Annex 4
附录 4

Guideline on data integrity
数据完整性指南

This document replaces the WHOGuidance on good data and record management practices (Annex 5, WHO Technical Report Series, No. 996, 2016) (1).
本文件取代了《WHO 良好数据和记录管理规范指南》(WHO 技术报告系列，No. 996, 2016 附件 5，)(1)。

1. Introduction and background
介绍和背景

1.1. In recent years, the number of observations made regarding the integrity of data, documentation and record management practices during inspections of good manufacturing practice (GMP) (2), good clinical practice (GCP), good laboratory practice (GLP) and Good Trade and Distribution Practices (GTDP) have been increasing. The possible causes for this may include
近年来，在对良好生产规范(GMP)(2)、良好临床规范(GCP)、良好实验室规范(GLP)和良好贸易和分销规范(GTDP)的检查过程中，对数据完整性、文件和记录管理规范的缺陷数量持续增加。可能的原因包括：

(ⅰ) reliance on inadequate human practices;
依赖于不适当的人员操作;
(ⅱ)poorly defined procedures;
规定糟糕的规程
(ⅲ)resource constraints;
资源限制
(ⅳ) the use of computerized systems that are not capable of meeting regulatory requirements or are inappropriately managed and validated (3, 4);
使用不满足法规要求，或管理/验证不当的计算机系统(3,4);
(ⅴ) inappropriate and inadequate control of data flow; and
不适当和不充分的数据流控制;和
(ⅵ)failure to adequately review and manage original data and records.
未能充分审核和管理原始数据和记录。

1.2. Data governance and related measures should be part of a quality system, and are important to ensure the reliability of data and records in good practice (GxP) activities and regulatory submissions. The data and records should be 'attributable, legible, contemporaneous, original' and accurate, complete, consistent, enduring, and available; commonly referred to as "ALCOA+".
数据治理和相关措施应该是质量体系的一部分，对于确保 GxP 活动和法规申报中的数据和记录的可靠性非常重要。数据和记录应是"可归属的、易读的、同步的、原始的"、准确的、完整的、一致的、持久的和可用的;通常称为"ALCOA+"。

1.3. This document replaces the WHO Guidance on good data and record management practices (Annex 5, WHO Technical Report Series, No. 996, 2016) (1).
本文件取代了《WHO 良好数据和记录管理规范指南》(WHO 技术报告系列，No. 996, 2016，附件 5)(1)。

2. Scope
范围

2.1. This document provides information, guidance and recommendations to strengthen data integrity in support of product quality, safety and efficacy. The aim is to ensure compliance with regulatory requirements in, for example clinical research, production and quality control, which ultimately contributes to patient safety. It covers electronic, paper and hybrid systems.

本文件提供了用以巩固数据完整性的信息、指南和建议，以支持产品质量、安全性和有效性。目的是确保在临床研究、生产和质量控制等方面符合法规要求，保证患者安全。它涵盖了电子，纸张和混合系统。

2.2. The guideline covers ”GxP” for medical products. The principles could also be applied to other products such as vector control products.
本指南涵盖了医药产品 “GxP”。这些原则也可应用于其他产品，如病媒控制产品。

2.3. The principles of this guideline also apply to contract givers and contract acceptors. Contract givers are ultimately responsible for the integrity of data provided to them by contract acceptors. Contract givers should therefore ensure that contract acceptors have the appropriate capabilities and comply with the principles contained in this guideline and documented in quality agreements.
本指南的原则也适用于委托方和受托方。委托方对受托方提供给他们的数据的完整性负有最终责任。因此，委托方应确保受托方具有适当的能力，并遵守本指南和质量协议中所包含的原则。

2.4. Where possible, this guideline has been harmonised with other published documents on data integrity. This guideline should also be read with other WHO good practices guidelines and publications including, but not limited to, those listed in the references section of this document.
本指南已尽可能与其他公布的数据完整性文件相协调。本指南还应与 WHO 其他良好规范指南和出版物一起阅读，包括但不限于本文件参考章节中所列的内容。

3. Glossary
术语

The definitions given below apply to the terms used in these guidelines. They may have different meanings in other contexts.
以下给出的定义适用于本指南中使用的术语。它们在其他环境可能有不同的含义。

ALCOA+.

A commonly used acronym for “attributable, legible, contemporaneous, original and accurate” which puts additional emphasis on the attributes of being complete, consistent, enduring and available throughout the data life cycle for the defined retention period.

Archiving.
归档

Archiving is the process of long-term storage and protection of records from the possibility of deterioration, and being altered or deleted, throughout the required retention period. Archived records should include the complete data, for example, paper records, electronic records including associated metadata such as audit trails and electronic signatures. Within a GLP context, the archived records should be under the control of independent data management personnel throughout the required retention period.

Audit trail.
审计追踪

The audit trail is a form of metadata containing information associated with actions that relate to the creation, modification or deletion of GxP records. An audit trail provides for a secure recording of life cycle details such as creation, additions, deletions or alterations of information in a record, either paper or electronic, without obscuring or overwriting the original record. An audit trail facilitates the reconstruction of the history of such events relating to the record regardless of its medium, including the “who, what, when and why” of the action.

Backup.
备份

The copying of live electronic data, at defined intervals, in a secure manner to ensure that the data are available for restoration.

Certified true copy or true copy.
经认证的真实副本或真实副本

A copy (irrespective of the type of media used) of the original record that has been verified (i.e. by a dated signature or by generation through a validated process) to have the same information, including data that describe the context, content, and structure, as the original.

Data.
数据

All original records and true copies of original records, including source data and metadata, and all subsequent transformations and reports of these data which are generated or recorded at the time of the GMP activity and which allow full and complete reconstruction and evaluation of the GMP activity. Data should be accurately recorded by permanent means at the time of the activity. Data may be contained in paper records (such as worksheets and logbooks), electronic records and audit trails, photographs, microfilm or microfiche, audio or video files or any other media whereby information related to GMP activities is recorded.

Data criticality.
数据关键性

This is defined by the importance of the data for the quality and safety of the product and how important data are for a quality decision within production or quality control.
由数据对产品质量和安全的重要性以及数据对生产或质量控制中的质量决策的重要性。

Data governance.
数据治理

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

保证数据质量的所有工作。确保数据，无论其产生、记录、处理、保存、检索和使用的过程、格式或技术，都将确保其在整个数据生命周期内具有可归属、可读、同步、原始、准确、完整、一致、持久和可用的记录。

Data integrity risk assessment (DIRA).
数据完整性风险评估

The process to map out procedures, systems and other components that generate or obtain data; to identify and assess risks and implement appropriate controls to prevent or minimize lapses in the integrity of the data.
一个过程：列出数据产生或获取的程序、系统及其他组件;识别和评估风险，并实施适当的控制措施，以防止或降低数据完整性方面的失效。

Data life cycle.
数据生命周期

All phases of the process by which data are created, recorded, processed, reviewed, analysed and reported, transferred, stored and retrieved and monitored, until retirement and disposal. There should be a planned approach to assessing, monitoring and managing the data and the risks to those data, in a manner commensurate with the potential impact on patient safety, product quality and/or the reliability of the decisions made throughout all phases of the data life cycle.

Dynamic data.
动态数据

Dynamic formats, such as electronic records, allow an interactive relationship between the user and the record content. For example, electronic records in database formats allow the user to track, trend and query data; chromatography records maintained as electronic records allow the user or reviewer (with appropriate access permissions) to reprocess the data and expand the baseline to view the integration more clearly.

Electronic signatures.
电子签名

A signature in digital form (bio-metric or non-biometric) that represents the signatory. In legal terms, it is the equivalent of the handwritten signature of the signatory.

Good practices (GxP).
良好规范

An acronym for the group of good practice guides governing the preclinical, clinical, manufacturing, testing, storage, distribution and post-market activities for regulated pharmaceuticals, biologicals and medical devices, such as GLP, GCP, GMP, good pharmacovigilance practices (GVP) and good distribution practices (GDP).

