modification, or deletion of an electronic record.

审计追踪应该允许重建与电子记录创建、修改或删除有关的事件的过程。

The system should be able to print and provide an electronic copy of the audit trail, and whether viewing in the system online or in a hardcopy, the audit trail should be available in a meaningful format.

系统应该能够打印和提供审计追踪的电子副本，可从系统在线查看或以纸质方式查看，审计追踪应该可以有含义的格式提供。

If possible, the audit trail should retain the dynamic functionalities found in the computerised system, (e.g. search functionality and ability to export data such as to a spreadsheet).

审计追踪应尽可能保留其在计算机化系统中发现的动态功能（例如，搜索功能，输出数据到例如数据表的功能）。

Note: An audit trail should not be confused with a change control system where changes may needed to appropriately controlled and approved under a PQS.

注：审计追踪不应该与变更控制系统混淆，变更控制系统中要对变更进行合适的控制，在 PQS 下进行批准。

Potential risk of not meeting expectations/items to be checked

潜在不符合要求风险/需检查的项目

- Verify the format of audit trails to ensure that all critical and relevant information is captured.
- 查验审计追踪的格式，是否确保采集到所有相关的关键信息。
- The audit trail should include all previous values and record changes should not overwrite or obscure previously recorded information.
- 审计追踪应该包括之前所有的值，记录变更应该不会覆盖或遮盖之前已记录的信息。
- 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 be 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 critical process parameter (CPP), then each addition should be recorded individually, with time stamps. If the order of addition is not a CPP then the addition of all 4

	materials could be recorded as a single timestamped activity. • 审计追踪输入信息应该实时记录，并反映活动的实际时间。系统在记录一系列顺序操作时，在所有动作完成时将其记录为同一时间，或者仅生成一条审计追踪，可能并不符合数据完整性要求，尤其是当每个具体的动作或序列比较关键的时候。例如，将 4 种原料加入混合罐中的电子记录中，如果加料顺序是关键工艺参数（CPP），则加料操作要分别记录，并含有时间戳；如果加料顺序不是 CPP，则 4 种物料的投料可以记录为同一时间戳下的活动。

9.6 Data capture/entry for computerised systems 计算机化系统的数据采集/输入

Item: 项目	**Data capture/entry 数据采集/输入**
1.	**Expectation 要求** Systems should be designed for the correct capture of data whether acquired through manual or automated means. 系统设计应该保证正确采集数据（无论是人工还是自动方式采集）。 For manual entry: 人工录入： - 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. - 关键数据应该仅由经过授权的人员录入，系统应该记录录入的详细信息、录入人身份和录入时间。 - 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. - 数据应该以由软件控制的指定格式录入，验证中应证明系统不会接受无效数据格式。 - All manual data entries of critical data should be verified, either by a second operator, or by a validated computerised means. - 所有人工录入的关键数据均应经过核查，可以是第二人，亦可以是经过验证的计算机化方式。 - Changes to entries should be captured in the audit trail and reviewed by an appropriately authorised and independent person. - 对录入数据的修改应该产生审计追踪，并由经过适当授权的独立人员进行审核。 For automated data capture: (refer also to table 9.3) 自动数据采集（参见表 9.3） - The interface between the originating system, data acquisition and recording systems should be validated to ensure the accuracy of data. - 原始系统、数据采集和记录系统之间的接口应该经过验证，确保数据的准确性。 - Data captured by the system should be saved into memory in a format that is not vulnerable to manipulation, loss or change. - 系统采集的数据应该以不易被篡改、丢失或修改的格式保存至存储器中。

	- The system software should incorporate validated checks to ensure the completeness of data acquired, as well as any relevant metadata associated with the data. - 系统软件应该集成有经过验证的校验，确保所需数据的完整性，以及数据伴随的相关元数据的完整性。 **Potential risk of not meeting expectations/items to be checked** **潜在不符合要求风险/需检查的项目** • Ensure that manual entries of critical data made into computerised systems are subject to an appropriate secondary check. • 确保人工输入关键数据至计算机化系统经过恰当的第二人检查。 • Validation records should be reviewed for systems using automated data capture to ensure that data verification and integrity measures are implemented and effective, e.g. verify whether an auto save function was validated and, therefore, users have no ability to disable it and potentially generate unreported data. • 应审核自动采集数据的系统的验证记录，确保实施了数据核查和完整性措施且有效，例如查验自动保存功能是否经过验证，用户就无法关闭从而产生未报告的数据。
2	**Expectation 要求** Any necessary changes to data should be authorised and controlled in accordance with approved procedures. 对数据的任何必须修改均应根据已批准的程序进行授权和控制。 For example, manual integrations and reprocessing of laboratory results should be performed in an approved and controlled manner. The firm's quality unit should 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 context. 例如，手动积分和实验室结果的重新处理应该经过批准后以受控方式执行。公司的质量部门应该建立措施确保数据修改仅在必要时由指定的人员执行。原始（未经修改的）数据应该保存在其原始环境中。 Any and all changes and modifications to raw data should be fully documented and should be reviewed and approved by at least one appropriately trained and qualified individual. 对原始数据所做的任何和所有变更和修改均应有完整记录，并应由至少一位经过合适培训和确认的人员审核和批准， **Potential risk of not meeting expectations/items to be checked** **潜在不符合要求风险/需检查的项目** • 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. • 查证是否存在合适的程序，对数据的所有修改或重新处理进行控制。应有证据证明所拟修改有正式恰当的批准流程，所做变更受控/受限/有规定并有正式审核。

