PHARMACEUTICAL INSPECTION CONVENTION
PHARMACEUTICAL INSPECTION CO-OPERATION SCHEME
医薬品査察協定および医薬品査察共同スキーム

PI 041-1
1 July 2021

PIC/S GUIDANCE

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

規制された GMP/GDP 環境におけるデータマネジメントとインテグリティのためのグッドプラクティス

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

1. DOCUMENT HISTORY 文書履歴

Adoption by Committee of PI 041-1	1 June 2021
Entry into force of PI 041-1	1 July 2021

2. INTRODUCTION 前書き

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 参加当局は、GMP（Good Manufacturing Practice）および GDP（Good Distribution Practice）の原則への準拠レベルを判断するために、医薬品有効成分（API）および医薬品の製造業者および販売業者の査察を定期的に実施している。これらの査察は通常、オンサイトで実行されるが、証拠書類のリモートまたはオフサイト評価を通じて実行される場合がある。その場合、データのリモートレビュの限界を考慮する必要がある。

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.

これらの査察プロセスの有効性は、査察官に提供された証拠の信頼性、そして最終的には基礎となるデータのインテグリティによって決定される。査察官が提示された証拠と記録の正確性と完全性を判断し、完全に信頼できることは、査察プロセスにとって重要である。

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.

データマネジメントとは、データポリシー、ドキュメント、品質、セキュリティなど、データの処理中に実行されるすべてのアクティビティを指す。適切なデータマネジメントの実施は、製造業者によって生成および記録されるすべてのデータの品質に影響を与える。これらの実施は、データが帰属可能、判読可能、同時性があり、オリジナルで、正確性、完全性、一貫性、永続性があり、利用可能であることを保証する必要がある。本ドキュメントの主な焦点は GMP/GDP の期待に関連しているが、ここでの原則は、設定された

API および医薬品管理戦略と仕様に基づいて登録書類に含まれるデータなどの適切なデータマネジメントをより広い文脈でも検討する必要がある。

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.

適切なデータマネジメントの実践は、医薬品品質システムのすべての要素に適用され、ここでの原則は、電子システムと紙ベースのシステムによって生成されたデータに等しく適用される。

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.

データインテグリティは、「データが完全で、一貫性があり、正確で、信用でき、信頼性があり、データのこれらの特性がライフサイクル全体にわたって維持される度合」と定義される。これは、医薬品が必要な品質であることを保証する効果的な医薬品品質システムの基本的な要件である。不十分なデータインテグリティの実践と脆弱性は、記録と証拠の品質を損ない、最終的には医薬品の品質を損なう可能性がある。

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.

データマネジメントとインテグリティに関する実践の責任は、査察を受ける製造業者または販売業者にある。彼らには、潜在的な脆弱性についてデータマネジメントシステムを評価し、データのインテグリティが維持されることを保証するための優れたデータガバナンス実践を設計および実装するための措置を講じる完全な責任と義務がある。

[1] ‘GXP’ Data Integrity Guidance and Definitions, MHRA, March 2018

3. PURPOSE 目的

3.1

This document was written with the aim of:

本ドキュメントは、次の目的で作成された。

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.

適切なデータマネジメントおよび査察の実施に関連する GMP/GDP 要件の解釈において査察官にガイダンスを提供する。

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.

GMP と GDP の PIC/S ガイドで説明されているように、最新の業界慣行とグローバル化されたサプライチェーンのコンテキストで実装されるデータの既存の要件を有効、完全かつ信頼性の高いものにするリスクベースの制御戦略に関する統合された例示的なガイダンスを提供する 。

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.

GMP/GDP 査察の定期的な計画と実施への適切なデータマネジメント要素の効果的な実装を促進する。
GMP/GDP 査察を調和させ、データインテグリティに期待する査察の質を確保するためのツールを提供する。

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.

本ガイダンスは、補佐官のメモなどの査察リソースとともに、査察官が査察時間を最適に利用し、査察中にデータインテグリティ要素を最適に評価できるようにする必要がある。

3.3

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

---

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

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

management practices.

ここでのガイダンスは、適切なデータマネジメントの実践に関連するリスクベースの査察を計画する際に査察官を支援する必要がある。

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.

適切なデータマネジメントは、常に GMP/GDP の不可欠な部分と見なされてきた。したがって、本ガイドは、規制対象のエンティティに追加の規制負担を課すことを意図したものではなく、現在の業界データマネジメント慣行に関連する既存の GMP/GDP 要件の解釈に関するガイダンスを提供することを目的としている。

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.

データマネジメントとインテグリティの原則は、紙ベースのコンピュータ化されたハイブリッドシステムにも同様に適用され、新しい概念やテクノロジーの開発や採用を制限するものではない。ICH Q10 の原則に従って、本ガイドは継続的な改善を通じて革新的な技術の採用を促進する必要がある。

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.

「医薬品品質システム」という用語は、本ドキュメント全体で主に品質目標の管理と達成に使用される品質マネジメントシステムを示すために使用される。「医薬品品質システム」という用語は主に GMP 規制対象事業体によって使用されるが、本ガイダンスの目的上、GDP 規制対象事業体によって使用される「品質システム」という用語と互換性があると見なす必要がある。

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.

本ガイドは、法律の下で義務または強制力を持っていない。医薬品および医薬品有効成分（医薬品有効成

分）の製造業者および販売業者のデータインテグリティ要件に関する国内法の制限、またはそれに取って代わることを意図したものではない。データインテグリティの欠陥は、国内法または PIC/SGMP または GDP ガイダンスの関連する段落に言及する必要がある。

4. SCOPE 範囲

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.

ガイダンスは、製造（GMP）および流通（GDP）活動を実行するサイトのオンサイト査察に適用するように作成されている。本ガイドの原則は、製品ライフサイクル全体のすべての段階に適用される。本ガイドは、査察中に考慮すべき領域の非網羅的なリストとして考慮する必要がある。

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.

本ガイダンスは、製造（GMP）および流通（GDP）活動を実行するサイトのリモート（デスクトップ）査察にも適用されるが、これはデータガバナンスシステムの評価に限定される。通常、データの検証と手順への運用コンプライアンスの証拠には、オンサイト評価が必要である。

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.

本ドキュメントは上記の範囲で作成されているが、ここで説明する適切なデータマネジメントの実践に関する多くの原則は、規制対象の製薬およびヘルスケア業界の他の分野にも適用される。

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.

本ガイドは、フォレンジックの専門知識が必要となる可能性のある重大なデータインテグリティの脆弱性の発見後の特別査察（for-cause inspection）に関する特定のガイダンスを提供することを目的としていない。

5. DATA GOVERNANCE SYSTEM　データガバナンスシステム

5.1 What is data governance?　データガバナンスとは何か？

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.

データガバナンスは、データインテグリティを保証する取り決めの総体である。これらの取り決めにより、データは、生成、記録、処理、保持、取得、および使用されるプロセス、形式、またはテクノロジーに関係なく、データライフサイクル全体を通じて、帰属性、判読可能、同時性、オリジナル、正確性、完全性、一貫性、永続性、および利用可能な記録が保証される。「データガバナンスシステム」を実装するための法的要件はないかも知れないが、その確立により、製造業者は一貫した方法でデータインテグリティ・リスクマネジメント活動を定義、優先順位付け、および伝達することができる。データガバナンスシステムがない場合、データインテグリティ・システムが調整されていないことを示し、管理手段にギャップが生じる可能性がある。

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).

データライフサイクルとは、データがどのように生成、処理、報告、チェックされ、意思決定に使用され、保存され、保存期間の終了時に最終的に破棄されるかを指す。製品またはプロセスに関連するデータは、ライフサイクル内のさまざまな境界を越える可能性がある。これには、紙ベースのシステムとコンピュータ化されたシステム間、または異なる組織の境界間のデータ転送が含まれる場合がある。内部（例：生産、QC、QA 間）と外部（例：サービスプロバイダーまたは委託者と受諾者の間）の両方。

5.2　Data governance systems

5.2.1

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

データガバナンスシステムは、PIC/S GMP/GDP で説明されている医薬品品質システムに不可欠である必要がある。ライフサイクル全体でデータの所有権に対処し、情報の意図的および非意図的な変更の制御や情報

の削除など、データインテグリティの原則に準拠するために、プロセスとシステムの設計、運用、モニタリングを検討する必要がある。

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.

データガバナンスシステムは、適切に設計されたシステムの組み込み、特定の専門知識を組み合わせてテクノロジーとデータセキュリティ対策を使用し、データマネジメントとインテグリティが効果的に制御されることを保証する。規制対象のエンティティは、システム、運用、およびデータの重要性とリスクの複雑さに応じて、データガバナンスシステムの設計、開発、運用、およびモニタリングに適切なリソースが利用可能であり、適用されるようにするための措置を講じる必要がある。

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:

データガバナンスシステムは、品質リスクマネジメントの原則に見合ったデータライフサイクルの制御を保証する必要がある。これらのコントロールは次のとおりである。

- Organisational
  - procedures, e.g. instructions for completion of records and retention of completed records
  - training of staff and documented authorisation for data generation and approval;
  - data governance system design, considering how data is generated, recorded, processed, retained and used, and risks or vulnerabilities are controlled effectively;
  - routine (e.g. daily, batch- or activity-related) data verification;
  - periodic surveillance, e.g. self-inspection processes seek to verify the effectiveness of the data governance system; or
  - the use of personnel with expertise in data management and integrity, including expertise in data security measures.