Hybrid system.
混合系统

The use of a combination of electronic systems and paper systems.

Medical product.
医疗产品

A term that includes medicines, vaccines, diagnostics and medical devices.
包括药品、疫苗、诊断试剂和医疗器械。

Metadata.
元数据

Metadata are data that provide the contextual information required to understand other data. These include structural and descriptive metadata, which describe the structure, data elements, interrelationships and other characteristics of data. They also permit data to be attributable to an individual. Metadata that are necessary to evaluate the meaning of data should be securely linked to the data and subject to adequate review. For example, in the measurement of weight, the number 8 is meaningless without metadata, such as, the unit, milligram, gram, kilogram, and so on. Other examples of metadata include the time or date stamp of an activity, the operator identification (ID) of the person who performed an activity, the instrument ID used, processing parameters, sequence files, audit trails and other data required to understand data and reconstruct activities.

Raw data.
原始数据

The original record (data) which can be described as the first-capture of information, whether recorded on paper or electronically. Raw data is synonymous with source data.

Static data.
静态数据

A static 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. For example, once printed or converted to static electronic format chromatography records lose the capability of being reprocessed or enabling more detailed viewing of baseline.

4. Data governance
数据治理

4.1. There should be a written policy on data integrity.
应有数据完整性的书面政策。

4.2. Senior management should be accountable for the implementation of systems and procedures in order to minimise the potential risk to data integrity, and to identify the residual risk using risk management techniques such as the principles of the guidance on quality risk management from WHO (5) and The International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use (ICH) (6).
高级管理层应对系统和程序的实施负责，以最小化数据完整性的潜在风险,并使用风险管理技术（如 WHO 质量风险管理原则指南(5)和 ICH 人用药物技术要求（6））确定剩余风险。

4.3. Senior management is responsible for the establishment, implementation and control of an effective data governance system. Data governance should be embedded in the quality system. The necessary policies, procedures, training, monitoring and other systems should be implemented.
高级管理层负责建立、实施和控制有效的数据治理体系。数据治理应作为质量体系的一部分。应执行必要的政策、程序、培训、监测和其他制度。

4.4. Data governance should ensure the application of ALCOA+ principles.
数据治理应确保应用 ALCOA+原则。

4.5. Senior management is responsible for providing the environment to establish, maintain and continually improve the quality culture, supporting the transparent and open reporting of deviations, errors or omissions and data integrity lapses at all levels of the organization. Appropriate, immediate action should be taken when falsification of data is identified. Significant lapses in data integrity that may impact patient safety, product quality or efficacy should be reported to the relevant medicine regulatory authorities.
高级管理人员应负责对建立、保持和持续改进质量文化提供环境，支持在组织的各个层级透明和公开地报告偏差、错误或遗漏和数据完整性缺失。当发现数据造假时，应立即采取适当的行动。可能影响患者安全、产品质量或疗效的数据完整性重大偏差，应向相关药品监管部门报告。

4.6. The quality system, including documentation such as procedures and formats for recording and reviewing of data, should be appropriately designed and implemented in order to provide assurance that records and data meet the principles contained in this guideline.
质量体系，包括数据记录和审核的程序和格式等文件，应适当设计和实施，以确保记录和数据符合本指南所包含的原则。

4.7. Data governance should address the roles, responsibilities, accountability and define the segregation of duties throughout the life cycle and consider the design, operation and monitoring of processes/systems to comply with the principles of data integrity, including control over authorized and unauthorized changes to data.
数据治理应该处理角色、责任、义务，并定义整个生命周期的职责划分，考虑流程/系统的设计、操作和监控，以符合数据完整性原则，包括对已授权和未授权的数据更改的控制。

4.8. Data governance control strategies using quality risk management (QRM) principles (5) are required to prevent or mitigate risks. The control strategy should aim to implement appropriate technical, organizational and procedural controls. Examples of controls may include, but are not limited to:
有必要使用基于质量风险管理(QRM)原则的数据治理控制策略，以防止或降低风险。控制策略应旨在实施适当的技术性、组织性和程序性控制。控制示例包括但不限于:

- the establishment and implementation of procedures that will facilitate compliance with data integrity requirements and expectations;
- 建立和实施有助于遵守数据完整性要求和期望的程序;
- the adoption of a quality culture within the company that encourages personnel to be transparent about failures, which includes a reporting mechanism inclusive of investigation and follow-up processes;

- 在公司内部采用一种质量文化，鼓励员工对失败做到透明，这包括一种报告机制，包括调查和后续过程;
- the implementation of appropriate controls to eliminate or reduce risks to an acceptable level throughout the life cycle of the data;
- 实施适当的控制，在数据的整个生命周期内消除或降低风险至可接受的水平;
- ensuring sufficient time and resources are available to implement and complete a data integrity programme; to monitor compliance with data integrity policies, procedures and processes through e.g. audits and self-inspections; and to facilitate continuous improvement of both;
- 确保有足够的时间和资源实施和完成一项数据完整性计划; 透过审计及自查等方式，检查符合数据完整性政策、程序及过程的情况;并促进他们持续改善;
- the assignment of qualified and trained personnel and provision of regular training for personnel in, for example, GxP, and the principles of data integrity in computerized systems and manual/ paper based systems;
- 分配有资质及经培训的人员，并定期为人员提供培训，例如 GxP，以及计算机化系统和手动/纸张系统的数据完整性原则;
- the implementation and validation of computerized systems appropriate for their intended use, including all relevant data integrity requirements in order to ensure that the computerized system has the necessary controls to protect the electronic data (3); and
- 实施和验证计算机化系统符合其预期用途，包括所有相关的数据完整性要求，以确保计算机化系统具有保护电子数据的必要控制(3);和
- the definition and management of the appropriate roles and responsibilities for contract givers and contract acceptors, entered into quality agreements and contracts including a focus on data integrity requirements.
- 定义和管理委托方和受托方的适当角色和责任，签订质量协议和合同，其中包含数据完整性的要求。

4.9. Data governance systems should include, for example:
数据治理系统应该包括，例如:

- the creation of an appropriate working environment;
- 创造适当的工作环境;
- active support of continual improvement in particular based on collecting feedback; and
- 积极支持持续改进，尤其在收集反馈的基础上;和
- review of results, including the reporting of errors, unauthorized changes, omissions and undesirable results.
- 对结果进行评审，包括对错误、未经授权的更改、遗漏和不良结果的报告。

4.10. The data governance programme should include policies and procedures addressing data management. These should at least where applicable, include:
数据治理程序应包括数据管理的政策和程序。这至少应包括（如适用）：

- management oversight and commitment;
- 管理监督和承诺
- the application of QRM;
- QRM 的使用
- compliance with data protection legislation and best practices;
- 遵守数据保护法律及最佳实践;

- qualification and validation policies and procedures;
- 确认和验证的政策和程序;
- change, incident and deviation management;
- 变更，事件和偏差管理
- data classification, confidentiality and privacy;
- 数据分类，保密和隐私
- security, cybersecurity, access and configuration control;
- 安全、网络安全、访问和配置控制;
- database build, data collection, data review, blinded data, randomization;
- 数据库建立，数据收集，数据审查，盲法数据，随机数据;
- the tracking, trending, reporting of data integrity anomalies, and lapses or failures for further action;
- 对数据完整性异常进行跟踪、趋势分析和报告，以及进一步行动的失效或失败;
- the prevention of commercial, political, financial and other organizational pressures;
- 防止商业、政治、金融和其他组织压力;
- adequate resources and systems;
- 充足的资源和体系
- workload and facilities to facilitate the right environment that supports DI and effective controls;
- 工作负荷和设施，以促进帮助支持数据完整性和有效控制的正确环境，;
- monitoring;
- 监测
- record-keeping;
- 记录保存
- training; and
- 培训
- awareness of the importance of data integrity, product quality and patient safety.
- 对数据完整性、产品质量和患者安全的重要性的认识。