9.7 Review of data within computerised systems 计算机化系统内数据的审核

Item: 项目	Review of electronic data 电子数据的审核
1	**Expectation 要求** 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, or whether any relevant unreported data was generated. All changes should be duly authorised. 受监管的用户应该执行风险评估，识别出计算机化系统生成的所有 GMP/GDP 相关的电子数据，以及这些数据的关键程度。识别后，受监管用户应该对关键数据进行审计，并核查确认操作均正确执行，查看电子记录中的原始信息是否有变化（修改、删除或重新写入），或者是否生成了未报告的相关数据。所有修改均应经过正式批准。 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. SOP 应描述由第二个操作员审核数据的过程。这些 SOP 应概述审核的关键原始数据、数据摘要审查、任何相关日志和纸质记录的审核，并解释该审核是如何执行、记录和授权的。 The review of audit trails should be part of the routine data review within the approval process. 审计追踪审核应是批准过程中常规数据审核的一部分。 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 prior to the point that the data is relied upon to make a critical decision, e.g. batch release. 应根据计算机化系统中记录的数据的 GMP/GDP 相关值进行的风险评估，据此风险评估确定审计追踪审核的频率、作用和职责。例如，对于可能对药品质量产生直接影响的电子数据更改，要求在依赖数据做出关键决策（例如批放行）之前对审计追踪进行审核。 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 review activity should be documented and recorded. 受监管用户应制定 SOP，详细描述如何审核审计追踪、查找什么以及如何执行搜索等。该程序应详细确定负责审计追踪审核的人员应遵循的流程。应记录和记录审计追踪审核活动。 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. 应全面调查和记录审计追踪审核期间发现的与预期结果的任何显着差异。如果审计追踪审核发现可能影响药品质量或数据完整性的严重问题，程序应描述要采取的措施。

	Potential risk of not meeting expectations/items to be checked **潜在不符合要求风险/需检查的项目** • Check local procedures to ensure that electronic 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. • 检查本地程序，确保根据电子数据的关键程度（对产品质量和/或决策的影响）对其进行了审核。每次审核的证据应记录，并可向检查员提供。 • 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. • 如果有数据摘要用于内部或外部报告，应有证据证明此类摘要已根据原始数据进行过核查。 • Check that the 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. • 检查受监管方是否有详细的 SOP，列出如何执行第二人审核和审计追踪审核的步骤，如果在审核过程中发现问题要采取的步骤。 • 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. • 如果使用的是全球系统，日期和时间记录可能有必要包括时区记录，证明记录的同步性。 • Check that known changes, modifications or deletions of data are actually recorded by the audit trail functionality. • 检查审计追踪功能是否实际记录了已知的数据变更、修改或删除。
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 in order to verify the effective implementation of current controls and to detect potential non-compliance issues. These reviews should be incorporated into the company's self-inspection programme. 公司的质量部门应该建立一个程序和计划，对审计追踪依据其关键程度和系统复杂程度执行持续审核，以查证最新控制措施的有效实施，发现潜在不符合问题。此类审核应该包括在公司的自检程序中。 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. **Potential risk of not meeting expectations/items to be checked** **潜在不符合要求风险/需检查的项目** • 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. • 查验自检程序是否包括有对审计追踪的检查，其目的是核查现有控制措施的有效性，以及是否符合内部的数据审核程序。 • Audit trail reviews should be both random (selected based on chance) and targeted (selected based on criticality or risk). • 审计追踪审核应该随机（随机选择），有目标性（根据关键程度或风险选择）。

9.8 Storage, archival and disposal of electronic data 电子数据的存贮、归档和处置

Item: 项目	**Storage, archival and disposal of electronica data** **电子数据的存贮、归档和处置**
1.	**Expectation 要求** Storage of data should include the entire original data and all relevant metadata, including audit trails, using a secure and validated process. 数据存贮应该包括整个原始数据和所有相关元数据，包括审核追溯，并使用经过验证的安全流程。 If the data is backed up, or copies of it are made, then the backup and copies should also have the same appropriate levels of controls so as to prohibit unauthorised access to, changes to and deletion of data or their alteration. For example, a firm that backs up data onto portable hard drives should prohibit the ability to delete data from the hard drive. Some additional considerations for the storage and backup of data include: 如果数据进行了备份，或者制作了副本，则备份和副本也应该有相同水平的控制，从而禁止未经授权的数据访问、修改和删除。例如，一个公司将数据备份至移动硬盘上可禁止从硬盘上删除数据。更多的数据存贮和备份考量包括： - True copies of dynamic electronic records can be made, with the expectation that the entire content (i.e. all data and all relevant metadata is included) and meaning of the original records are preserved. - 动态电子记录的真实备份，预期可保存完整内容（即包括所有数据和所有相关元数据）和原始记录的含义 - 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 - 所存贮的数据应能够以全面可读格式进行访问。公司可能需要维持合适的软件和硬件用于在保存期内访问以电子形式存贮的数据备份或副本。 - Routine backup copies should be stored in a remote location (physically separated) in the event of disasters. - 日常备份副本应该存贮在一个较远的地方（物理分离），以防灾难发生。 - 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. - 备份数据应该在指定的法规保存期限内可读，即使已更新或替换至具有更优性能的新版本软件更新。 - Systems should allow backup and restoration of all data, including meta-data and audit trails. - 系统应该允许对所有数据进行备份和恢复，包括元数据和审计追踪。 **Potential risk of not meeting expectations/items to be checked** **潜在不符合要求风险/需检查的项目** • Check that data storage, back-up and archival systems are designed to capture all data and relevant metadata. There should be documented evidence that these systems have been validated and verified. • 检查数据存贮、备份和归档系统的设计是否能够捕获所有数据和相关元数据。应该有书面证据证明此类系统已经过验证和核查。 • The extent of metadata captured should be based on risk management