•組織

- 手順、例： 記録の完成と完成した記録の保持に関する指示
- スタッフのトレーニングとデータ生成および承認のための文書化された承認
- データの生成、記録、処理、保持、使用方法、およびリスクや脆弱性の効果的な管理方法を考慮したデータガバナンスシステムの設計
- ルーチン（例：毎日、バッチ、またはアクティビティ関連）のデータ検証。
- 定期的な調査、例：自己点検プロセスは、データガバナンスシステムの有効性を検証しようとする。 または
- データセキュリティ対策の専門知識を含む、データマネジメントとインテグリティの専門知識を持

つ人材の使用。

- Technical
  - computerised system validation, qualification and control;
  - automation; or
  - the use of technologies that provide greater controls for data management and integrity.

- テクニカル
  - コンピュータ化されたシステムの検証、認定、および制御
  - 自動化; または
  - データマネジメントとインテグリティをより強力に制御するテクノロジーの使用。

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.

効果的なデータガバナンスシステムは、適切な組織文化と行動の組み合わせの必要性（セクション 6)、データの重要性、データリスク、データライフサイクルの理解など、効果的なデータガバナンス実施に対する上級管理職の理解とコミットメントを示す。また、失敗や改善の機会を報告する権限を確実に与える方法で、組織内のすべてのレベルの担当者に期待を伝える証拠が必要である。これにより、データを改ざん、変更、または削除するインセンティブが軽減される。

5.2.5

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

データガバナンスに関する組織の取り決めは、医薬品品質システム内で文書化され、定期的にレビュされる必要がある。

5.3 Risk management approach to data governance　データガバナンスへのリスクマネジメントアプローチ

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).

上級管理職は、ICH Q9 の原則を使用して、データインテグリティに対する潜在的なリスクを最小限に抑えるためのシステムと手順の実装、および残留リスクの特定に責任がある。契約提供者は、ベンダー保証プロ

グラムの一環として、契約受諾者のデータマネジメントポリシーと管理戦略のレビュを実行する必要がある。このようなレビュの頻度は、リスクマネジメントの原則を使用して、契約受諾者によって提供されるサービスの重要度に基づく必要がある（セクション 10 を参照)。

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.

データガバナンスに割り当てられる労力とリソースは、製品の品質に対するリスクに見合ったものである必要があり、他の品質のリソース要求ともバランスを取る必要がある。GMP/GDP 原則に従って規制されているすべての事業体（製造業者、分析研究所、輸入業者、卸売業者を含む）は、データ品質リスクに基づいて許容可能な管理された状態（state of control）を提供し、裏付けとなる根拠とともに文書化されたシステムを設計および運用する必要がある。

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.

望ましい管理された状態を達成するために長期的な対策が特定された場合、リスクを軽減するために暫定的な対策を実施し、有効性を監視する必要がある。暫定措置またはリスクの優先順位付けが必要な場合は、データインテグリティの残留リスクを上級管理職に伝達し、レビュを続ける必要がある。自動化およびコンピュータ化されたシステムから紙ベースのシステムに戻しても、データガバナンスの必要性がなくなるわけではない。このような逆行的アプローチは、管理上の負担とデータリスクを増大させ、3.5 項で言及されている継続的な改善イニシアチブを妨げる可能性がある。

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:

すべてのデータまたは処理ステップが、製品の品質と患者の安全にとって同じ重要性を持っているわけではない。リスクマネジメントを利用して、各データ/処理ステップの重要性を判断する必要がある。データガバナンスへの効果的なリスクマネジメントアプローチでは、以下を検討する。

- Data criticality (impact to decision making and product quality) and
- Data risk (opportunity for data alteration and deletion, and likelihood of detection / visibility of changes

by the manufacturer's routine review processes).

•データの重要性（意思決定と製品品質への影響）および
•データリスク（データの変更と削除の機会、および製造業者の定期的なレビュプロセスによる変更の検出/可視性の可能性）。

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.

この情報から、リスクに比例した管理措置を実施することができる。 リスクマネジメントアプローチに言及する本ガイダンスの以降のセクションでは、「リスク」をデータリスクとデータ重要度の概念の組み合わせとして言及する。

5.4 Data criticality　データの重要性

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:

データの影響を決定する重要性が異なる場合があり、データが決定に与える影響も異なる場合がある。 データの重要性に関して考慮すべき点は次のとおりである。

- Which decision does the data influence?

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

•データはどの決定に影響するか？

例：バッチリリースの決定を行う場合、重要な品質属性への準拠を決定するデータは、通常、倉庫の清掃記録よりも重要である。

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

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

•データが製品の品質や安全性に与える影響は何であるか？

例：経口錠剤の場合、API 試験データは、錠剤の不適合性データよりも、一般に製品の品質と安全性に大きな影響を与える。

5.5 Data risk　データリスク

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.

データインテグリティ要件はすべての GMP/GDP データに関連しているが、データの重要度の評価は、組織がデータガバナンスの取り組みに優先順位を付けるのに役立つ。 この優先順位付けの根拠は、品質リスクマネジメントの原則に従って文書化する必要がある。

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.

データリスク評価では、不本意な変更、削除、損失（偶発的またはセキュリティ障害による)、再作成または意図的な改ざんに対するデータの脆弱性、およびそのようなアクションの検出の可能性を考慮する必要がある。災害が発生した場合に、完全でタイムリーなデータ回復を保証することも考慮する必要がある。不正行為を防止し、可視性/検出可能性を高める制御対策は、リスク軽減アクションとして使用することができる。

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.

データ障害のリスクを高める要因の例として、オープンエンドおよび主観的な結果を伴う複雑なプロセスや矛盾したプロセスなどがある。 一貫性があり、明確に定義され、客観的なタスクを伴う単純なプロセスは、リスクの軽減につながる。

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:

リスク評価では、情報技術（IT）システムの機能や複雑さだけでなく、ビジネスプロセス（生産、QC など）に焦点を当て、データフローとデータの生成および処理方法を評価する必要がある。 考慮すべき要素は次のとおりである。

- process complexity (e.g. multi-stage processes, data transfer between processes or systems, complex data processing);
- methods of generating, processing, storing and archiving data and the ability to assure data quality and integrity;
- process consistency (e.g. biological production processes or analytical tests may exhibit a higher degree of variability compared to small molecule chemistry);
- degree of automation / human interaction;

- subjectivity of outcome / result (i.e. is the process open-ended vs well defined);
- 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
- inherent data integrity controls incorporated into the system or software.

•プロセスの複雑さ（例：多段階プロセス、プロセスまたはシステム間のデータ転送、複雑なデータ処理）。
•データを生成、処理、保存、アーカイブする方法、およびデータの品質とインテグリティを保証する機能。
•プロセスの一貫性（例えば、生物学的生産プロセスまたは分析試験は、小分子化学と比較してより高度な変動性を示す可能性がある）；
•自動化の程度/人間の相互作用;
•結果/結果の主観性（すなわち、プロセスはオープンエンドであるか、明確に定義されているか）。
•電子システムデータと手動で記録されたイベントとの比較結果（例：分析レポートと生データの取得時間の間の明らかな不一致）；および
•システムまたはソフトウェアに組み込まれた固有のインテグリティ制御。

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.

コンピュータ化されたシステムの場合、リスク評価プロセスでは IT システムとの手動インターフェースを考慮する必要がある。特に、ユーザがバリデートされたシステムからのデータの報告に影響を及ぼすことが可能で、システムバリデーションが本ドキュメントのセクション 9 に置いて概説されている基本要件に対応していない場合、コンピュータ化されたシステムバリデーションを単独で実行してもデータインテグリティのリスクが低くなることはない。人間の介入を許可しない、あるいは人間の介入を最小限に抑えるコンフィグレーション設定の、完全に自動化され、バリデートされたプロセスは、この設計によりデータインテグリティリスクを低減するため、望ましい方法である。技術的な理由で統合制御が不可能な場合は、適切な手順制御をインストールして検証する必要がある。

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.

批判的思考スキルは、コントロールおよびレビュ手順が望ましい結果を効果的に達成するかどうかを判断するために査察官によって使用されるべきである。データガバナンスの成熟度の指標は、アクションを優先す

る残留リスクの組織的な理解と受容である。データインテグリティ障害の「リスクがない」と考える組織は、データライフサイクルに内在するリスクを適切に評価していない可能性がある。したがって、データのライフサイクル、重要度、およびリスクを評価するアプローチを詳細に検討する必要がある。これは、査察中に調査できる潜在的な故障モードを示している可能性がある。

5.6 Data governance system review データガバナンスシステムのレビュー

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.

データインテグリティ管理手段の有効性は、自己点検（内部監査）またはその他の定期的なレビュプロセスの一環として定期的に評価する必要がある。 これにより、データライフサイクルのコントロールが意図したとおりに機能するようになる。

5.6.2

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:

定期的なデータ検証チェック（例：毎日、バッチまたはアクティビティ関連）に加えて、自己点検アクティビティは、以下を含む制御手段のより広範なレビュに拡張する必要がある。

• 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).