4.11. There should be a system for the regular review of data for consistency with ALCOA+ principles. This includes paper records and electronic records in day-to-day work, system and facility audits and self-inspections.
应有一个定期审查数据的系统，以符合 ALCOA+原则。包括日常工作、系统及工厂审计及自查的纸质记录及电子记录。

4.12. The effort and resources applied to assure the integrity of the data should be commensurate with the risk and impact of a data integrity failure.
用于确保数据完整性的努力和资源应与数据完整性失败的风险和影响相称。

4.13. Where weaknesses in data integrity are identified, the appropriate corrective and preventive actions (CAPA) should be implemented across all relevant activities and systems and not in isolation.
当发现数据完整性缺陷时，应对所有相关活动和系统均实施适当的纠正和预防措施(CAPA)，而不是孤立地实施。

4.14. Changing from paper-based systems to automated or computerised systems (or vice-versa) will not in itself remove the need for appropriate data integrity controls.
从基于纸张的系统转变为自动化或计算机化系统本身并不能消除对适当的数据完整性控制的需要(或反之亦然)。

4.15. Records (paper and electronic) should be kept in a manner that ensures compliance with the principles of this guideline. These include but are not limited to:
记录(纸质和电子)的保存方式应确保符合本指南的原则。这包括但不限于:

- ensuring time accuracy of the system generating the record, accurately configuring and verifying time zone and time synchronisation, and restricting the ability to change dates, time zones and times for recording events;
- 确保生成记录的系统时间准确，准确地配置和核实时区和时间同步，并限制更改记录事件日期、时区和时间的能力;
- using controlled documents and forms for recording GxP data;
- 使用受控的文件和表格来记录 GxP 数据;
- defining access and privilege rights to GxP automated and computerized systems, ensuring segregation of duties;
- 规定进入 GxP 自动化和计算机化系统的访问和权限，确保职责分离;
- ensuring audit trail activation for all interactions and restricting the ability to enable or disable audit trails (Note: 'back-end' changes and 'hard' changes, such as hard deletes, should not be allowed). Where audit trials can be disabled then this this action should also appear in the audit trail;
- 确保对所有交互活动激活审计追踪，并限制启用或禁用审计追踪的能力(注意:不应允许"后台"更改和"硬"更改，如硬删除)。如果可以禁用审计追踪，那么这个操作也应该出现在审计追踪中;
- having automated data capture systems and printers connected to equipment and instruments in production (such as Supervisory Control and Data Acquisition (SCADA), Human Machine Interface (HMI) and Programme Logic Control (PLCs) systems), in , quality control, and in clinical research (such as Clinical Data Management (CDM) systems), where possible;
- 在可能的情况下，将自动数据采集系统和打印机连接到生产车间、QC 和临床试验的设备和仪器(如监测控制和数据采集（SCADA）、人机界面(HMI)和程序逻辑控制(PLC)系统、临床数据管理(CDM)系统);
- designing processes in a way to avoid the unnecessary transcription of data or unnecessary conversion from paper to electronic and vice versa; and
- 设计流程，以避免不必要的数据誊写，或不必要地将纸质转换成电子，或将电子转换成纸质;和
- ensuring the proximity of an official GxP time source to site of GxP activity and record creation.
- 确保公司的 GxP 活动和记录的创建接近一个正式的 GxP 时间源。

4.16. Systems, procedures and methodology used to record and store data should be periodically reviewed for effectiveness. These should be updated throughout the data life cycle, as necessary, where new technology becomes available. New technology implementation must be evaluated before implementation to verify the impact on data integrity.
应定期审查用于记录和存储数据的系统、程序和方法的有效性。当有新技术可用时，这些数据应该在整个数据生命周期中进行更新。新技术的实施必须在实施前进行评估，以验证对数据完整性的影响。

5. Quality risk management

质量风险管理

Note: documentation of data flows and data process maps are recommended to facilitate the assessment, mitigation and control of data integrity risks across the actual and intended data process(es).
注:建议将数据流程和数据流程图形成文件，以帮助对实际和预期数据流程的数据完整性风险的评估、降低和控制。

5.1. Data Integrity Risk Assessment (DIRA) should be carried out in order to identify and assess areas of risk. This should cover systems and processes that produce data or, where data are obtained and inherent risks. The DIRAs should be risk-based, cover the life cycle of data and consider data criticality. Data criticality may be determined by considering how the data is used to influence the decisions made. The DIRAs should be documented and reviewed, as required, to ensure that it remains current.
应进行数据完整性风险评估(DIRA)，以识别和评估风险的领域。这应该包括产生数据的系统和过程，或者获得数据地方和固有的风险。DIRAs 应该基于风险，涵盖数据的生命周期并考虑数据的关键性。数据的关键性可以通过考虑该数据如何影响所做的决策来确定。DIRAs 应形成文件并进行审核，必要时确保其保持更新。

5.2. The risk assessments should evaluate, for example, the relevant GxP computerised systems, supporting personnel, training, quality systems and outsourced activities.
风险评估应评估，例如相关的 GxP 计算机化系统、支持人员、培训、质量体系和外包活动。

5.3. DI risks should be assessed and mitigated. Controls and residual risks should be communicated. Risk review should be done throughout the document and data life cycle at a frequency based on the risk level, as determined by the risk assessment process.
应该评估和降低 DI 的风险。应对控制措施和剩余风险进行沟通。在文件和数据的整个生命周期中，应根据基于风险水平的频率进行风险审核，这因通过风险评估过程确定。

5.4. Where the risk assessment has highlighted areas for remedial action, the prioritisation of actions (including the acceptance of an appropriate level of residual risk) and the prioritisation of controls should be documented and communicated. Where long-term remedial actions are identified, risk-reducing short-term measures should be implemented in order to provide acceptable data governance in the interim.
当风险评估提出补救措施时，应对补救措施的优先级(包括对适当水平的剩余风险的接受)和控制措施的优先级进行记录并沟通。如确定了长期的补救措施，应实施降低风险的短期措施，以便在短期内提供可接受的数据治理。

5.5. Controls identified may include organizational, procedural and technical controls such as procedures, processes, equipment, instruments and other systems in order to both prevent and detect situations that may impact on data integrity. Examples include the appropriate content and design of procedures, formats for recording, access control, the use of computerized systems and other means.
控制措施可能包括组织性、程序性和技术性控制，如程序、流程、设备、仪器和其他系统，以预防和检测可能影响数据完整性的情况。示例包括程序的适当内容和设计、记录的格式、访问控制、计算机化系统的使用和其他手段。

5.6. Efficient risk-based controls should be identified and implemented to address risks impacting data integrity. Risks include, for example, the deletion of, changes to and exclusion of data or results from data sets without written justification, authorisation where appropriate, and detection. The effectiveness of the controls should be verified (see Appendix 1 for examples).
应确定和实施有效的基于风险的控制措施，以解决影响数据完整性的风险。风险包括，例如，在没有书面理由，适当授权和检测的情况下，从数据集中删除、更改和排除数据或结果。控制措施的有效性应进行确认(示例见附录 1)。

6. Management review
管理评审

6.1. Management should ensure that systems (such as computerized systems and paper systems) are meeting regulatory requirements in order to support data integrity compliance.
管理层应确保系统(如计算机化系统和纸质系统)满足法规要求，以支持数据完整性合规。

6.2. The acquisition of non-compliant computerized systems and software should be avoided. Where existing systems do not meet current requirements, appropriate controls should be identified and implemented based on risk assessment.
应避免购买不符合规定的计算机化系统和软件。当现有的系统不能满足当前的要求时，应根据风险评估确定并实施适当的控制措施。

6.3. The effectiveness of the controls implemented should be evaluated through, for example:
所实施控制措施的有效性应通过以下方式进行评估:

- the tracking and trending of data;
- 数据的跟踪和趋势分析
- a review of data, metadata and audit trails (e.g. in warehouse and material management, production, quality control, case report forms and data processing); and
- 数据、元数据及审计追踪(例如仓库及物料管理、生产、质量控制、个案报告表格及数据处理)的审核;和
- routine audits and/or self-inspections, including data integrity and computerized systems.
- 例行审计和/或自检，包括数据完整性和计算机化系统。

7. Outsourcing
外包

7.1. The selection of a contract acceptor should be done in accordance with an authorized procedure. The outsourcing of activities, ownership of data, and responsibilities of each party (contract giver and contract accepter) should be clearly described in written agreements. Specific attention should be given to ensuring compliance with data integrity requirements. Provisions should be made for responsibilities relating to data when an agreement expires.