	principles, and users should ensure that all metadata critical in the reconstruction of activities or processes are captured. • 元数据采集的程度应该基于风险管理原则，用户应确保采集到所有对活动或工艺重建至关重要的元数据。 • Check that data associated with superseded or upgraded systems is managed appropriately and is accessible. • 检查与被取代或被升级系统有关的数据是否进行了恰当的管理，并可以访问。
2.	**Expectation 要求** The record retention procedures should include provisions for retaining the metadata. This allows for future queries or investigations to reconstruct the activities that occurred related to a batch. 记录保存程序应该包括有保存元数据的条款。这样将来查询 或调查时可以重建与某批次有关的已发生的活动。
3.	**Expectation 要求** Data should be backed-up periodically and archived in accordance with written procedures. Archive copies should be physically (or virtually, where relevant) secured in a separate and remote location from where back up and original data are stored. 数据应定期备份并按照书面程序存档。归档副本应该物理地（或虚拟地，如果相关）保护在一个单独的远程位置，与备份和原始数据的存储位置不同。 The data should be accessible and readable and its integrity maintained for all the period of archiving. 数据应该是可访问和可读的，并且在整个归档期间保持其完整性。 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. 应该有一个程序来恢复存档数据，以防需要调查。应定期测试用于恢复存档数据的程序。 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. 如果存档过程需要设施，则应实施特定的环境控制和仅授权人员访问，以确保保护记录免受故意或无意的更改或丢失。当设施中的系统因预期长期访问数据的问题而不得不退役时，程序应确保存档数据的持续可读性。例如，可以将数据传输到另一个系统。 **Potential risk of not meeting expectations/items to be checked** **潜在不符合要求风险/需检查的项目** • 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. • 存档数据存在风险，数据的访问和可读性可能会因软件应用程序更新或被取代的设备而丢失。 查证公司是否有权访问存档数据，并且保持对必要软件的访问权限，以便能够查看存档数据。

	• Where external or third party facilities are utilised for the archiving of data, these service providers should be subject to 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. • 如果使用外部或第三方设施归档数据，这些服务提供商应接受评估，所有责任均应记录在质量技术协议中。 检查协议和评估记录，以确认已适当考虑确保存档记录的完整性。
4.	**Expectation 要求** It should be possible to print out a legible and meaningful record of all the data generated by a computerised system (including metadata). 计算机化系统生成的所有数据（包括元数据）均应可以打印出清晰有含义的记录。 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. 如果允许对记录进行修改，应该可将记录修改打印出来，显示原始数据是何时以及如何被修改的。 **Potential risk of not meeting expectations/items to be checked** **潜在不符合要求风险/需检查的项目** • Check validation documentation for systems to ensure that systems have been validated for the generation of legible and complete records. • 检查系统的验证文件，确保系统经过验证，可以生成清晰完整的记录 • Samples of print-outs may be verified. • 查证打印件样本
5.	**Expectation 要求** 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 disposal of data that is no longer required. 应有程序描述电子形式存贮的数据的处置流程。这些程序应该能够指导对数据进行评估，设置保存期限，描述不再需要的数据的处置要求。 **Potential risk of not meeting expectations/items to be checked** **潜在不符合要求风险/需检查的项目** • 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. • 检查程序是否清楚规定了数据处置的条件，是否注意避免无意中处理了未达保存期限的所需数据。

9.9 Management of Hybrid Systems 混合系统的管理

Item: **项目**	**Management of Hybrid Systems 混合系统的管理**
1.	Hybrid systems require specific and additional controls in reflection of their complexity and potential increased vulnerability to manipulation of data. For this reason, the use of hybrid systems is discouraged and such systems should be replaced whenever possible.

混合系统需要特定和额外的控制，以反映其复杂性和潜在增加的数据操纵脆弱性。因此，不鼓励使用混合系统，并且应尽可能更换此类系统。

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.

混合系统的每个要素都应根据与上述手动和计算机化系统相关的指南进行识别和控制。

Appropriate quality risk management principles should be followed when assessing, defining, and demonstrating the effectiveness of control measures applied to the system.

在评估、定义和证明应用于系统的控制措施的有效性时，应遵循适当的质量风险管理原则。

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.