•患者の保護に関連した適切なデータマネジメントの実施についての担当者の理解の継続的なチェック、および問題の品質とオープンな報告に焦点を当てた作業環境の維持の確保（例、適切なデータマネジメントの原則と期待に関する継続的なトレーニングのレビュによる）。

• 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.

•生のエントリに対する報告されたデータ/結果の一貫性のレビュ。 これにより、定期的なデータ検証チェック（リスクに基づいて正当化される場合）に含まれないデータ、および/または以前に検証されたデータのサンプルをレビュし、定期的なプロセスの継続的な有効性を確保できる。

•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]

[4] An 'exception report' is a validated search tool that identifies and documents predetermined 'abnormal' data or actions, which requires

•GMP/GDP 活動に関連する情報が正確に報告するための、コンピュータ化されたシステムログ/監査証跡のリスクベースのサンプル。 これは、通常のコンピュータ化されたシステムデータが手動で、または検証済みの「例外レポート」によってレビュされる状況に関連している。

• A review of quality system metrics (i.e. trending) that may also be indicators of data governance effectiveness.

•データガバナンスの有効性の指標にもなり得る品質システムメトリック（すなわち、傾向）のレビュ。

5.6.3

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.

データガバナンスシステムの効果的なレビュは、企業の行動と組織的および技術的統制との相互作用の重要性に関する理解を示す。レビュの結果は上級管理職に伝達され、残留データのインテグリティリスクの評価に使用される必要がある。

---

further attention or investigation by the data reviewer.

6. ORGANISATIONAL INFLUENCES ON SUCCESSFUL DATA INTEGRITY MANAGEMENT　データインテグリティマネジメントの成功に対する組織の影響

6.1　General　一般事項

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.

行動が、(i) データの修正、削除、または改ざんするインセンティブ、および (ii) データインテグリティを確保するために設計された手続き型制御の有効性にどのように影響するかを理解することで、査察官に詳細に調査できるリスクの有用な指標を提供することができる。

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.

査察官は、組織行動に対する文化の影響に敏感であり、ガイダンスの本セクションで説明されている原則を適切な方法で適用する必要がある。効果的な「品質文化」とデータガバナンスは、場所によって実装が異なる場合がある。ただし、文化的アプローチがデータインテグリティの懸念につながっていることが明らかな場合、これらの懸念は、是正のために査察官によって組織に効果的かつ客観的に報告されるべきである。

6.1.3

Depending on culture, an organisation's control measures may be:

文化に応じて、組織のコントロールの手段は次のようになる。

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

•「オープン」(部下が挑戦できる組織であり、ビジネスにおいて体系的または個々の障害の完全な報告が期待される場合)
•「クローズド」(障害の報告や組織への挑戦が文化的に難しい場合)

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.

「オープン」な文化における優れたデータガバナンスは、医薬品品質システムを通じて問題を特定して報告する従業員のエンパワーメントによって促進される可能性がある。「クローズド」の文化では、望ましくない情報を伝達するという社会的障壁において、同等のレベルの管理を達成するために、監視および二次レビューにさらに重点を置く必要がある場合がある。この状況では、上級管理職への機密エスカレーションプロセスの可用性もより重要になる可能性があり、これらの取り決めは、報告が上級管理職によって積極的にサポートおよび奨励されていることを明確に示す必要がある。

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.

データインテグリティに関する経営陣の知識と理解の度合いは、組織のデータインテグリティ管理の成功に影響を与える可能性がある。経営陣はデータインテグリティの欠如を防ぎ、発生した場合にそれらを検出するための法的および道徳的義務（すなわち、義務と権限）を知る必要がある。経営陣は、紙とコンピュータ化された（ハイブリッドおよび電子両方）ワークフローのデータインテグリティリスクを十分に可視化して理解する必要がある。

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.

データインテグリティの欠如は、詐欺や改ざんに限定されない。意図的でない可能性があり、依然としてもリスクを引き起こす可能性がある。データの信頼性を損なう可能性はリスクであり、適切なコントロールを整備するために特定して理解する必要がある（セクション 5.3～5.5 を参照)。直接的なコントロールは通常、書面によるポリシーおよび手順の形式を取るが、従業員の行動に対する間接的な影響（過度の圧力、プロセス能力を超える生産性へのインセンティブ、データを危険にさらす機会、従業員の否定的な行動の合理化など）も理解し、対処する必要がある。

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.

データインテグリティの侵害は、いつでも、どの従業員によっても発生する可能性があるため、マネジメントは問題の検出に注意を払い、欠如の背後にある理由を理解する必要がある。見つかった場合に問

題の調査と是正措置および予防措置の実施を可能にするためである。

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.

データインテグリティの欠如は、患者の安全に直接影響を与え、組織とその製品に対する信頼を損なうなど、さまざまな利害関係者(患者、規制当局、顧客)に影響を与える結果をもたらす。これらの結果に対する従業員の認識と理解は、品質が優先される環境を促進するのに役立つ。

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.

経営陣は、データインテグリティ侵害を防止、検出、評価および修正するためのコントロールを確立し、それらの制御がデータインテグリティを保証するために意図したとおりに実行されていることを確認する必要がある。セクション 6.2 から 6.7 では、データインテグリティを成功させるために経営陣が取り組むべき重要な項目の概要を示している。

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.

上級経営陣は、適切な組織文化と行動の組み合わせの必要性（セクション 6)、データの重要性、データリスク、データライフサイクルの理解など、効果的なデータガバナンスの実践に対する適切なレベルの理解とコミットメントを持っている必要がある。また、失敗や改善の機会を報告する権限を確保し、組織内のすべてのレベルの人員に期待を伝えていることの証拠が必要である。これにより、データを改ざん、変更、または削除するインセンティブが低下する。

6.2 Policies related to organisational values, quality, staff conduct and ethics
組織の価値観、品質、スタッフの行動および倫理に関連するポリシー

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.

スタッフの行動、品質への取り組み、組織の価値観および倫理に対する適切な期待が、組織全体に明確に伝えられ、適切な品質文化の実施と維持をサポートするためのポリシーを利用できるようにする必要がある。ポリシーは、品質に関する経営陣の理念を反映する必要があり、すべての個人が患者の安全と製品の品質を確保する責任と責任を負う信頼の環境を開発することを目的として作成する必要がある。

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.

経営陣は、データ品質を確保する上での役割の重要性と、製品の品質を保証し、患者の安全を保護するための活動の影響を従業員に認識させる必要がある。

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.

ポリシーは、正直などの倫理的行動への期待を明確に定義する必要がある。 これは、すべての従業員に伝達され、十分に理解されている必要がある。コミュニケーションは、要件を知ることだけでなく、要件が確立された理由と要件を満たさなかった場合の結果にも限定されるべきではない。

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.

意図的なデータの改ざん、不正な変更、データの破壊、またはデータ品質を損なうその他の行為などの望ましくない行動には、迅速に対処する必要がある。望ましくない行動や態度の例は、企業のポリシーに文書化する必要がある。望ましくない動作に対処するアクションを文書化する必要がある。ただし、実行されたアクション（懲戒処分など）が、特定されたデータインテグリティの問題に対するその後の調査を妨げないように注意する必要がある。 例えば、厳しい報復は、他のスタッフが調査に価値のある情報を開示することを妨げる可能性がある。

6.2.5

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

データマネジメントとインテグリティの適正な実践に準拠した行動の表示は、積極的に奨励され、適切に認

識されるべきである。

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.

企業のポリシーと手順に裏付けられた機密エスカレーションプログラムが必要である。これにより、情報提供者/従業員に影響を与えることなく、ポリシー違反の可能性のある事例を上級経営陣に知らせることができる。上級経営陣によるポリシー違反の可能性を認識し、それらのケースに適した報告メカニズムを利用できるようにする必要がある。

6.2.7

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

可能な場合、経営陣は、デフォルトで企業のポリシーの意図と要件を維持する制御を備えたシステムを実装する必要がある。

6.3 Quality culture 品質文化

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.

経営陣は、透明性と開放性のある職場環境（すなわち、品質文化）の構築し、データの信頼性の問題の可能性を含め、障害や間違いを自由に伝え、是正措置と予防措置を講じることを目指すべきである。 組織の報告構造では、すべてのレベルの従業員間の情報フローを許可する必要がある。

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.

これは、経営陣、チームリーダー、品質担当者、およびデータの品質とインテグリティを保証するための品質文化の構築に貢献するすべての担当者によって一貫して示される価値観、信念、思考、および行動の集まりである。

6.3.3

Management can foster quality culture by: • Ensuring awareness and understanding of expectations (e.g. Code of Values and Ethics and Code of

Conduct),
- Leading by example, management should demonstrate the behaviours they expect to see,
- Being accountable for actions and decisions, particularly delegated activities,
- Staying continuously and actively involved in the operations of the business,
- Setting realistic expectations, considering the limitations that place pressures on employees,
- Allocating appropriate technical and personnel resources to meet operational requirements and expectations,
- Implementing fair and just consequences and rewards that promote good cultural attitudes towards ensuring data integrity, and
- Being aware of regulatory trends to apply "lessons learned" to the organisation

経営陣は次の方法で品質文化を育むことができる。
•期待の認識と理解を確保する（例：価値観と倫理の規範および行動規範）
•例を挙げて、経営陣は期待する行動を示す必要がある。
•行動と決定、特に委任された活動に責任を持つ、
•事業の運営に継続的かつ積極的に関与し続ける、
•従業員に圧力をかける制限を考慮し、現実的な期待を設定する、
•運用要件と期待に応えるために、適切な技術リソースと人的リソースを割り当てる。
•データインテグリティを確保するための優れた文化的態度を促進する、公正で公正な結果と報酬を実装し、および
•「教訓」を組織に適用するための規制の傾向を認識する

6.4 Modernising the Pharmaceutical Quality System　医薬品品質システムの近代化

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.