应按照经批准的程序选择受托方。应在书面协议中明确描述所外包的活动、数据的所有权以及各方(委托方和受托方)的责任。应特别注意确保遵守数据完整性要求。应规定合同到期后与数据有关的责任。

7.2. Compliance with the principles and responsibilities should be verified during periodic site audits. This should include the review of procedures and data (including raw data and metadata, paper records, electronic data, audit trails and other related data) held by the relevant contract accepter identified in risk assessment.
应在定期的现场审计中确认其对原则和职责的符合性。这应包括对风险评估中确定的相关受托方保存的程序和数据(包括原始数据和元数据、纸质记录、电子数据、审计追踪和其他相关数据)的审查。

7.3. Where data and document retention are contracted to a third party, particular attention should be given to security, transfer, storage, access and restoration of data held under that agreement, as well as controls to ensure the integrity of data over their life cycle. This includes static data and dynamic data. Mechanisms, procedures and tools should be identified to ensure data integrity and data confidentiality, for example, version control, access control, and encryption.
如果数据和文件由第三方保存，应特别注意根据委托保存的数据的安全、转移、存储、访问和恢复，以及确保数据在其生命周期内的完整性的控制。这包括静态数据和动态数据。应该确定机制、程序和工具，以确保数据完整性和数据保密性，例如版本控制、访问控制和加密。

7.4. GxP activities, including outsourcing of data management, should not be sub-contracted to a third party without the prior approval of the contract giver. This should be stated in the contractual agreements.
GxP 活动，包括数据管理外包，未经委托方事先批准，不得再分包给第三方。这应该在委托协议中说明。

7.5. All contracted parties should be aware of the requirements relating to data governance, data integrity and data management.
所有受托方都应该了解与数据治理、数据完整性和数据管理相关的要求。

8. Training
培训

8.1. All personnel who interact with GxP data and who perform GxP activities should be trained in relevant data integrity principles and abide by organization policies and procedures. This should include understanding the potential consequences in cases of non-compliance.
所有接触 GxP 数据和执行 GxP 活动的人员都应接受相关数据完整性原则的培训，并遵循组织政策和程序。这应包括对不遵循情况下潜在后果的理解。

8.2. Personnel should be trained in good documentation practices and measures to prevent and detect data integrity issues.
人员应接受良好文件记录规范，以及预防和检测数据完整性问题的措施的培训。

8.3. Specific training should be given in cases where computerized systems are used in the generation, processing, interpretation and reporting of data and where risk assessment has

shown that this is required to relevant personnel. Such training should include validation of computerized systems and for example, system security assessment, back-up, restoration, disaster recovery, change and configuration management, and reviewing of electronic data and metadata, such as audit trails and logs, for each GxP computerized systems used in the generation, processing and reporting of data.
当计算机化系统用于数据的产生、处理、解释和报告，并且风险评估表明有关人员需要这样做时，应提供具体的培训。此类培训应包括计算机化系统的验证，例如，系统安全评估、备份、恢复、灾难恢复、变更和配置管理，以及对用于数据生成、处理和报告的每个 GxP 计算机化系统的电子数据和元数据的审查，如审计追踪和日志。

9. Data, data transfer and data processing
数据，数据转移和数据处理

9.1. Data may be recorded on paper or captured electronically by using equipment and instruments including those linked to computerised systems. A combination of paper and electronic formats may also be used, referred to as a “hybrid system”.
数据可以记录于纸张，也可以通过使用设备和仪器(包括与计算机化系统相连的设备和仪器)进行电子采集。纸张和电子格式的结合也可以使用，称为“混合系统”。

9.2. Data integrity consideration are also applicable to media such as photographs, videos, DVDs, imagery and thin layer chromatography plates. There should be a documented rationale for the selection of such a method.
数据完整性考虑也适用于媒介，如照片，视频，DVD，图像和薄层色谱板。选择这样一种方法应该有一个文件化的基本说明。

9.3. Risk-reducing measures such as scribes, second person oversight, verification and checks should be implemented where there is difficulty in accurately and contemporaneously recording data related to critical process parameters or critical quality attributes.
当关键工艺参数或关键质量属性相关数据难以准确同时记录时，应采取抄写、第二人监督、确认和检查等降低风险的措施。

9.4. Results and data sets require independent verification if deemed necessary from the DIRA or by another requirement.
当 DIRA 或其他要求认为有必要时，结果和数据集需要独立的确认。

9.5. Programmes and methods (such as processing methods in sample analysis (see also Good Chromatography Practices, TRS 1025) should ensure that data meet ALCOA+ principles. Where results or data are processed using a different method/parameters, then each version of the processing method should be recorded. Data records, content versions together with audit trails containing the required details should allow for reconstruction of all data processing in GxP computerized systems over the data life cycle.
程序和方法(如样品分析中的处理方法(参见 TRS 1025《良好色谱规范》))应确保数据符合 ALCOA+原则。如果使用不同的方法/参数对结果或数据进行处理，应记录处理方法的每个版本。数据记录、内容版本以及包含所需细节的审计追踪应允许在数据生命周期内重建 GxP 计算机化系统的所有数据处理。

9.6. Data transfer/migration procedures should include a rationale and be robustly designed and validated to ensure that data integrity is maintained during the data life cycle. Careful consideration should be given to understanding the data format and the potential for

alteration at each stage of data generation, transfer and subsequent storage. The challenges of migrating data are often underestimated, particularly regarding maintaining the full meaning of the migrated records.
数据传输/迁移过程应包括基本说明，并经过可靠的设计和验证，以确保数据完整性在数据生命周期中得到维护。在数据生成、传输和随后存储的每个阶段，应仔细考虑了解数据格式和可能发生的更改。迁移数据的挑战常常被低估，特别是在维护所迁移记录的完整含义方面。

Data transfer should be validated. The data should not be altered during or after it is transferred to the worksheet or other application. There should be an audit trail for this process. The appropriate quality procedures should be followed if the data transfer during the operation has not occurred correctly. Any changes in the middle layer software should be managed through the appropriate Quality Management Systems (7).
数据传输应被验证。数据在转移到工作表或其他应用程序期间或之后不应被更改。此过程应有一个审计追踪。如果操作过程中的数据传输没有正确进行，应遵循适当的质量程序。中间层软件中的任何变更都应该通过适当的质量管理体系进行管理(7)。

注释：中间层一般指用户接口与数据库之间的逻辑层

10. Good documentation practices
良好文件记录规范

Note: The principles contained in this section are applicable to paper data.
注:本节所载原则适用于纸质数据。

10.1. Good documentation practices should be implemented and enforced to ensure compliance with ALCOA+ principles.
应实施和执行良好文件记录规范以确保符合 ALCOA+原则。

10.2. Data and recorded media should be durable. Ink should be indelible. Temperature-sensitive or photosensitive inks and other erasable inks should not be used. Where related risks are identified, means should be identified in order to ensure traceability of the data over their life cycle.
数据和记录的媒体应持久。墨水应不得褪色。不应使用温度敏感或光敏油墨和其他可擦除油墨。如确定相关风险，应确定措施以确保数据在其生命周期内的可追溯性。