应具备对整个系统的详细系统描述，其中应列出系统的所有主要组件、每个组件的功能、数据管理和完整性的控制以及系统组件交互的方式。

Procedures and records should be available to manage and appropriately control the interface between manual and automated systems, particularly steps associated with:

应该有程序和记录来管理和适当控制手动和自动系统之间的接口，特别是与以下相关的步骤：

- manual input of manually generated data into computerised systems;
- 将人工生成的数据手动输入计算机化系统；
- transcription (including manual) of data generated by automated systems onto paper records; and
- 将自动化系统生成的数据转录（包括手动）到纸质记录上；和
- automated detection and transcription of printed data into computerised systems.
- 自动检测打印数据并将其转录到计算机化系统中。

Potential risk of not meeting expectations/items to be checked
潜在不符合要求风险/需检查的项目

- Check that hybrid systems are clearly defined and identified, and that each contributing element of the system is validated.
- 检查混合系统是否被明确定义和识别，并且系统的每个贡献元素都经过验证。
- Attention should be paid to the interface between the manual and computerised system. Inspectors should verify that adequate controls and secondary checks are in place where manual transcription between systems takes place.
- 应注意手动和计算机化系统之间的接口。 检查员应查证在系统之间进行手动转录的地方是否有足够的控制和二次检查。
- Original data should be retained following transcription and processing.
- 在转录和处理后应保留原始数据。
- Hybrid systems commonly consist of a combination of computerised and manual systems. Particular attention should be paid to verifying:

	• 混合系统通常由计算机和手动系统的组合组成。应特别注意验证： ○ The extent of qualification and/or validation of the computerised system; and, ○ 计算机系统的确认和/或验证范围； 和， ○ 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. ○ 混合系统中的手动元素管理所用控制措施的稳健性，因为手动流程的应用难以保持一致性
2	Procedures should be in place to manage the review of data generated by hybrid systems which clearly outline the process for the evaluation and approval of electronic and paper-based data. Procedures should outline: 应该制定程序来管理混合系统生成的数据的审查，这些程序清楚地概述了电子和纸质数据的评估和批准过程。 程序应列出： - Instructions for how electronic data and paper-based data is correlated to form a complete record. - 电子数据和纸质数据如何关联以形成完整记录的说明。 - Expectations for approval of data outputs for each system. - 要求每个系统的数据输出需要批准。 - Risks identified with hybrid systems, with a focus on verification of the effective application of controls - 混合系统识别的风险，重点是查证控制的有效应用 **Potential risk of not meeting expectations/items to be checked** **潜在不符合要求风险/需检查的项目** • Verify that instructions for the review of hybrid system data is in place. • 查证是否制订了对混合系统数据进行审核的指导

10 DATA INTEGRITY CONSIDERATIONS FOR OUTSOURCED ACTIVITIES 外包活动的数据完整性考量

10.1 General supply chain considerations 一般供应链考量

10.1.1 Modern supply chains often consist of multiple partner companies working together to ensure safe and continued supply of medicinal products. Typical supply chains require the involvement of API producers, dosage form manufacturers, analytical laboratories, wholesale and distribution organisations, often from differing organisations and locations. These supply chains are often supported by additional organisations, providing outsourced services, IT services and infrastructure, expertise or consulting services.

10.1.2 数据完整性在保证供应链的安全和完整性中扮演着重要的角色。合同发包方的数据管理措施可能会被供应链伙伴所提供的不可靠或伪造数据或材料大大削弱。此原则适用于所有外包活动，包括原料供应商，合同生产商/分析服务提供商。

10.1.3 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, contracted service providers and

consultants.

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

对供应链伙伴和外包活动的初始和定期再确认应包括对数据完整性风险和适当的控制措施的考虑。

10.1.5 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.

很重要的一点是公司应了解从供应链所获得的数据（例如，摘要记录和副本/打印件）完整性局限性，以及远程监督的挑战。这些局限性与本指南第 8.11 中所讨论的内容相类似。这会有助于采用质量风险管理方法，集中资源用于数据完整性核查和监管。

10.2 Routine document verification 日常文件核查

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 a robust qualification process for outsourced supplier and contractor, using quality risk management principles.

供应链依赖于从一个公司传送到另一个公司的文件记录和数据的使用。通常合同发包方去审核所有与报告结果相关的原始数据并不现实。应使用质量风险管理原则，重点关注供应商的稳健程度和合同方确认。

10.3 Strategies for assessing data integrity in the supply chain 供应链中数据完整性评估策略

10.3.1 Companies should conduct regular risk reviews of supply chains and outsourced activity that evaluate the extent of data integrity controls required. The frequency of such reviews should be based on the criticality of the services provided by the contract acceptor, using risk management principles, Information considered during risk reviews may include:

公司应对供应链和外包活动实施定期风险评审，评估所需数据完整性控制的程度。此类审核的频次应该基于合同受托方所提供服务的关键程度，并使用风险管理原则。在风险审核过程中考虑的信息可包括：

- The outcome of site audits, with focus on data governance measures
- 对审核的结果，关注数据管理措施
- Demonstrated compliance with international standards or guidelines related to data integrity and security
- 已证明符合国际标准或与数据完整性和安全性有关的指南
- Review of data submitted in routine reports, for example:
- 审核日常报告中所提交的数据，例如：

Area for review 审核领域	**Rationale 理由**
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
将合同方或供应商所报告的分析数据与公司内对相同物料的分析数据进行比较	寻找有差异的数据，这可能是做假的征兆

10.3.2 Quality agreements (or equivalent) should be in place between manufacturers and suppliers of materials, service providers, contract manufacturing organisations (CMOs) and (in the case of distribution) suppliers of medicinal products, 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.

生产商和供应商/合同生产组织（CMO）之间应签署质量协议，协议应有特定条款确保供应链中的数据完整性。这可以通过设定数据管理要求，要求合同接受方向合同发包方提交透明的错误/偏差报告来实现。还应该要求合同接受方通知合同发包方在其场所内识别出的所有数据完整性失败情况。

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. Contract acceptors are expected to provide reasonable access to data generated on behalf of the contract giver during audits, so that compliance with data integrity and management principles can be assessed and demonstrated.