最新の品質リスクマネジメントの原則と適切なデータマネジメント手法を現在の医薬品品質システムに適用することで、複雑なデータの生成に伴う課題に対応するためにシステムを最新化することができる。

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:

企業の医薬品品質システムは、データインテグリティの欠如につながる可能性のあるシステムまたはそのプロセスの弱点を防止、検出、および修正できる必要がある。 企業は、データのライフサイクルを把握し、生成されたデータが有効で完全で信頼性が高くなるように、適切なコントロールと手順を統合する必要がある。 具体的には、このような管理および手順の変更は、次の領域に含まれる可能性がある。

- Quality Risk Management,
- Investigation programs,
- Data review practices (section 9),
- Computerised system validation,
- IT infrastructure, services and security (physical and virtual),
- Vendor/contractor management,
- Training program to include company's approach to data governance and data governance SOPs,
- Storage, processing, transfer and retrieval of completed records, including decentralised/cloud-based data storage, processing and transfer activities,
- 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)
- Self-inspection program to include data quality and integrity, and
- Performance indicators (quality metrics) and reporting to senior management.

•品質リスクマネジメント、
•調査プログラム、
•データレビュの実践（セクション 9)、
•コンピュータ化されたシステムのバリデーション
•IT インフラストラクチャ、サービス、およびセキュリティ（物理的および仮想的)、
•ベンダー/請負業者の管理、
•データガバナンスおよびデータガバナンス SOP に対する企業のアプローチを含めたトレーニングプログラム、
•分散型/クラウドベースのデータストレージ、処理および転送アクティビティを含む、完了した記録の保存、処理、転送、および取得、
•データインテグリティの期待に応えるように設計された要件を組み込んだ GMP/GDP 重要機器および IT インフラストラクチャの購入の適切な監視。ユーザ要件仕様（セクション 9.2 を参照）
•データの品質とインテグリティを含めるための自己点検プログラム、および
•パフォーマンス指標（品質指標）と上級経営陣への報告。

6.5 Regular management review of performance indicators (including quality metrics)
パフォーマンス指標（品質指標を含む）の定期的な管理レビュ

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.

重要な問題が特定され、エスカレーションされ、タイムリーに対処されるように、データインテグリティに関連するものを含め、パフォーマンス指標の定期的な管理レビュが必要である。主要業績評価指標（KPI）を選択するときは、データインテグリティの優先度を落とさないように注意する必要がある。

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.

品質部門の責任者は、リスクを直接伝達するために上級経営陣に直接アクセスできる必要がある。これにより、上級経営陣は問題を認識し、リソースを割り当てて問題に対処できる。

6.5.3

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

経営陣は、独立した専門家にシステムと制御の有効性を定期的に検証させることができる。

6.6 Resource allocation 資源の配分

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.

経営陣は、適切なリソースを割り当てて、適正なデータインテグリティ管理をサポートおよび維持する必要がある。これにより、データ生成と記録保持の責任者に対する作業負荷とプレッシャーによって、エラーの可能性やデータインテグリティを故意に損なう機会が増加しない。

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.

品質とマネジメントの監視、IT サポート、調査の実施、および組織の運営に見合ったトレーニングプログラムの管理のために十分な数の人員が必要である。

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.

問題のデータの重要性に基づいて、ニーズに適した機器、ソフトウェア、およびハードウェアを購入するための規定が必要である。 企業は、ALCOA +の原則への準拠を改善し、データの品質とインテグリティに関する弱点を軽減する技術ソリューションを実装する必要がある。

6.6.4

---

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

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.

担当者は、適切なドキュメントの実践（GdocP）の重要性を含め、職務を適切に分離して、特定の職務について資格を持ち、訓練を受ける必要がある。 電子データレビュなどの重要な手順に関するトレーニングの有効性の証拠が必要である。 適切なデータマネジメントの実施の概念は、IT やエンジニアリングなどの分野を含め、GMP/GDP で役割を果たすすべての部門に適用される。

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.

データ品質とインテグリティはすべての人に知られているはずだが、さまざまなレベルのデータ品質の専門家（SME、スーパーバイザー、チームリーダー）が協力して調査を実施/サポートし、システムギャップを特定し、改善の実装を推進するよう求められる場合がある。

6.6.6

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

データマネジメント者など、適切なデータマネジメントに関連する組織での新しい役割の導入が検討される可能性がある。

6.7 Dealing with data integrity issues found internally
内部で見つかったデータインテグリティの問題への対処

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.

データインテグリティの欠如が見つかった場合、逸脱は医薬品品質システムに従って行われるため、それらを処理する必要がある。 問題の範囲と根本原因を特定し、問題を完全に修正して予防策を講じることが重要である。 これには、システムの弱点を特定するためのギャップ評価を含む、追加の専門知識または視点のためのサードパーティの使用が含まれる場合がある。

6.7.2

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

患者の安全と製品の品質への影響を検討する場合、導き出された結論は、健全な科学的証拠によって裏付けられる必要がある。

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.

修正には、製品のリコール、クライアントへの通知、規制当局への報告が含まれる場合がある。 是正措置と是正措置計画およびそれらの実施を記録し、モニタリングする必要がある。

6.7.4

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

詳細なガイダンスは、本ガイドのセクション 12 に記載されている。

7. GENERAL DATA INTEGRITY PRINCIPLES AND ENABLERS 一般的なデータインテグリティの原則とイネーブラー

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.

医薬品品質システムは、API および医薬品のライフサイクルのさまざまな段階を通じて実装する必要があり、科学とリスクベースのアプローチの使用を奨励する必要がある。

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).

意思決定に十分な情報が提供されていることを確認し、情報が信頼できることを確認するには、それらの決定に情報を提供したイベントまたはアクションを十分に文書化する必要がある。 そのため、適正なドキュメンテーションプラクティスは、データインテグリティを確保するための鍵であり、適切に設計された医薬品品質システムの基本的な部分である（セクション 6 で説明)。

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 の適用は、データの記録に使用される媒体（すなわち、物理的記録と電子的記録）によって異なる場合があるが、原則は両方に適用できる。 本セクションでは、これらの主要な原則を紹介し、次のセクション（8 および 9）では、紙ベースと電子ベースの両方の記録管理における文書化に関連し、これらの原則について説明する。

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 の主要な概念の一部は、ALCOA の頭字語によって要約されている：帰属可能、判読可能、同時性、オリジナル、および正確性。 次の属性をリストに追加できる：完全性、一貫性、永続性。利用可能（ALCOA +)。これらの期待を合わせることにより、イベントが適切に文書化され、データを使用して情報に基づいた意思決定をサポートできるようになる。

---

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

7.5

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

紙と電子システムの両方に適用可能である基本的なデータインテグリティの原則（すなわち、ALCOA +）：

Data Integrity Attribute データインテグリティ属性	Requirement 要件
Attributable 帰属可能	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. 記録されたタスクを実行した個々のシステムまたはコンピュータ化されたシステム、およびタスクがいつ実行されたかを特定できる必要がある。 これは、修正、削除、変更など、記録に加えられた変更にも適用される。変更を実施したユーザ、時期、および理由を知ることが重要である。
Legible 判読可能	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, 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. すべての記録は判読可能である必要がある。情報が理解可能で使用できるようにするには、情報が読み取り可能で明確である必要がある。 これは、すべてのオリジナルの記録またはエントリを含め、完全であると見なされる必要があるすべての情報に適用される。 電子データの「動的」な性質（検索、照会、トレンドなど）が記録の内容と意味にとって重要である場合、適切なアプリケーションを使用してデータと対話する機能は、記録の「可用性」にとって重要である。
Contemporaneous 同時性	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. アクション、イベント、または決定の証拠は、発生時に記録する必要がある。この文書は、何が行われたか、何が決定されたか、そしてその理由、すなわちその時点での決定に影響を与えたものの正確な証明として役立つ必要がある。
Original オリジナル	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.