10.3. Paper should not be temperature-sensitive, photosensitive or easily oxidizable. If this is not feasible or limited, then true or certified copies should be generated.
纸张不应是温敏的、光敏的或易氧化的。如不可避免，则应生成真实或经认证的副本。

10.4. Specific controls should be implemented in order to ensure the integrity of raw data and results recorded on paper records. These may include, but are not limited to:
应实施特定的控制，以确保记录在纸张上的原始数据和结果的完整性。这些可能包括但不限于:

- control over the issuance and use of loose paper sheets at the time of recording data;
- 对于散装纸张，在记录数据时，对其发放和使用进行控制;

- no use of pencil or erasers;
- 不使用铅笔或橡皮擦;
- use of single-line cross-outs to record changes with the identifiable person who made the change, date and reason for the change recorded (i.e. the paper equivalent to an electronic audit trail);
- 使用单行划线，以记录作出的更改、更改人员、更改日期及更改的原因(即该纸张可相当于电子审计追踪);
- no use of correction fluid or otherwise, obscuring the original record;
- 不使用修正液或其他方法掩盖原始记录;
- controlled issuance of bound, paginated notebooks;
- 对于装订、分页的记录本，受控的发放;
- controlled issuance and reconciliation of sequentially numbered copies of blank forms with authenticity controls;
- 空白表格复印件按顺序编号的受控发放和平衡，并对真实性进行控制;
- maintaining a signature and initial record for traceability and defining the levels of signature of a record; and
- 维护签名和缩写的记录，以便可追溯性，并规定记录的签名级别;和
- archival of records by designated personnel in secure and controlled archives.
- 记录归档由指定人员保存在安全的、受控的资料室中。

11. Computerized systems
计算机化系统

(Note. This section highlights some specific aspects relating to the use of computerized systems. It is not intended to repeat the information presented in the other WHO guidelines here, such as the WHO Guideline on computerized systems (3), WHO Guideline on validation (2) and WHO Guideline on good chromatography practices (7). See references.)
注：本节重点介绍与计算机化系统使用有关的一些具体方面。此处不会重复其他 WHO 指南中的信息，例如 WHO 计算机化系统指南(3)，WHO 验证指南(2)和 WHO 良好色谱规范(7)。参见参考文献。

11.1. Each computerized system selected should be suitable, validated for its intended use, and maintained in a validated state.
选择的每个计算机化系统都应合适，并验证其符合预期用途，和维持在验证状态。

11.2. Where GxP systems are used to acquire, record, transfer, store or process data, management should have appropriate knowledge of the risks that the system and users may pose to the integrity of the data.
当 GxP 系统用于获取、记录、传输、存储或处理数据时，管理层应适当了解系统和用户可能对数据完整性构成的风险。

11.3. Software of computerized systems, used with GxP instruments and equipment, should be appropriately configured (where required) and validated. The validation should address for example the design, implementation and maintenance of controls in order to ensure the integrity of manually and automatically acquired data; ensure that Good Documentation Practices will be implemented; and that data integrity risks will be appropriately managed throughout the data life cycle. The potential for unauthorized and adverse manipulation of data during the life cycle of the data should be mitigated and, where possible, eliminated.

与 GxP 仪器和设备一起使用的计算机化系统的软件应进行适当的配置(如需要)和验证。验证应涉及例如控制的设计、实现和维护，以确保手动和自动获取的数据的完整性;确保实施良好的文件记录规范;数据完整性风险在整个数据生命周期中得到适当的管理。在数据的生命周期内，应减少对数据未经授权或不良操纵的可能性，并在可能的情况下，消除这种可能性。

11.4. Where electronic instruments (e.g. certain pH meters, balances and thermometers) or systems with no configurable software and no electronic data retention are used, controls should be put in place to prevent the adverse manipulation of data and to prevent repeat testing to achieve the desired result.
当使用电子仪器(例如某些 pH 计、天平和温度计)或没有可配置软件和没有电子数据保存的系统时，应采取控制措施，以防止对数据的不利操纵，并防止为了达到合格结果而进行的重复测试。

11.5. Appropriate controls for the detection of lapses in data integrity principles should be in place. Technical controls should be used whenever possible but additional procedural or administrative controls should be implemented to manage aspects of computerised system control where technical controls are missing. For example, when stand-alone computerized systems with a user-configurable output are used, Fourier-transform infrared spectroscopy (FTIR) and UV spectrophotometers have user-configurable output or reports that cannot be controlled using technical controls. Other examples of non-technical detection and prevention mechanisms may include, but are not limited to, instrument usage logbooks and electronic audit trails.
应有适当的控制来检测违反数据完整性原则。在可能的情况下应采用技术性控制，但在缺少技术性控制的情况下，应实施额外的程序性或管理性控制，以管理计算机化系统控制的各个方面。例如，当使用用户可配置输出的单机版计算机化系统时，傅里叶变换红外光谱(FTIR)和紫外分光光度计的输出或报告是用户可配置的，无法使用技术性控制。非技术性检测和预防机制的其他例子可能包括，但不限于，仪器使用日志和电子审计追踪。

Access and privileges
访问和权限

11.6. There should be a documented system in place that defines the access and privileges of users of systems. There should be no discrepancy between paper records and electronic records where paper systems are used to request changes for the creation and inactivation of users. Inactivated users should be retained in the system. A list of active and inactivated users should be maintained throughout the system life cycle.
应该有一个文件化的系统来定义系统用户的访问和权限。当使用纸质系统申请用户创建和停用时，纸质记录和电子记录之间不应存在差异。停用的用户应在系统中保留。应在整个系统生命周期中维护活动用户和非活动用户的列表。

11.7. Access and privileges should be in accordance with the role and responsibility of the individual with the appropriate controls to ensure data integrity (e.g. no modification, deletion or creation of data outside the defined privilege and in accordance with the authorized procedures defining review and approval where appropriate).

访问和权限应与人员的角色和责任相一致，并进行适当的控制以确保数据完整性(例如，不得在规定权限之外修改、删除或创建数据，并在适当情况下按照已批准程序审查和批准)。

11.8. A limited number of personnel, with no conflict of interest in data, should be appointed as system administrators. Certain privileges such as data deletion, database amendment or system configuration changes should not be assigned to administrators without justification – and such activities should only be done with documented evidence of authorization by another responsible person. Records should be maintained and audit trails should be enabled in order to track activities of system administrators. As a minimum, activity logging for such accounts and the review of logs by designated roles should be conducted in order to ensure appropriate oversight.
应该一定数量且在数据上没有利益冲突的人员作为系统管理员。某些权限，如数据删除、数据库修改或系统配置更改，不应该在没有正当理由的情况下分配给管理员，且此类活动应在另一个负责人批准的书面证明下进行。为了跟踪系统管理员的活动，应该保持记录并启用审计追踪。至少，应有这些帐户的活动日志并指定角色审查该日志，以确保适当的监督。

11.9. For systems generating, amending or storing GxP data, shared logins or generic user access should not be used. The computerised system design should support individual user access. Where a computerised system supports only a single user login or limited numbers of user logins and no suitable alternative computerised system is available, equivalent control should be provided by third-party software or a paper-based method that provides traceability (with version control). The suitability of alternative systems should be justified and documented (8). The use of legacy hybrid systems should be discouraged and a priority timeline for replacement should be established.
对于产生、修改或存储 GxP 数据的系统，不应使用共享登录或通用用户。计算机化系统设计应支持个人用户访问。如果计算机化系统只支持单个用户登录或有限数量的用户登录，且没有合适的替代计算机化系统，应由第三方软件或提供可追溯性(通过版本控制)的纸质方法提供相应的控制。替代系统的适用性应被证明并记录(8)。不建议使用遗留混合系统，并应建立更换的优先时间表。