生产商（或委派第三方）对原料药供应商和生产商、关键中间体供应商、内包材和印刷包材供应商、合同生产商和服务提供商实施的审计应包括对受托方组织内数据完整性措施的核查。审计期间，受托方应提供合理权限访问其代表委托方生成的数据，如此方可评估并证明其是否符合数据完整性和管理原则。

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:

审计和日常监管应包括委托方质量部门采用质量风险管理方法对电子源数据和元数据的充分核查。可以通过如下一些方法达成目标：

Site audit	Review the contract acceptors organisational behaviour, and understanding of data governance, data lifecycle, risk and criticality.
现场审核	审核合同接受方的组织行为，了解数据管理、数据生命周期、风险和关键程度。
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. Periodic proficiency testing of samples may be considered where relevant.
物料测试VS检验报告书	将分析测试的结果与供应商提交的COA进行比较。检查准确度、精确度或纯度结果之间的差异。可以日常、定期或以飞行检查的方式实施，具体取决于物料和供应商的风险。相关时可考虑定期使用样品进行熟练程度测试。
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.

远程数据审核	合同委托方可以考虑向受托工厂/供应商提供使用其自己的硬件和软件体系（通过宽域网WAN实现），用于批生产和批检验。合同委托方可以实时监测受托工厂人员所产生的数据的质量和完整性。在此情形下，应该有明确的职责划分，确保合同委托方对数据的监测不会修改合同受托方产所生的数据。
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.
质量监测	质量和绩效监测可以显示出数据做假的诱因（例如，频繁发生原料勉强符合质量标准的情况）。

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 acceptors 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.

合同委托方可与合同受托方合作，确保对所有客户机密信息进行编码，以消除客户身份信息。 这将有助于在合同委托方的站点审查源电子数据和元数据，而不会违反对其他客户的保密义务。 通过审查更大的数据集，可以对合同受托方的数据治理措施进行更可靠的评估。 这样还可以检索数据完整性失败的指标，例如重复的数据集或未按预期波动的数据。

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.

应注意确保所提供文件的真实性和准确性（参见第 8.11 节）。在决定分包商和供应链资格时，应考虑“真实副本”与“摘要报告”数据之间的数据完整性和可追溯性风险差异。

11 REGULATORY ACTIONS IN RESPONSE TO DATA INTEGRITY FINDINGS 数据完整性缺陷所引发的官方行动

11.1 Deficiency references 缺陷依据

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.

数据完整性对 GMP 是基本要求，优良数据管理的要求是嵌入现行的 PIC/S 药品 GMP/GDP 指南。以下表格提供了参考点，特别是一些已有要求。

ALCOA principle	PIC/S Guide to Good Manufacturing Practice for Medicinal products, PE 009 (Part I):	PIC/S Guide to Good Manufacturing Practice for Medicinal products, PE 009 (Part II):	Annex 11 (Computerised Systems)	PIC/S Guide to Good Distribution Practice for Medicinal products, PE 011:
ALCOA原则	**PIC/S药品GMP指南，PE009（第一部分）**	**PIC/S药品GMP指南，PE009（第二部分）**	**附录11（计算机化系统）**	**PIC/S药品GDP指南，PE011**
Attributable 可追溯性	[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 清晰	[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 同步	[4.8]	[6.14]	[12.4], [14]	[4.1], [4.2.9]
Original 原始	[4.9], [4.27], [Paragraph "Record"]	[6.14], [6.15], [6.16]	[8.2], [9]	[4.2.5]
Accurate 准确	[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 完整	[4.8]	[6.16], [6.50], [6.60], [6.61]	[4.8], [7.1], [7.2], [9]	[4.2.3], [4.2.5]
Consistent 一致	[4.2]	[6.15], [6.50]	[4.8], [5]	[4.2.3]
Enduring 持久	[4.1], [4.10]	[6.11], [6.12], [6.14]	[7.1], [17]	[4.2.6]
Available 可及	[Paragraph "Principle"], [4.1]	[6.12], [6.15], [6.16]	[3.4], [7.1], [16], [17]	[4.2.1]

11.2 Classification of deficiencies 缺陷分类

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.

注意：以下指南旨在帮助数据完整性缺陷的报告和分类保持一致，无意影响检查机构根据其内部政策或国家监管框架采取行动的能力。

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 actions of a single employee to an endemic failure throughout the inspected organisation.

与数据完整性失败相关的缺陷可能对产品质量产生不同的影响。从单个员工的行为到整个受检组织的地方性故障，故障的发生率也可能有所不同。

11.2.2 The PIC/S guidance[12] 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".

PIC/S 缺陷分类指南规定：

关键缺陷是指一种做法或工艺已造成，或将导致生产的一种产品对人体或动物患者产生伤害，或者可能在食用动物中产生有害残留的严重风险。如果发现生产商有欺诈、虚假陈述或伪造产品或数据的行为，亦归为关键缺陷。

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:

尽管与欺诈、虚假陈述或伪造有关的缺陷属于"关键"分类，但可以理解的是，数据完整性缺陷也可能涉及：

- Data integrity failure resulting from bad practice,
- 不良做法导致的数据完整性失败；
- Opportunity for failure (without evidence of actual failure) due to absence of the required data control measures.
- 由于缺乏所需数据控制措施而导致失败的机会（没有实际失败的证据）。