	元の記録は、紙に記録されているか（静的)、電子的に記録されているか（通常は動的で、システムの複雑さに応じる)、情報の最初のキャプチャとして説明できる。 元々動的な状態でキャプチャされた情報は、その状態で引き続き利用できる必要がある。
Accurate 正確性	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. 正確な情報を得るためには、記録が事実を真実に表現する必要がある。記録が正確であることを保証することは、堅牢な医薬品品質システムの多くの要素を通じて達成される。 これは、次のもので構成できる。 •認定、校正、メンテナンス、コンピュータバリデーションなどの機器関連の要素。 •手順要件の順守を検証するためのデータレビュ手順を含む、アクションと行動をコントロールするためのポリシーと手順 •根本原因分析、影響評価、CAPA を含む逸脱管理 •確立された手順に従い、行動と決定を文書化することの重要性を理解している、訓練を受けた資格のある人材。 これらの要素を組み合わせることで、製品の品質に関する重要な決定を行うために使用される科学データなど、情報の正確性を確保することを目的としている。
Complete 完全性	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). イベントを理解しようとするとき、イベントを再現するために重要となるすべ

	ての情報が重要である。 情報が失われたり削除されたりしないことが重要である。 情報セットが完全であると見なされるために必要な詳細レベルは、情報の重要度によって異なる（セクション 5.4 データの重要度を参照)。 電子的に生成されたデータの完全な記録には、関連するメタデータが含まれる（セクション 9 を参照)。
Consistent 一貫性	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.). 情報は、定義された一貫性を持つ論理的な方法で作成、処理、および保存する必要がある。 これには、データのコントロールまたは標準化に役立つポリシーまたは手順が含まれる（たとえば、時系列、日付形式、測定単位、四捨五入へのアプローチ、有効数字など)。
Enduring 永続性	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. 記録は、必要になる可能性のある全期間にわたって存在するような方法で保持する必要がある。 これは、記録の保持期間を通じて、それらが無傷であり、消えない/耐久性のある記録としてアクセス可能である必要があることを意味する。
Available 利用可能	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. 記録は、必要な保持期間中いつでもレビュできるようにし、定期的なリリースの決定、調査、傾向分析、年次報告書、監査、または査察のいずれの場合でも、レビュを担当するすべての該当する担当者が読み取り可能な形式でアクセスできるようにする必要がある。

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.

これらの要素が、医薬品品質システムの他のサポート要素とともに、GMP および GDP 関連活動のすべての該当する領域に適切に適用される場合、医薬品に関する重要な決定を行うために使用される情報の信頼性は適切に保証される。

7.7 True copies 真のコピー

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).

元の紙の記録のコピー（分析要約レポート、検証レポートなど）は、一般的に、異なる場所で事業を行っている企業間のコミュニケーションの目的で非常に有用である。これらの記録は、別のサイト(姉妹企業、請負業者など)から受信したデータが必要に応じて「真のコピー」として維持されるように、または「真のコピー」の要件が満たされない「要約レポート」として使用されるように、ライフサイクル中に制御する必要がある(例えば、複雑な分析データの要約)。

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.

電子的手段によって生成された生データは、許容可能な紙または pdf 形式で保持されることが考えられる。この場合、静的記録が元のデータのインテグリティを維持することが正当化される。 ただし、データ保持プロセスでは、医薬品の品質のあらゆる側面に直接的または間接的に影響を与えるすべてのアクティビティのすべてのデータ（メタデータを含む）を記録する必要がある（たとえば、分析の記録の場合、生データ、メタデータ、関連する監査証跡ファイルと結果ファイル、各分析実行に固有のソフトウェア/システム構成設定、および特定の生データセットの再構築に必要なすべてのデータ処理実行（メソッドと監査証跡を含む）が含まれる場合がある)。 また、印刷された記録が正確な表現であることを確認するための文書化された手段が必要になる。 このアプローチは、GMP/GDP 準拠の記録を有効にするために、その管理において面倒になる可能性がある。

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.

多くの電子記録は、データとの相互作用を可能にするために、動的な形式で保持することが重要である。 データは動的な形式で保持する必要がある。これは、データのインテグリティまたは後の検証にとって重要である。リスクマネジメントの原則を利用して、データを動的形式で保存するかどうか、および保存する期間をサポートおよび正当化する必要がある。

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.

受信サイトでは、これらの記録（真のコピー）は紙または電子形式（PDF など）で管理でき、承認された QA 手順に従って管理する必要がある。

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.

手書きまたは電子署名の使用、または真のコピーを作成するための検証済みのプロセスに従って生成するなど、ドキュメントの信頼性を容易に検証できるように、ドキュメントが「真のコピー」として適切に認証されるように注意する必要がある。

Item 項目	How should the “true copy” be issued and controlled? 「真のコピー」はどのように発行および管理する必要があるか？
1.	**Creating a “true copy” of a paper document.** **紙の文書の「真のコピー」を作成する。** At the company who issues the true copy: -Obtain the original of the document to be copied -Photocopy the original document ensuring that no information from the original copy is lost; -Verify the authenticity of the copied document and sign and date the new hardcopy as a “true copy”; 真のコピーを発行する企業で： -コピーするドキュメントの原本を入手する -元のドキュメントをコピーして、元のコピーの情報が失われないようにする。 -コピーされたドキュメントの信憑性を確認し、新しいハードコピーに「真のコピー」として署名して日付を記入する。 The “True Copy” may now be sent to the intended recipient. これで、「TrueCopy」が目的の受信者に送信される可能性がある。 **Creating a “true copy” of a electronic document.** **電子文書の「真のコピー」を作成する。** 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. 電子記録の「真のコピー」は、必要なすべてのメタデータを含む電子的手段（電子ファイルコピー）によって作成する必要がある。 メタデータが失われる可能性がある場合

	は、PDF バージョンの電子データを作成することは禁止する必要がある。 The “True Copy” may now be sent to the intended recipient. これで、「TrueCopy」が目的の受信者に送信される可能性がある。 A distribution list of all issued “true copies” (soft/hard) should be maintained. 発行されたすべての「真のコピー」（ソフト/ハード）の配布リストを維持する必要がある。
	Specific elements that should be checked when reviewing records: **記録を確認するときにチェックする必要がある特定の要素：** • Verify the procedure for the generation of true copies, and ensure that the generation method is controlled appropriately •真のコピーの生成手順を確認し、生成方法が適切に管理されていることを確認する • 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. •発行された真のコピーが元の記録と同一（完全かつ正確）であることを確認すること。コピーした記録を元のドキュメントの記録と照合し、スキャンした画像が改ざんされていないことを確認する必要がある。 • Check that scanned or saved records are protected to ensure data integrity. •スキャンまたは保存された記録が保護されていることを確認し、データインテグリティを確保する。 • After scanning paper records and verifying creation of a ‘true copy’: -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.

	-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. •紙の記録をスキャンし、「真のコピー」の作成を確認した後： -配信目的で真のコピーが生成される場合、たとえば、クライアントに送信される場合、配信目的で実際のコピーが生成される元のドキュメント、たとえばクライアントに送信される元のドキュメントは、スキャンされた画像が作成された元のドキュメントを記録所有者が保持する期間、保持する必要がある。 -ドキュメントの保持を支援するために真のコピーが生成される場合、スキャンされた画像が作成された元の記録ドキュメントの代わりにコピーを保持できる場合がある。
2.	At the company who receives the true copy: - The paper version, scanned copy or electronic file should be reviewed and filed according to good document management practices. 真のコピーを受け取る企業で： -紙のバージョン、スキャンしたコピー、または電子ファイルは、適切なドキュメント管理慣行に従ってレビュおよび提出する必要がある。 The document should clearly indicate that it is a true copy and not an original record. 文書は、それが真のコピーであり、元の記録ではないことを明確に示す必要がある。
	Specific elements that should be checked when reviewing records: **記録を確認するときにチェックする必要がある特定の要素：** •Check that received records are checked and retained appropriately. •A system should be in place to verify the authenticity of “true copies” e.g. through verification of the correct signatories. •受信した記録がチェックされ、適切に保持されていることを確認する。 •正しい署名者の検証を通じて、「真のコピー」の信憑性を検証するためのシステムを導入する必要がある。。

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.

「真のコピー」の生成と転送、およびデータインテグリティ管理の責任に対処するために、品質協定を締結する必要がある。 「真のコピー」の発行とコントロールのためのシステムは、プロセスが堅牢でデータインテグリティの原則を満たしていることを確認するために、契約の提供者と受信者によって監査される必要がある。

7.8 Limitations of remote review of summary reports 要約レポートのリモートレビュの制限

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.

要約レポート内のデータのリモートレビュは一般的な必要性である。 ただし、データインテグリティを適切にコントロールできるようにするには、リモートデータレビュの制限を十分に理解する必要がある。

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.

データの要約レポートは、多くの場合、物理的に離れた製造サイト、市場承認保有者、およびその他の利害関係者の間で提供される。 ただし、重要なサポートデータとメタデータが含まれていないことが多く、元のデータを確認できないという点で、要約レポートは本質的に限定的であることを認識しておく必要がある。

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.

したがって、要約報告書はデータ転送のプロセスの 1 つの要素にすぎないと見なされ、利害関係者および査察官が要約報告書データのみに依存しないことが不可欠である。

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.

要約データを受け入れる前に、サプライヤの品質システムの評価とデータインテグリティの原則への準拠を確立する必要がある。 デスクトップまたは同様の評価を使用してデータインテグリティの原則への準拠を判断することは、通常は受け入れられず、不可能である。

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.

外部エンティティの場合、これは、品質リスクマネジメントのコンテキストで重要であると見なされた場合、オンサイト監査を通じて決定する必要がある。 監査では、企業が生成したデータの信憑性を保証し、要約データとレポートを生成および配布するために使用されるメカニズムのレビュを含める必要がある。

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.).

要約データが同じ組織の異なるサイト間で配布される場合、供給サイトのコンプライアンスの評価は、代替手段（たとえば、企業手順へのコンプライアンスの証拠、内部監査レポートなど）によって決定される場合がある。

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.