Audit trail
审计追踪

11.10. GxP systems should provide for the retention of audit trails. Audit trails should reflect, for example, users, dates, times, original data and results, changes and reasons for changes (when required to be recorded), and enabling and disenabling of audit trails.
GxP 系统应保存审计追踪。审计追踪应该反映，例如，用户、日期、时间、原始数据和结果、更改和更改的原因(当需要记录时)，以及启用和禁用审计跟踪。

11.11. All GxP relevant audit trails should be enabled when software is installed and remain enabled at all times. There should be evidence of enabling the audit trail. There should be periodic verification to ensure that the audit trail remains enabled throughout the data life cycle.
所有 GxP 相关的审计追踪应该在软件安装时启用，并始终保持激活。应有启用审计追踪的证据。应定期进行确认，以确保审计追踪在整个数据生命周期中保持启用状态。

11.12. Where a system cannot support ALCOA+ principles by design (e.g. legacy systems with no audit trail), mitigation measures should be taken for defined temporary periods. For example, add-on software or paper-based controls may be used. The suitability of alternative systems should be justified and documented. This should be addressed within defined timelines.
如果一个系统不能从设计上支持 ALCOA+原则(例如没有审计追踪的遗留系统)，应在规定的临时期间采取补救措施。例如，可以使用附加软件或基于纸张的控制。替代系统的适用性应该进行论证并记录。应该在规定的时间内解决此问题。

Electronic signatures
电子签名

11.13. Each electronic signature should be appropriately controlled by, for example, senior management. An electronic signature should be:
每个电子签名都应该被适当的控制，例如，高级管理人员。电子签名应包括:

- attributable to an individual;
- 可归属至个人
- free from alteration and manipulation
- 不受更改和操纵
- be permanently linked to their respective record; and
- 与其记录永久关联;和
- date- and time-stamped.
- 日期和时间戳

11.14. An inserted image of a signature or a footnote indicating that the document has been electronically signed is not adequate unless it was created as part of the validated electronic signature process. The metadata associated with the signature should be retained.
插入签名图片或说明文件已签名的脚注是不充分的，除非它是作为已验证的电子签名过程的一部分产生的。应该保留与签名相关联的元数据。

Data backup, retention and restoration
数据备份，保存和恢复

11.15. Data should be retained (archived) in accordance with written policies and procedures, and in such a manner that they are protected, enduring, readily retrievable and remain readable throughout the records retention period. True copies of original records may be retained in place of the original record, where justified. Electronic data should be backed up according to written procedures.
数据应按照书面政策和程序保存(存档)，并在记录保存期间确保保护，持久，易于检索和保持可读。如经论证，可以保留原记录的真实副本代替原记录。电子数据应按书面程序备份。

11.16. Data and records, including backup data, should be kept under conditions which provide appropriate protection from deterioration. Access to such storage areas should be controlled and should be accessible only by authorized personnel.

数据和记录，包括备份数据，应保存在适当的保护条件下，以免恶化。进入这些储存区域应受控，并只有经授权的人员才能进入。

11.17. Data retention periods should be defined in authorized procedures.
数据保存期限应在经授权的程序中加以规定。

11.18. The decision for and manner in which data and records are destroyed, should be described in written procedures. Records for the destruction should be maintained.
应在书面程序中描述数据和记录被销毁的决定和方式。销毁记录应予以保存。

11.19. Backup and restoration processes should be validated. The backup should be done routinely and periodically be restored and verified for completeness and accuracy of data and metadata. Where any discrepancies are identified, they should be investigated and appropriate action taken.
应该对备份和恢复过程进行验证。应定期进行备份，并定期恢复，并确认数据和元数据的完整性和准确性。当发现任何差异时，应进行调查并采取适当的行动。

12. Data review and approval
数据审核和批准

12.2. There should be a documented procedure for the routine and periodic review, as well as the approval of data. Personnel with appropriate knowledge and experience should be responsible for reviewing and checking data. They should have access to original electronic data and metadata.
应有书面程序对数据进行日常和定期审查，以及批准。应由具有相应知识和经验的人员负责审核数据。他们应能够访问原始电子数据和元数据。

12.3. The routine review of GxP data and meta data should include audit trails. Factors such as criticality of the system (high impact versus low impact) and category of audit trail information (e.g. batch specific, administrative, system activities, and so on) should be considered when determining the frequency of the audit trail review.
GxP 数据和元数据的日常审核应包括审计追踪。当确定审计追踪审核的频率时，应该考虑诸如系统的关键性(高影响 VS 低影响)和审计追踪信息的类别(例如批次层次，管理层次，系统活动，等等)等因素。

12.4. A procedure should describe the actions to be taken where errors, discrepancies or omissions are identified in order to ensure that the appropriate corrective and preventive actions are taken.
程序应描述发现错误、差异或遗漏时应采取的措施，以确保采取适当的纠正和预防措施。

12.5. Evidence of the review should be maintained.
应保存审核的证据。

12.6. A conclusion, where required, following the review of original data, metadata and audit trail records should be documented, signed and dated.
需要时，在审核原始数据、元数据和审计追踪记录后，应记录结论，并签名和注明日期。

13. Corrective and preventive actions
纠正和预防措施

13.1. Where organizations use computerized systems (e.g. for GxP data acquisition, processing, interpretation, reporting) which do not meet current GxP requirements, an action plan towards upgrading such systems should be documented and implemented in order to ensure compliance with current GxP.
当组织使用的计算机化系统(例如用于 GxP 数据获取、处理、解释、报告)不符合现行 GxP 要求时，应制定并实施升级此类系统的行动计划，以确保符合现行的 GxP 要求。

13.2. When lapses in GxP relevant data regarding data integrity are identified, a risk-based approach may be used to determine the scope of the investigation, root cause, impact and CAPA, as appropriate. Health authorities, contract givers and other relevant organizations should be notified if the investigation identifies a significant impact or risk to, for example, materials, products, patients, reported information or data in application dossiers, and clinical trials.
当发现 GxP 相关数据的数据完整性方面的缺陷时，可以使用基于风险的方法来确定调查的范围、根本原因、影响和 CAPA(视情况而定)。如果调查发现对物料、产品、患者、申报资料中报告的信息或数据以及临床试验等产生重大影响或风险，应通知卫生当局、委托方和其他相关组织。

References
参考文献

Guidelines on good manufacturing practices for pharmaceutical products: main principle. In:

WHO Expert Committee on Specifications for Pharmaceutical Preparations: forty-eighth report.

Geneva: World Health Organization; 2013: Annex 2 (WHO Technical Report Series, No. 986; https:// www.who.int/medicines/areas/quality_safety/quality_assurance/TRS986annex2.pdf?ua=1, accessed 4 May 2020).
Good manufacturing practices: guidelines on validation. In: WHO Expert Committee on

Specifications for Pharmaceutical Preparations; fifty-third report. Geneva: World Health

Organization; 2019: Annex 3 (WHO Technical Report Series, No. 1019; http://digicollection.org/ whoqapharm/documents/s23430en/s23430en.pdf, accessed 5 May 2020).
Good manufacturing practices: guidelines on validation. Appendix 5. Validation of computerized

systems. In: WHO Expert Committee on Specifications for Pharmaceutical Preparations: fifty-third

report. Geneva: World Health Organization; 2019: Annex 3 (WHO Technical Report Series, No. 1019;
https://www.who.int/medicines/areas/quality_safety/quality_assurance/WHO_TRS_1019_Annex3.pdf?ua=1, accessed 4 May 2020).
Guidelines on quality risk management. In: WHO Expert Committee on Specifications for

Pharmaceutical Preparations: forty-seventh report. Geneva: World Health Organization; 2013: Annex 2 (WHO Technical Report Series, No. 981;
https://www.who.int/medicines/areas/quality_ safety/quality_assurance/Annex2TRS-981.pdf, accessed 4 May 2020).
ICH harmonised tripartite guideline. Quality risk management Q9. Geneva: International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceutical for Human Use; 2005 (https://database.ich.org/sites/default/files/Q9%20Guideline.pdf, accessed 12 June 2020).