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

在这些情况下，适合通过考虑以下因素（仅指导性清单）来判定缺陷分类：

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

对产品产生的影响已对患者健康产生实际或潜在风险。关键缺陷：

- Product failing to meet Marketing Authorisation specification at release or within shelf life.
- 产品在放行时或货架期内不满足上市许可标准。
- Reporting of a 'desired' result rather than an actual out of specification result when reporting of QC tests, critical product or process parameters.
- 在报告 QC 检测结果、关键产品或工艺参数时，报告的是"期望的"结果而非实际 OOS 结果。
- Wide-ranging misrepresentation 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.
- 无论是否有高级管理人员知情和协助，大面积虚假陈述或捏造数据，其程度严重破坏了药

[12] PI 040 PIC/S Guidance on Classification of GMP Deficiencies PI 040 PIC/S GMP 缺陷分类指南

品质量体系的可靠性，并丧失了对该场所生产或处理的药品的质量和安全性的所有信心。

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

对产品产生的影响未对患者健康产生风险：主要缺陷：

- Data being misreported, e.g. original results 'in specification', but altered to give a more favourable trend.
- 数据漏报，例如原始结果"符合质量标准"，但进行修改给出更好的趋势。
- 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.
- 在报告非 QC 检测、关键产品或工艺参数数据时，报告"所需"结果，而不是报告实际的 OOS 结果
- Failures arising from poorly designed data capture systems (e.g. using scraps of paper to record info for later transcription).
- 设计不良的数据捕获系统产生的失败（例如，使用废弃的纸记录信息，事后再转抄）。

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

对产品没有影响；有发现广泛的失败证据：主要缺陷

- Bad practices and poorly designed systems which may result in opportunities for data integrity issues or loss of traceability across a limited number of functional areas (QA, production, QC etc.). Each in its own right has no direct impact to product quality.
- 可能会导致数据完整性问题或大量功能性领域（QA、生产、QC 等）可追溯性缺失机会的不良做法和设计不良的系统。

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

对产品没有影响；失败证据有限：其它缺陷

- Bad practice or poorly designed system which result in opportunities for data integrity issues or loss of traceability in a discrete area.
- 不良做法或设计不良的系统，会导致数据完整性问题或零散领域内可追溯性缺失的机会。
- Limited failure in an otherwise acceptable system, e.g. manipulation of non-critical data by an individual.
- 其它可接受系统里有限的失败，例如，一个人捏造非关键数据

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.

很重要的一点是要建立关键要素（数据管理流程、系统设计促进符合性数据记录、使用和核对审核追踪和 IT 用户权限等）充分性的整体画面，以做出稳健的评估，确定是否在公司范围内都存在失败，还是在有限的范围/影响的缺陷。

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* PI 040.

个别环境（加剧/缓解因素）可能也会影响分级和法规行动。关于缺陷分级和药监局内报告符合性问题的更多指南在 PI 040【PIC/S 缺陷分类指南】中可以找到。

12 REMEDIATION OF DATA INTEGRITY FAILURES 数据完整性失败的补救

12.1 Responding to Significant Data Integrity issues 对重大数据完整性问题的响应

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 as part of a remediation plan. Responses from implicated manufacturers should include:

应主要考虑解决已发现的紧迫问题，并评估与数据完整性问题有关的风险。相关公司的回复应该列出作为补救计划一部分所采取的措施。受影响生产商的回复应该包括：

12.1.1.1 A comprehensive investigation into the extent of the inaccuracies in data records and reporting, to include: 对数据记录和报告的不准确程度全面调查，在其中包括：

- A detailed investigation protocol and methodology; a summary of all laboratories, manufacturing operations, products and systems to be covered by the assessment; and a justification for any part of the operation that the regulated user proposes to exclude[13];
- 详细的调查方案和方法学；一份准备包括在评估中的所有实施室、生产操作、产品和系统的汇总；并说明为何将受监管用户运营的一部分工作排除在外；
- Interviews of current and where possible and appropriate, former employees to identify the nature, scope, and root cause of data inaccuracies. These interviews may be conducted by a qualified third party;
- 在可能和适当的情况下，与现任和前任员工进行面谈，以确定数据不准确的性质、范围和根本原因。这些面谈可由具备资质的第三方执行；
- 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;
- 对设施内数据完整性缺陷程度的评估。识别出遗漏、修改、删除、记录销毁、非同步记录和其它缺陷；
- Determination of the scope (data, products, processes and specific batches) and timeframe for the incident, with justification for the time-boundaries applied;
- 确定事件的范围（数据、产品、工艺和特定批次）以及时间框架，并说明为何框定该时间范围；
- A description of all parts of the operations in which data integrity lapses occurred, additional consideration should be given to global corrective actions for multinational companies or those that operate across multiple sites;
- 描述发生数据完整性问题的操作的所有部分，跨国公司或多场所运营的公司还要考虑全球纠正措施。
- A comprehensive retrospective evaluation of the nature of the data integrity deficiencies, and the identification of root cause(s) or most likely root cause that will form the basis of corrective and preventative actions, as defined in the investigation protocol. The services of a qualified third-party consultant with specific expertise in the areas where potential breaches were identified may be required;
- 对数据完整性缺陷的性质进行全面的回顾性评估，并确定根本原因或最可能的根本原因，这些原因将按调查方案所规定的成为 CAPA 的基础。可能需要在已发现有潜在问题的领域具备专业知识的具备资质第三方顾问提供服务。