要約データは、合意された手順に従って作成され、元のサイトの認定スタッフによってレビュおよび承認される必要がある。 要約には、要約の信憑性と正確性を示す、認可された人物が署名した宣言を添付する必要がある。 要約レポートの生成、転送、および検証の取り決めは、品質/技術的合意の範囲内で対処する必要がある。

8. SPECIFIC DATA INTEGRITY CONSIDERATIONS FOR PAPER- BASED SYSTEMS
紙ベースのシステムに関する特定のデータインテグリティに関する考慮事項

8.1 Structure of Pharmaceutical Quality System and control of blank forms/templates/records 医薬品品質システムの構造と空白のフォーム/テンプレート/記録の管理

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.

紙ベースのドキュメントの効果的な管理は、GMP/GDP の重要な要素である。 したがって、文書化システムは、GMP/GDP 要件を満たし、ドキュメントと記録がインテグリティを維持するために効果的に管理されるように設計する必要がある。

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.

紙の記録は管理されるべきであり、データのライフサイクル全体を通じて、帰属可能、判読可能、同時性、オリジナル、正確性、完全性、一貫性、永続性（消えない/耐久性がある）があり、利用可能（ALCOA +）である必要がある。

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:

適正な文書化実践とドキュメント管理の取り決めを概説する手順は、医薬品品質システム内で利用可能であ

る必要がある。 これらの手順では、次のようなデータのライフサイクル全体でデータインテグリティを維持する方法を指定する必要がある。

- creation, review, and approval of master documents and procedures;
- generation, distribution and control of templates used to record data (master, logs, etc.);
- retrieval and disaster recovery processes regarding records;
- 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;
- 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
- filing, retrieval, retention, archival and disposal of records.

•マスタードキュメントおよび手順の作成、レビュ、および承認。
•データ（マスター、ログなど）の記録に使用されるテンプレートの生成、配布、および制御。
•記録に関する検索および災害復旧プロセス。
•日常的に使用するためのドキュメントの作業コピーの生成。特に、ドキュメントのコピーの確保に重点を置いている。 SOP および空白のフォームは、コントロールされ追跡可能な方法で使用するために発行および調整される。
•紙ベースのドキュメントの完成、個々のオペレーターの識別方法、データ入力型式、記録の修正、および正確性、信頼性、完全性の定期的なレビュを指定する。および
•記録のファイリング、検索、保持、アーカイブ、および廃棄。

8.2 Importance of controlling records 記録を管理することの重要性

8.2.1

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

記録は GMP/GDP 運用にとって重要であるため、以下を確実に実施するためにコントロールが必要である。

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

•実行されたアクティビティの証拠。
•GMP/GDP 要件および企業のポリシー、手順、作業指示への準拠の証拠。

•医薬品品質システムの有効性。
•トレーサビリティ。
•プロセスの信頼性および一貫性。
•製造された医薬品の高品質属性の証拠。
•苦情またはリコールの場合、記録は調査目的で使用される可能性がある。および
•逸脱またはテストの失敗の場合、記録は効果的な調査を完了するために重要である。

8.3 Generation, distribution and control of template records テンプレート記録の生成、配布、および制御

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).

マスタードキュメントのマネジメントおよびコントロールは、誰かが「通常の手段」で記録を不適切に使用および/または改ざんするリスク（すなわち、専門家による不正スキルの使用を必要としない）を許容可能なレベルまで確実に低減するために必要である。記録されたデータのリスクと重要性を考慮し、品質リスクマネジメントアプローチを使用して、以下の期待を実装する必要がある（セクション 5.4、5.5 を参照）。

8.4 Expectations for the generation, distribution and control of records 記録の生成、配布、および制御に対する期待

Item 項目	Generation 生成
1.	**Expectation 期待** All documents should have a unique identifier (including the version number) and should be checked, approved, signed and dated. すべてのドキュメントには一意の識別子（バージョン番号を含む）が必要であり、チェック、承認、署名、および日付を付ける必要がある。 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. コントロールされていないドキュメントの使用は、ローカルの手続きにより禁止する必要がある。 紙のスクラップなど、一時的な記録慣行の使用は禁止する必要がある。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** • 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.

	• It might be easier to falsify uncontrolled records. • Use of temporary recording practices may lead to data omission, and these temporary original records are not specified for retention. • If records can be created and accessed without control, it is possible that the records may not have been recorded at the time the event occurred. • There is a risk of using superseded forms if there is no version control or controls for issuance. •コントロールされていないドキュメントは、追跡可能性なしに破棄または破壊される可能性があるため、重要なデータの欠落または損失の可能性を高める。 さらに、コントロールされていない記録は、重要なデータを正しく記録するように設計されていない可能性がある。 •コントロールされていない記録を改ざんする方が簡単な場合がある。 •一時的な記録方法を使用すると、データが欠落する可能性があり、これらの一時的な元の記録は保持対象として指定されていない。 •記録を作成して制御せずにアクセスできる場合は、記録はイベントの発生時に記録されていない可能性がある。 •バージョン管理または発行管理がない場合、置き換えられたフォームを使用するリスクがある。
2.	**Expectation　期待** The document design should provide sufficient space for manual data entries. ドキュメント設計では、手動でデータを入力するための十分なスペースを確保する必要がある。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** • Handwritten data may not be clear and legible if the spaces provided for data entry are not sufficiently sized. • Documents should be designed to provide sufficient space for comments, e.g. in case of a transcription error, there should be sufficient space for the operator to cross out, initial and date the error, and record any explanation required. • If additional pages of the documents are added to allow complete documentation, the number of, and reference to any pages added should be clearly documented on the main record page and signed. • 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. •データ入力用のスペースのサイズが十分でない場合、手書きデータは明確に判読できない場合がある。 •ドキュメントは、コメント用の十分なスペースを提供するように設計する必要がある。例えば転記エラーの場合、オペレータがそのエラーを取り消し、初期化し、日付を記入し、そして必要な説明を記録するために十分なスペースが必要である。

	•完全な文書化を可能にするためにドキュメントにページが追加された場合、追加されたページの数と参照は、メイン記録ページに明確に文書化され、署名されている必要がある。 •必要なすべてのデータを追加するために十分なスペースをドキュメント形式で提供する必要がある。また例えば、本目的では意図されていない印刷ページの裏面に記録が印刷され、その裏に記録されることを避けるために、データをドキュメントに無計画に記録しないこと。
3.	**Expectation　期待** The document design should make it clear what data is to be provided in entries. ドキュメント設計では、エントリで提供されるデータを明確にする必要がある。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** • Ambiguous instructions may lead to inconsistent/incorrect recording of data. • Good design ensures all critical data is recorded and ensures clear, contemporaneous and enduring (indelible/durable) completion of entries. • The document should also be structured in such a way as to record information in the same order as the operational process and related SOP, to minimize the risk of inadvertently omitting critical data. •あいまいな指示により、データが一貫性のない/不正確な記録につながる可能性がある。 •適正な設計により、すべての重要なデータが記録され、エントリの完了が、明確で同時的でかつ永続的（消えない/永続的な）であることが保証される。 •ドキュメントは、重要なデータを誤って省略してしまうリスクを最小限に抑えるために、運用プロセスおよび関連する SOP と同じ順序で情報を記録するように構造化する必要もある。
4.	**Expectation　期待** Documents should be stored in a manner which ensures appropriate version control. ドキュメントは、適切なバージョン管理を保証する方法で保存する必要がある。 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. マスタードキュメントには、マスターとコピーを区別するために、特徴的なマーキングを含める必要がある。例えば、不注意による使用を防ぐため色紙またはインクを使用する。 Master documents (in electronic form) should be prevented from unauthorised or inadvertent changes. マスタードキュメント（電子形式）は、不正または不注意による変更を防ぐ必要がある。 E.g.: For the template records stored electronically, the following precautions should be in place: - access to master templates should be controlled; - process controls for creating and updating versions should be clear and practically applied/verified; and - master documents should be stored in a manner which prevents unauthorised changes.

	例：電子的に保存されたテンプレート記録の場合、次の予防措置を講じる必要がある。 -マスターテンプレートへのアクセスをコントロールする必要がある。 -バージョンを作成および更新するためのプロセス制御は明確で、実際に適用/検証されている必要がある。 および -マスタードキュメントは、不正な変更を防ぐ方法で保存する必要がある。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** • Inappropriate storage conditions can allow unauthorised modification, use of expired and/or draft documents or cause the loss of master documents. • The processes of implementation and the effective communication, by way of appropriate training prior to implementation when applicable, are just as important as the document. •不適切な保管条件により、不正な変更、期限切れまたはドラフトのドキュメントの使用、マスタードキュメントの損失が発生する可能性がある。 •実装のプロセスおよび、該当する場合は実装前の適切なトレーニングによって効果的なコミュニケーションをとることは、ドキュメントと同じくらい重要である。

Item 項目	Distribution and Control　流通と管理
1.	**Expectation　期待** Updated versions should be distributed in a timely manner. 更新されたバージョンは、タイムリーに配布する必要がある。 Obsolete master documents and files should be archived and their access restricted. 廃止されたマスタードキュメントおよびファイルはアーカイブし、アクセスを制限する必要がある。 Any issued and unused physical documents should be retrieved and reconciled. 発行済みおよび未使用の物理ドキュメントはすべて取得して調整する必要がある。 Where authorised by Quality, recovered copies of documents may be destroyed. However, master copies of authorised documents should be preserved. 品質によって承認された場合、回復されたドキュメントのコピーは破棄される可能性がある。ただし、許可されたドキュメントのマスターコピーは保持する必要がある。