Good chromatography practices. In: WHO Expert Committee on Specifications for Pharmaceutical

Preparations: fifty-fourth report. Geneva: World Health Organization; 2020: Annex 4 (WHO Technical Report Series, No. 1025; https://www.who.int/publications/i/item/978-92-4-000182-4, accessed 12 June 2020).

MHRA GxP data integrity guidance and definitions; Revision 1: Medicines & Healthcare Products Regulatory Agency (MHRA), London, March 2018
(https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/687246/MHRA_GxP_data_integrity_guide_March_edited_Final.pdf, accessed 12 June 2020).

Further reading
拓展阅读

■■ Data integrity and compliance with CGMP guidance for industry: questions and answers guidance for industry. U.S. Department of Health and Human Services, Food and Drug Administration; 2016 (https://www.fda.gov/files/drugs/published/Data-Integrity-and-Compliance-With-Current-Good-Manufacturing-Practice-Guidance-for-Industry.pdf, accessed 15 June 2020).
■■ Good Practices for data management and integrity in regulated GMP/GDP environments. Pharmaceutical Inspection Convention and Pharmaceutical Inspection Co-operation Scheme (PIC/S), November 2018
(https://picscheme.org/layout/document.php?id=1567, accessed 15 June 2020).

■■ Baseline guide Vol 7: risk-based manufacture of pharma products; 2nd edition.

■■ ISPE Baseline® Guide, July 2017. ISPEGAMP® guide: records and data integrity; March 2017.

■■ Data integrity management system for pharmaceutical laboratories PDA Technical Report, No. 80; August 2018.

■■ ICH harmonised tripartite guideline. Pharmaceutical Quality System Q10. Geneva: International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceutical for Human Use; 2008 (https://database.ich.org/sites/default/files/Q10%20Guideline.pdf, accessed 2 October 2020).

Appendix 1
附录 1

Examples in data integrity management
数据完整性管理示例

This Appendix reflects on some examples in data integrity management in order to support the main text on data integrity. It should be noted that these are examples and are intended for the purpose of clarification only.
本附录反映了一些数据完整性管理的例子，以支持关于数据完整性的正文。应该指出的是，这些示例仅用于说明。

Example 1: Quality risk management and data integrity risk assessment
示例 1:质量风险管理和数据完整性风险评估

Risk management is an important part of good practices (GxP). Risks should be identified and assessed and controls identified and implemented in order to assist manufacturers in preventing possible DI lapses.
风险管理是良好规范(GxP)的重要组成部分。应识别和评估风险，确定和实施控制措施，以帮助制造商防止可能的 DI 失效。

As an example, a Failure Mode and Effects Analysis (FMEA) model (or any other tool) can be used to identify and assess the risks relating to any system where data are, for example, acquired, processed, recorded, saved and archived. The risk assessment can be done as a prospective exercise or retrospective exercise. Corrective and preventive action (CAPA) should be identified, implemented and assessed for its effectiveness.
例如，失效模式和影响分析(FMEA)模型(或任何其他工具)可以用于识别和评估与数据获取、处理、记录、保存和归档等任何系统相关的风险。风险评估可以作为前瞻性工作或回顾性工作。应确定和实施纠正和预防措施(CAPA)并对其有效性进行评估。

For example, if during the weighing of a sample, the entry of the date was not contemporaneously recorded on the worksheet but the date is available on the print-out from a weighing balance and log book for the balance for that particular activity. The fact that the date was not recorded on the worksheet may be considered a lapse in data integrity expectations. When assessing the risk relating to the lack of the date in the data, the risk may be considered different (lower) in this case as opposed to a situation when there is no other means of traceability for the activity (e.g. no print-out from the balance). When assessing the risk relating to the lapse in data integrity, the severity could be classified as “low” (the data is available on the print-out); it does not happen on a regular basis (occurrence is “low”), and it could easily be detected by the reviewer (detection is “high”) – therefore the overall risk factor may be considered low. The root cause as to why the record was not made in the analytical report at the time of weighing should still be identified and the appropriate action taken to prevent this from happening again.
例如，如果在样品称量期间，没有同时记录日期，但是日期可以从称量天平和日志中打印出来。未记录日期的事实可能被认为是数据完整性要求的失效。当评估与数据中缺少日期相关的风险时，这种情况下的风险与没有其他可追溯手段的情况(例如不能从天平中打印出来)相比是不同的（较低）。当评估与数据完整性缺失有关

的风险时，严重性可被归类为“低”(数据可在打印输出上获得);它也不是频繁发生(可能性“低”)，而且易于被审核人发现(可检测性“高”)——因此，总体风险因素可能被认为是低。在称量时没有在分析报告中记录的根本原因仍然应该被确定，并采取适当的措施来防止这种情况再次发生。

Example 2: Good documentation practices in data integrity
示例 2：数据完整性的良好文件记录规范

Documentation should be managed with care. These should be appropriately designed in order to assist in eliminating erroneous entries, manipulation and human error.
应小心地管理文件。应适当设计，以帮助消除错误的输入，操纵和人为错误。

Formats
格式

Design formats to enable personnel to record or enter the correct information contemporaneously. Provision should be made for entries such as, but not limited to, dates, times (start and finish time, where appropriate), signatures, initials, results, batch numbers and equipment identification numbers. When a computerized system is used, the system should prompt the personnel to make the entries at the appropriate step.
设计格式，使人员能够同时记录或输入正确的信息。应规定，例如，但不限于，日期、时间(适当时，开始和结束时间)、签名、首字母、结果、批号和设备编号的填写。当使用计算机化系统时，系统应在适当的步骤提示人员输入。

Blank sheets of paper
空白纸张

The use of blank sheets should not be encouraged. Where blank sheets are used (e.g. to supplement worksheets, laboratory notebooks and master production and control records), the appropriate controls have to be in place and may include, for example, a numbered set of blank sheets issued which are reconciled upon completion. Similarly, bound paginated notebooks, stamped or formally issued by designated personnel, allow for the detection of unofficial notebooks and any gaps in notebook pages. Authorization may include two or three signatures with dates, for example, “prepared by” or “entered by”, “reviewed by” and “approved by”.
不应鼓励使用空白纸张。当使用空白纸张时(例如，作为工作记录本，实验室记录本，主生产和控制记录的补充)，应有适当的控制，包括，例如，发放一套带有序号的空白纸张，并在完成时核对。同样，经指定人员盖章或正式发布的装订分页的记录本，可以发现非正式的记录本和记录本上的任何空白页。授权可包括两到三个签名，并注明日期，例如:“打印人”“记录人”“审核人”“批准人”。

Error in recording data
记录数据的错误

Care should be taken when entries of data and results (electronic and paper records) are made. Entries should be made in compliance with good documentation practices. Where incorrect information had been recorded, this may be corrected provided that the reason for the error is documented, the original entry remains readable and the correction is signed and dated.