[13] 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. 调查范围应包括对公司层面数据完整性程度的评估，包括所有可能受影响的设施、场所和部门。

- A risk assessment of the potential effects of the observed failures on the quality of the substances, medicines, and products 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 integrity of data submitted to regulatory agencies, including data related to product registration dossiers.
- 对所涉及物质、药品和产品中发现的问题的潜在后果进行风险评估。评估应包括对受数据完整性失效影响的产品放行/销售导致的患者潜在风险、持续运营带来的风险以及对提交给监管机构的数据完整性的任何影响的分析，包括与产品注册文件有关的数据。

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

为解决数据完整性薄弱点而采取的 CAPA，及其实施时间表，并包括：

- 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. Interim measures should be monitored for effectiveness and residual risks should be communicated to senior management, and kept under review.
- 描述保护患者和确保药品质量的行动的临时措施，例如通知客户、召回产品、进行额外测试、增加稳定性试验批次以确保稳定性、药物申报措施，以及加强投诉监测。应监测临时措施的有效性，应与高级管理层沟通残余风险，并保持审核。
- 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. Where long term measures are identified interim measures should be implemented to mitigate risks.
- 描述指在确保数据完整性的程序、流程、方法、控制、系统、管理监督和人力资源（例如培训、人员配备改进）的任何补救工作和改进的长期措施。如果确定了长期措施，则应执行临时措施缓解风险。

12.1.1.3 CAPA effectiveness checks implemented to monitor if the actions taken has eliminated the issue.

所实施的 CAPA 有效性检查，从而监测所采取措施是否已将问题消除。

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 a comprehensive investigation and a 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:

在可能情况下，检查人员应该与受影响公司的高级代表会面，告知所发现的缺陷情况，要求公司出具书面确认书，承诺全面调查和和坦白问题，以及快速解决问题。应该向监管机构提交一份管理策略，其中包括全球 CAPA 计划。策略应包括：

- 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 should indicate if individuals responsible for data integrity lapses remain able to influence GMP/GDP-related or drug application data.
- 全面措施数据完整性失效的根本原因，包括证明当前行动计划的范围和深度与调查和风险评估结果相称的证据。这应该表明负责数据完整性失误的个人是否仍然能够

影响 GMP/GDP 相关数据或药物申报数据。

- 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.
- 详细的纠正措施计划，说明受监管用户准备如何确保生成的所有数据的 ALOCA+ 属性（参见 7.4），包括分析数据、生产记录，以及所有提交给或呈现给药监当局的数据。

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.

检查组应执行政策对检查期间发现严重数据完整性问题进行管理，从而管理和控制与数据完整性问题有关的风险。

12.2 Indicators of improvement 改进指标

12.2.1 An on-site inspection is recommended to verify the effectiveness of actions taken to address serious data integrity issues. Alternative approaches to verify effective remediation may be considered in accordance with risk management principles. Some indicators of improvement are:

建议进行现场检查，以核查为解决严重数据完整性问题而采取的措施的有效性。可以根据风险管理原则考虑采用其它方法核查补救措施的有效性。以下是一些改进指标：

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;

对已识别的问题进行彻底和公开评估并及时实施有效纠正和预防措施的证据，包括在组织层面适当实施纠正和预防措施；

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;

与客户和其它监管机构公开沟通问题的证据。应在整个调查和补救阶段保持透明的沟通。监管机构应该意识到，详细调查的结果可能会报告进一步的数据完整性问题。对这些通知的任何额外反应均应与公众卫生风险相称，以鼓励继续报告；

12.2.1.3 Evidence of communication of data integrity expectations across the organisation, incorporating and encouraging processes for open reporting of potential issues and opportunities for improvement;

在组织内沟通数据完整性要求的证据，制订并鼓励公开报告潜在问题和改进机会的流程；

12.2.1.4 The regulated user should ensure that an appropriate evaluation of the vulnerability of electronic systems to data manipulation takes place to ensure that follow-up actions have fully resolved all the violations. For this evaluation the services of qualified third party consultant with the relevant expertise may be required;

受监管的用户应确保对所有电子系统的可能发生数据篡改的弱点进行适当的评估，确保跟踪措施能全面解决所有违规情况。此类评估可能需要具有相关专业知识的合格第三方顾问提供服务；

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

实施数据完整性方针，符合本指南中的原则。

12.2.1.6 Implementation of routine data verification practices.

实施日常数据核查规范。

13 Glossary 术语

Archiving 归档

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

完整数据和相关元数据以其最终可以重新构建过程和活动的形式被长期永久保存。

Audit Trail 审计追踪

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

GMP/GDP审计追踪是GMP/GDP关键信息（例如，GMP/GDP相关数据的创建、修改和删除）记录的元数据，它使得可以重新构建GMP/GDP活动。

Back-up 备份

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.

现行（可编辑）数据、元数据和系统参数设置（例如，与分析运行有关的可变设置）为保证灾难后恢复而保存的副本。

Computerised system 计算机化系统

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

一套包括有数据输入、电子处理和信息输出用于报告或自动化控制的系统。

Data 数据

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

所收集用于参考或分析的事实、数值和统计结果。

Data Flow Map 数据流向图

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

以图形方式呈现的数据在整个信息系统中的“流向”。

Data Governance 数据治理

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.