	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** • There may be a risk that obsolete versions can be used by mistake if available for use. •使用可能な場合、廃止されたバージョンが誤って使用される可能性があるリスクがある。
2.	**Expectation　期待** Document issuance should be controlled by written procedures that include the following controls: - details of who issued the copies and when they were issued; - 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; - ensuring that only the current approved version is available for use; - allocating a unique identifier to each blank document issued and recording the issue of each document in a register; - numbering every distributed copy (e.g.: copy 2 of 2) and sequential numbering of issued pages in bound books; - 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”; - 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 - 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. 文書の発行は、以下のコントロールを含む手順書によってコントロールする必要がある。 -誰がコピーを発行したか、いつ発行されたかの詳細。 -承認された文書のコピーを区別する明確な手段。安全なスタンプ、または作業エリアや他の適切なシステムでは利用できない紙のカラーコードを使用する。 -現在承認されているバージョンのみを使用できるようにする。 -発行された各空白のドキュメントに一意の識別子を割り当て、各ドキュメントの発行をレジスタに記録する。 -配布されたすべてのコピーに番号を付け（例：コピー2/2)、製本された本の発行されたページに順番に番号を付ける。 -空白のテンプレートの追加コピーの再発行が必要な場合は、再発行に関する管理されたプロセスに従い、すべての配布コピーを維持し、追加コピーの必要性の正当化と承認を記録する必要がある。例、「元のテンプレート記録が破損した」; -重要な GMP/GDP 空白フォーム（例：ワークシート、実験ノート、バッチ記録、管理記録）は、記録の正確性と完全性を確保するために、使用後に調整する必要がある。および

	-記録以外のドキュメントのコピー（手順など）が参照用にのみ印刷されている場合、ドキュメントの生成時にタイムスタンプが付けられ、その短期的な有効性がドキュメントにマークされていれば、調整は必要ない場合がある。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** • Without the use of security measures, there is a risk that rewriting or falsification of data may be made after photocopying or scanning the template record (which gives the user another template copy to use). • Obsolete versions can be used intentionally or by error. • A filled record with an anomalous data entry could be replaced by a new rewritten template. • All unused forms should be accounted for, and either defaced and destroyed, or returned for secure filing. • 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. •セキュリティ対策を講じない場合、テンプレート記録をコピーまたはスキャンした後にデータの書き換えや改ざんが行われるおそれがある（これにより、ユーザは別のテンプレートコピーを使用できるようになる）。 •廃止されたバージョンは、意図的にまたは誤って使用される可能性がある。 •異常なデータエントリで埋められた記録は、新しく書き直されたテンプレートに置き換えることができる。 •未使用のフォームはすべて説明し、汚損して破壊するか、安全なファイリングのために返送する必要がある。 •（使用されている場合）ドキュメントの参照コピーに、生成日、有効期間、および参照専用であり、公式コピーではないことを明確に示すマークが付いていることを確認する。 印刷時に「管理されていない」とマークされている。

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.).

承認されたすべてのマスタードキュメント（SOP、フォーム、テンプレート、および記録）のインデックスは、医薬品品質システム内で維持する必要がある。 このインデックスには、テンプレート記録の種類ごとに、少なくとも次の情報を記載する必要がある：タイトル、バージョン番号を含む識別子、場所（ドキュメントデータベース、発効日、次のレビュ日など)。

8.5 Use and control of records located at the point-of-use 使用場所にある記録の使用およびコントロール

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.).

記録はオペレーターの使用時に利用できるようにし、これらの記録を管理するための適切なコントロールを行う必要がある。 これらのコントロールは、記録の損傷または損失のリスクを最小限に抑え、データインテグリティを確保するために実施する必要がある。 必要に応じて、記録が汚れるのを防ぐための対策を講じる必要がある（たとえば、濡れたり、材料で汚れたりするなど)。

8.5.2

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

記録は、書面による手順に従って、指定された人物またはプロセスによってこれらの領域で適切にコントロールされる必要がある。

8.6 Filling out records 記録への記入

8.6.1

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

以下の表にリストされている項目は、記録が適切に入力されるようにコントロールする必要がある。

Item 項目	Completion of records 記録の完成
1.	Expectation 期待

	Handwritten entries should be made by the person who executed the task[7]. 手書きのエントリは、タスクを実行した人が作成する必要がある。 Unused, blank fields within documents should be voided (e.g. crossed-out), dated and signed. ドキュメント内の未使用の空白のフィールドは、無効にし（取り消し線など)、日付を記入して署名する必要がある。 Handwritten entries should be made in clear and legible writing. 手書きのエントリは、明確で読みやすい書き込みで実施する必要がある。 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. 日付フィールドの入力は、サイトに定義された明確な形式で行う必要がある。 例えば、 dd / mm / yyyy または mm / dd / yyyy。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** • Check that handwriting is consistent for entries made by the same person. • Check the entry is legible and clear (i.e. unambiguous; and does not include the use of unknown symbols or abbreviations, e.g. use of ditto(“) marks. • Check for completeness of data recorded. • Check correct pagination of the records and are all pages present. •同じ人物が作成したエントリの手書きが一貫していることを確認する。 •エントリが読みやすく明確であることを確認する（すなわち、明確である。不明な記号や略語の使用（ditto（ "）マークの使用など）が含まれていない。 •記録されたデータインテグリティを確認する。 •記録の正しいページ付けを確認し、すべてのページが存在することを確認する。
2.	**Expectation　期待** Records relating to operations should be completed contemporaneously[8]. 運用に関連する記録は、同時に完了する必要がある。

[7] Scribes may only be used in exceptional circumstances, refer footnote 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:　‘exceptional’, and only take place where:

☒ The act of recording places the product or activity at risk e.g. documenting line interventions by sterile operators.

☒ To accommodate cultural or staff literacy / language limitations, for instance where an activity is performed by an operator, but witnessed and recorded by a scribe. In these cases, bilingual or controlled translations of documents into local languages and dialect are advised.

	Potential risk of not meeting expectations/items to be checked • 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. •記録が使用されているすぐ近くの領域で利用できることを確認する。すなわち、査察官は、操作の現場で順次記録を実行できることを期待する必要がある。 フォームが使用時に利用できない場合、オペレーターは発生時に記録に入力できない。
3.	**Expectation　期待** Records should be enduring (indelible). 記録は永続的（消えない）である必要がある。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** • Check that written entries are in ink, which is not erasable, and/or will not smudge or fade (during the retention period). • Check that the records were not filled out using pencil prior to use of pen (overwriting). • Note that some paper printouts from systems may fade over time, e.g. thermal paper. Indelible signed and dated true copies of these should be produced and kept. •書き込まれたエントリがインクであるかどうか、インクは消去できないか、汚れたり色あせたりしない（保持期間中）を確認する。 •ペンを使用する前に、鉛筆を使用して記録に記入されていないことを確認する（上書き）。 •感熱紙等、システムからの一部の紙のプリントアウトは、時間の経過とともに色あせする可能性があることに注意すること。これらの消えない署名と日付の付いた真のコピーを作成して保管する必要がある。
4.	**Expectation　期待** Records should be signed and dated using a unique identifier that is attributable to the author. 記録は、作成者に起因する一意の識別子を使用して署名および日付を記入する必要がある。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** • Check that there are signature and initials logs, that are controlled and current and that

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.

	demonstrate the use of unique examples, not just standardized printed letters. • Ensure that all key entries are signed & dated, particularly if steps occur over time, i.e. not just signed at the end of the page and/or process. • The use of personal seals is generally not encouraged; however, where used, seals 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. •標準化された印刷文字だけでなく、署名ログとイニシャルログがコントロールされ、最新ものであり、独自の例の使用を示していることを確認する。 •特に、ステップが時間の経過とともに発生する場合、すなわち、ページやプロセスの最後で署名されるだけではなく、すべての重要なエントリが署名され、日付が付けられていることを確認する。 •個人印鑑の使用は一般的に推奨されていない。 ただし、使用する場合は、シールはアクセスに対してコントロールされる必要がある。 個人と個人の印鑑との間のトレーサビリティを明確に示すログが必要である。 個人用シールの使用は、許容できると見なされるように、(所有者が)日付を記入する必要がある。

8.7 Making corrections on records 記録を修正する

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

記録の修正は、完全なトレーサビリティが維持されるように行う必要がある。

Item 項目	How should records be corrected? 記録はどのように修正する必要があるか？
1.	**Expectation 期待** Cross out what is to be changed with a single line. 変更する内容を単線で取り消す。 Where appropriate, the reason for the correction should be clearly recorded and verified if critical. 必要に応じて、修正の理由を明確に記録し、重要な場合は検証する必要がある。 Initial and date the change made. 変更が行われた初期および日付。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** • Check that the original data is readable not obscured (e.g. not obscured by use of liquid paper; overwriting is not permitted). • If changes have been made to critical data entries, verify that a valid reason for the change has been recorded and that supporting evidence for the change is available.