在输入数据和结果(电子和纸张记录)时，应小心谨慎。应符合良好的文件记录规范。如果记录了不正确的信息，如记录了错误的原因，原始内容仍然可读，可以修改并签名，注明日期。

Example 3: Data entry
示例 3：数据填写

Data entry includes for example sample receiving registration, sample analysis result recording, logbook entries, registers, batch manufacturing record entries and information in case report forms. The recording of source data on paper records should be done using indelible ink, in a way that is complete, accurate, traceable, attributable and free from errors. Direct entry into electronic records should be done by responsible and appropriately trained individuals. Entries should be traceable to an individual (in electronic records, thus having an individual user access) and traceable to the date (and time, where relevant). Where appropriate, the entry should be verified by a second person or entered through technical means such as the scanning of bar-codes, where possible, for the intended use of these data. Additional controls may include the locking of critical data entries after the data are verified and a review of audit trails for critical data to detect if they have been altered. The manual entry of data from a paper record into a computerized system should be traceable to the paper records used which are kept as original data.
数据填写包括，例如样品接收登记、样品分析结果记录、日志填写、登记、批生产记录填写和个例报告信息表格等。纸质记录上的源数据应使用不褪色油墨，以完整、准确、可追溯、可归属、无错误的方式记录。电子记录的直接录入应由负责的、经适当培训的人员完成。数据的输入应可追溯至个人(电子记录，即有个人用户访问)，并可追溯至日期(和时间，如相关)。在适当的情况下，输入应由第二个人进行确认，或在可能的情况下通过扫描条形码等技术手段输入，以满足这些数据的预期用途。其他控制可能包括在数据经确认后锁定关键数据条目，并对关键数据的审计追踪进行审核，以检测它们是否被更改。从纸质记录手动输入到计算机化系统的数据应该可以追溯到作为原始数据保存的纸质记录。

Example 4: Dataset
示例 4：数据集

All data should be included in the dataset unless there is a documented, justifiable, scientific explanation and procedure for the exclusion of any result or data. Whenever out of specification or out of trend or atypical results are obtained, they should be investigated in accordance with written procedures. This includes investigating and determining CAPA for invalid runs, failures, repeats and other atypical data. The review of original electronic data should include checks of all locations where data may have been stored, including locations where voided, deleted, invalid or rejected data may have been stored. Data and metadata related to a particular test or product should be recorded together. The data should be appropriately stored in designated folders. The data should not be stored in other electronic folders or in other operating system logs. Electronic data should be archived in accordance with a standard operating procedure. It is important to ensure that associated metadata are archived with the relevant data set or securely traceable to the data set through relevant documentation. It should be possible to successfully retrieve all required data and metadata from the archives. The retrieval and verification should be done at defined intervals and in accordance with an authorized procedure.

所有数据都应该包括在数据集中，除非有一个书面的，合理的，科学的解释和程序来排除任何结果或数据。当发现 OOS 或 OOT 或异常结果时，应按照书面程序进行调查。这包括调查和确定无效运行、失败、重复和其他异常数据的 CAPA。对原始电子数据的审核应包括对所有可能存储数据的位置的检查，包括已丢弃、已删除、无效或拒绝的数据的可能存储的位置。与特定测试或产品相关的数据和元数据应该一起记录。数据应适当地存储在指定的文件夹中。数据不应存储在其他电子文件夹或其他操作系统日志中。电子数据应按照标准操作程序进行归档。应确保关联的元数据与相关数据集一起归档，或者通过相关文件安全地跟踪到数据集。应可以成功地从归档中检索所有所需的数据和元数据。应按照经批准的程序定期检索和确认。

Example 5: Legible and enduring
示例 5：清晰和持久

Data and metadata should be readable during the life cycle of the data. Electronic data are normally only legible/readable through the original software application that created it. In addition, there may be restrictions around the version of a software application that can read the data. When storing data electronically, ensure that any restrictions which may apply and the ability to read the electronic data are understood. Clarification from software vendors should be sought before performing any upgrade, or when switching to an alternative application, to ensure that data previously created will be readable.

Other risks include the fading of microfilm records, the decreasing readability of the coatings of optical media such as compact disks (CDs) and digital versatile/video disks (DVDs), and the fact that these media may become brittle.

Similarly, historical data stored on magnetic media will also become unreadable over time as a result of deterioration. Data and records should be stored in an appropriate manner, under the appropriate conditions.

Example 6: Attributable
示例 6：可归属

Data should be attributable, thus being traceable to an individual and where relevant, the measurement system. In paper records, this could be done through the use of initials, full handwritten signature or a controlled personal seal. In electronic records, this could be done through the use of unique user logons that link the user to actions that create, modify or delete data; or unique electronic signatures which can be either biometric or non-biometric. An audit trail should capture user identification (ID), date and time stamps and the electronic signature should be securely and permanently linked to the signed record.

Example 7: Contemporaneous
示例 7：同步

Personnel should record data and information at the time these are generated and acquired. For example, when a sample is weighed or prepared, the weight of the sample (date, time, name of the person, balance identification number) should be recorded at that time and not before or at a later stage. In the case of electronic data, these should be automatically date- and time-stamped. In case hybrid systems are to be used, including the use for an interim

period, the potential and criticality of system breaches should be covered in the assessment with documented mitigating controls in place. (The replacement of hybrid systems should be a priority with a documented CAPA plan.) The use of a scribe to record an activity on behalf of another operator should be considered only on an exceptional basis and should only take place where, for example, the act of recording places the product or activity at risk, such as, documenting line interventions by aseptic area operators. It needs to be clearly documented when a scribe has been applied.

“In these situations, the recording by the second person should be contemporaneous with the task being performed, and the records should identify both the person performing the task and the person completing the record. The person performing the task should countersign the record wherever possible, although it is accepted that this countersigning step will be retrospective. The process for supervisory (scribe) documentation completion should be described in an approved procedure that specifies the activities to which the process applies.” (Extract taken from the Medicines & Healthcare Products Regulatory Agency (MHRA) GxP data integrity guidance and definitions (10).)

A record of employees indicating, their name, signature, initials or other mark or seal used should be maintained to enable traceability and to uniquely identify them and the respective action.

Example 8: Changes
示例 8：变更

When changes are made to any GxP result or data, the change should be traceable to the person who made the change as well as the date, time and reason for the change. The original value should not be obscured. In electronic systems, this traceability should be documented via computer generated audit trails or in other metadata fields or system features that meet these requirements. Where an existing computerized system lacks computer-generated audit trails, personnel may use alternative means such as procedurally controlled use of log-books, change control, record version control or other combinations of paper and electronic records to meet GxP regulatory expectations for traceability to document the what, who, when and why of an action.

Example 9: Original
示例 9：原始

The first or source capture of data or information and all subsequent data required to fully reconstruct the conduct of the GxP activity should be available. In some cases, the electronic data (electronic chromatogram acquired through high-performance liquid chromatography (HPLC)) may be the first source of data and, in other cases, the recording of the temperature on a log sheet in a room – by reading the value on a data logger. This data should be reviewed according to the criticality and risk assessment.

Example 10: Controls
示例 10：控制措施

Based on the outcome of risk assessment which should cover all areas of data governance and data management, appropriate and effective controls should be identified and implemented in order to assure that all data, whether in paper records or electronic records,

will meet GxP requirements and ALCOA+ principles. Examples of controls may include, but are not limited to:

the qualification, calibration and maintenance of equipment, such as balances and pH meters, that generate printouts;
the validation of computerized systems that acquire, process, generate, maintain, distribute, store or archive electronic records;
review and auditing of activities to ensure that these comply with applicable GxP data integrity requirements;
the validation of systems and their interfaces to ensure that the integrity of data will remain while transferring between/among computerized systems;

evaluation to ensure that computerized systems remain in a validated state;
the validation of analytical procedures;

the validation of production processes;

a review of GxP records;

ensuring effective review and oversight of the Batch Release Systems and processes by using different oversight and review techniques to ensure that data have not changed since the original entry; and
the investigation of deviations, out of trend and out of specifications results.

Example 11: Accuracy

Points to consider for assuring accurate GxP records:

the entry of critical data into a computer by an authorized person (e.g. entry of a master processing formula) requires an additional check on the accuracy of the data entered manually. This check may be done by independent verification and release for use by a second authorized person or by validated electronic means. For example, to detect and manage risks associated with critical data, procedures would require verification by a second person;

validation and control over formulae for calculations including electronic data capture systems;

ensuring correct entries into the laboratory information management system (LIMS) such as fields for specification ranges;

other critical master data, as appropriate. Once verified, these critical data fields should normally be locked in order to prevent further modification and only be modified through a formal change control process;
the process of data transfer between systems should be validated;

the migration of data including planned testing, control and validation; and

when the activity is time-critical, printed records should display the date and time stamp.