保证数据（不管其格式如何、如何生成）的记录、处理、保存和使用过程的一系列安排的总和，用以确保整个数据生命周期中其完整性、一致性和准确性。

Data Integrity 数据完整性

The degree to which data are complete, consistent, accurate, trustworthy, reliable and that these characteristics of the data are maintained throughout the data life cycle.

The data should be collected and maintained in a secure manner, so that they are attributable, legible, contemporaneously recorded, original (or a true copy) and accurate. Assuring data integrity requires appropriate quality and risk management systems, including adherence to sound scientific principles and good documentation practices. The data should comply with ALCOA+ principles.

所有数据在其生命周期内的完整、一致、准确、值得信任、可靠，以及在数据生命周期内这些特

性得到维护的程度。

数据应以安全方式采集和保存，应可追溯、清晰、同步记录、原始（或真实副本）和准确。保证数据的完整性需要有合适的质量和风险管理系统，包括遵守科学合理的原则和优良文件规范。数据应该符合ALCOA+原则。

Data Lifecycle 数据生命周期

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.

数据（包括原始数据）生命中所有阶段，从最初产生和记录到处理（包括转化或迁移）、使用、数据保存、归档、恢复和销毁。

Data Quality 数据质量

The assurance that data produced is exactly what was intended to be produced and fit for its intended purpose. This incorporates ALCOA + principles.[14]

使得数据按其预期准确产生，且符合其既定用途的保障。其中包括 ALCOA+原则。

Data Ownership 数据所有权

The allocation of responsibilities for control of data to a specific process owner. Companies should implement systems to ensure that responsibilities for systems and their data are appropriately allocated and responsibilities undertaken.

将数据控制的职责分配给特定的流程所有者的过程。公司所实施的系统应确保恰当地分配系统及其数据的职责，以及这些职责得到恰当的履行。

Dynamic Record 动态记录

Records, such as electronic records, that allow an interactive relationship between the user and the record content[14].

允许用户和记录内容进行互动的记录，如电子记录。

Exception Report 异常报告

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

一个经过验证的搜索工具，它识别并记录预定为“异常”的数据或行为，需要数据审核员更多关注或进一步调查。

Good Documentation Practices (GdocP) 优良文件规范

Those measures that collectively and individually ensure documentation, whether paper or electronic, meet data management and integrity principles, e.g. ALCOA+.

集中和单独保证文件（纸质或电子）符合数据管理和完整性原则（即 ALCOA+）的措施。

Hybrid Systems 混合系统

A system for the management and control of data that typically consists of an electronic system generating electronic data, supplemented by a defined manual system that typically generate a paper-based record. The complete data set from a hybrid system therefore consists of both electronic and paper data together. Hybrid systems rely on the effective management of both sub-systems for correct operation.

一个管理和控制数据的系统，一般包括有生成电子数据的电子系统，由规定的人工系统（一般生成纸质记录）进行补充。因此来自混合系统的完整的数据组同时包括有电子和纸质数据。混合系统依赖于对子系统正确运行的有效管理。

[14] 'GXP' Data Integrity Guidance and Definitions, MHRA, March 2018 GXP 数据完整性指南和定义，MHRA，2018 年 3 月

Master Document 主文件

An original approved document from which controlled copies for distribution or use can be made.

经过批准的原始文件，采用该文件制作受控副本供分发或使用。

Metadata 元数据

In-file data that describes the attributes of other data, and provides context and meaning.

Typically, these are data that describe the structure, data elements, inter-relationships and other characteristics of data e.g. audit trails. Metadata also permit data to be attributable to an individual (or if automatically generated, to the original data source). Metadata form an integral part of the original record. Without the context provided by metadata the data has no meaning.

描述其他数据的属性并提供上下文和含义的文件内数据。

通常，这些是描述数据的结构、数据元素、相互关系和其他特征的数据，例如 审计追踪。 元数据还允许将数据追溯至个人（或者如果是自动生成的，则追溯至原始数据源）。 元数据是原始记录的组成部分。 如果没有元数据提供的上下文，数据就没有意义。

Quality Unit 质量部门

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.

受监管实体内负责质量监督的部门，尤其包括药品质量体系的设计、有效实施、监控和维护。

Raw Data 原始数据

Raw data is defined as the original record (data) which can be described as the first- capture of information, whether recorded on paper or electronically. Information that is originally captured in a dynamic state should remain available in that state.[14]

原始数据被定义为原始记录（数据），它可以被描述为第一次捕获的信息，无论是记录在纸上还是电子形式。 最初在动态状态下捕获的信息应在该状态下保持可用。

Static Record 静态记录

A record format, such as a paper or electronic record, that is fixed and allows little or no interaction between the user and the record content.[14]

一种固定的记录格式，如纸质记录或电子记录，用户与记录内容只能进行很少或者无法进行互动。

Supply Chain 供应链

The sum total of arrangements between manufacturing sites, wholesale and distribution sites that ensure that the quality of medicines in ensured throughout production and distribution to the point of sale or use.

生产场所、批发和分发地点之间的安排总和，以确保药品质量在整个生产和分发到销售或使用点的整个过程中得到保证。

System Administrator 系统管理员

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

管理计算机化系统或特定电子通信服务操作的人。

14 REVISION HISTORY 修订历史

Date 日期	Version Number 版本号	Reasons for revision 修订原因