	• Check for unexplained symbols or entries in records. •元のデータが読み取り可能で、隠されていないことを確認する（たとえば、液体紙を使用して隠されていない、上書きは許可されていない)。 •重要なデータエントリに変更が加えられた場合は、変更の正当な理由が記録されていること、および変更の裏付けとなる証拠が利用可能であることを確認すること。 •説明のつかない記号または記録内のエントリを確認する。
2.	**Expectation　期待** Corrections should be made in indelible ink. 修正は、消えないインクで行う必要がある。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** • Check that written entries are in ink, which is not erasable, and/or will not smudge or fade (during the retention period). • Check that the records were not filled out using pencil prior to use of pen (overwriting). •書き込まれたエントリがインクであるかどうかを確認する。インクは消去できないか、汚れたり色あせたりしない（保持期間中)。 •ペンを使用する前に、鉛筆を使用して記録に記入されていないことを確認すること（上書き)。

8.8　Verification of records (secondary checks) 記録の検証（二次チェック）

Item 項目	When and who should verify the records? いつ、誰が記録を確認する必要があるか？
1.	**Expectation　期待** Records of critical process steps, e.g. critical steps within batch records, should be: - reviewed/witnessed by independent and designated personnel at the time of operations occurring; and - reviewed by an approved person within the production department before sending them to the Quality unit ; and - reviewed and approved by the Quality Unit (e.g. Authorised Person /Qualified Person) before release or distribution of the batch produced. 重要なプロセスステップの記録。例えば、バッチ記録内の重要な手順は次のとおりである。 -操作の発生時に、独立し指定された担当者によりレビュ/立ち会い。 そして -品質部門に送る前に、製造部門内の承認された人によりレビュ。 そして -生産されたバッチのリリースまたは配布の前に、品質部門（権限をもつ人/資格のある人など）によってレビュおよび承認される。

	Batch production records of non-critical process steps is generally reviewed by production personnel according to an approved procedure. 重要でないプロセスステップのバッチ生産記録は、通常、承認された手順に従い生産担当者によってレビュされる。 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. テストステップのラボ記録も、テストの完了後に指定された担当者（例：2 番目のアナリスト）が確認する必要がある。 レビュアは、すべてのエントリ、重要な計算をチェックし、データインテグリティの原則に従ってテスト結果の信頼性の適切な評価を行うことが期待されている。 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. 重要なテストの解釈が単一の個人によって行われる場合（例えば、寒天プレート上の微生物コロニーの記録)、追加のコントロールを検討する必要がある。 リスクマネジメントの原則に従って、二次審査が必要になる場合がある。 場合によっては、このレビュをリアルタイムで実行する必要がある。 重要なデータを検証する適切な電子的手段は、例えば、保持のためにデータの写真画像を撮る等、許容できる代替手段である可能性がある。 This verification should be conducted after performing production-related tasks and activities and be signed or initialled and dated by the appropriate persons. この検証は、生産関連のタスクとアクティビティを実施した後に実行し、適切な担当者が署名または初期化して日付を記入する必要がある。 Local SOPs should be in place to describe the process for review of written documents. 書面による文書のレビュのプロセスを説明するために、ローカル SOP を設置する必要がある。
	Specific elements that should be checked when reviewing records: **記録を確認するときにチェックする必要がある特定の要素：** • 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. • Verify that any secondary checks performed during processing were performed by

	appropriately qualified and independent personnel, e.g. production supervisor or QA. • Check that documents were reviewed by production personnel and then quality assurance personnel following completion of operational activities. •処理エリア内での生産記録の処理プロセスを検証して、記録に関連するアクティビティを実行するときに、適切な担当者が生産記録をすぐに利用できるようにする。 •処理中に実行された二次チェックが、生産監督者または QA 等、適切な資格を持った独立した担当者によって実行されたことを確認する。 •運用アクティビティの完了後、ドキュメントが生産担当者によってレビュされ、次に品質保証担当者によってレビュされたことを確認する。

Item 項目	How should records be verified? 記録はどのように検証する必要があるか？
2.	**Expectation　期待** 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. 現在の（承認された）テンプレートを使用してすべてのフィールドが正しく入力されていること、およびデータが受け入れ基準と厳密に比較されていることを確認すること。 Check items 1, 2, 3, and 4 of section 8.6 and Items 1 and 2 of section 8.7 セクション 8.6 の項目 1、2、3、および 4 とセクション 8.7 の項目 1 および 2 を確認すること。
	Specific elements that should be checked when reviewing records: **記録を確認するときにチェックする必要がある特定の要素：** • Inspectors should review company procedures for the review of manual data to determine the adequacy of processes. • The need for, and extent of a secondary check should be based on quality risk management principles, based on the criticality of the data generated. • Check that the secondary reviews of data include a verification of any calculations used. • View original data (where possible) to confirm that the correct data was transcribed for the calculation. •査察官は、プロセスの妥当性を判断するために、手動データをレビュするため企業の手順をレビュする必要がある。 •二次チェックの必要性と範囲は、生成されたデータの重要性に基づく品質リスクマネジメントの原則に基づく必要がある。 •データの二次レビュに、使用された計算の検証が含まれていることを確認する。 •元のデータを表示し（可能な場合)、計算のために正しいデータが転記されたことを確認する。

8.9　Direct print-outs from electronic systems 電子システムからの直接プリントアウト

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.

いくつかの非常に単純な電子システム、例えば 天びん、pH メーター、またはデータを保存しない単純な処理装置は、直接印刷された紙の記録を生成する。 これらのタイプのシステムと記録は、電子日付/タイムスタンプの（再）処理、変更によってデータの表示に影響を与える限られた機会を提供する。 このような状況では、元の記録は、記録を生成する人によって署名および日付が付けられ、サンプル ID、バッチ番号などのトレーサビリティを確保するための情報が記録に記録される必要がある。 これらの元の記録は、バッチ処理またはテスト記録に添付する必要がある。

8.9.2

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

これらの記録が永続的であることを確認することを検討する必要がある（セクション 8.6.1 を参照)。

8.10 Document retention (Identifying record retention requirements and archiving records) ドキュメントの保持（記録の保持要件の特定と記録のアーカイブ）

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.

各タイプの記録の保持期間は、（少なくとも）GMP/GDP 要件で指定された期間を満たす必要がある。 より長い保管期間を規定する可能性のある他の地方または国の法律を考慮する必要がある。

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.

記録は、内部で保持することも、品質契約に従って外部のストレージサービスを使用して保持することもできる。 この場合、データセンターの場所を特定する必要がある。 保持システム/施設/サービスが適切であり、残留リスクが理解されていることを実証するために、リスク評価が利用可能である必要がある。

Item 項目	Where and how should records be archived? 記録はどこにどのようにアーカイブする必要るか？

1.	**Expectation　期待** 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.). 記録をアーカイブするためのさまざまな手順（アーカイブボックスの識別、ボックスごとの記録のリスト、保存期間、アーカイブ場所など）を説明するシステムを導入する必要がある。 Instructions regarding the controls for storage, as well as access and recovery of records should be in place. ストレージの制御、および記録へのアクセスと回復に関する指示を実施する必要がある。 Systems should ensure that all GMP/GDP relevant records are stored for periods that meet GMP/GDP requirements[9]. システムは、すべての GMP/GDP 関連記録が、GMP/GDP 要件を満たす期間保存されていることを確認する必要がある。
	Specific elements that should be checked when reviewing records: **記録を確認するときにチェックする必要がある特定の要素：** • Check that the system implemented for retrieving archived records is effective and traceable. • Check if the records are stored in an orderly manner and are easily identifiable. • Check that records are in the defined location and appropriately secured. • Check that access to archived documents is restricted to authorised personnel ensuring integrity of the stored records. • Check for the presence of records of accessing and returning of records. • The storage methods used should permit efficient retrieval of documents when required. •アーカイブされた記録を取得するために実装されたシステムが効果的で追跡可能であることを確認する。 •記録が整然と保存されており、簡単に識別できるかどうかを確認する。 •記録が定義された場所にあり、適切に保護されていることを確認する。 •アーカイブされたドキュメントへのアクセスが許可された担当者に制限されていることを確認し、保存された記録のインテグリティを確保する。 •記録へのアクセスと記録の返却の記録の存在を確認する。 •使用する保存方法は、必要に応じてドキュメントを効率的に取得できるようにする必要がある。

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

2.	**Expectation　期待** All hardcopy quality records should be archived in: - secure locations to prevent damage or loss, - such a manner that it is easily traceable and retrievable, and - a manner that ensures that records are durable for their archived life. すべてのハードコピー品質記録は、以下のようににアーカイブする必要がある。 -損傷や紛失を防ぐために場所を確保、 -簡単に追跡および取得できるような方法、および -記録がアーカイブ寿命の間耐久性があることを保証する方法。
	Specific elements that should be checked when reviewing records: **記録を確認するときにチェックする必要がある特定の要素：** • Check for the outsourced archived operations if there is a quality agreement in place and if the storage location was audited. • Ensure there is some assessment of ensuring that documents will still be legible/available for the entire archival period. • In case of printouts which are not permanent (e.g. thermal transfer paper) a verified ('true') copy should be retained. • Verify whether the storage methods used permit efficient retrieval of documents when required. •品質協定が締結されているかどうか、および保管場所が監査されているかどうか、外部委託されたアーカイブ操作を確認する。 •アーカイブ期間全体にわたってドキュメントが引き続き判読可能/利用可能であることを確認するための評価があることを確認する。 •永続的ではないプリントアウトの場合（例：熱転写紙）検証済みの（「真の」）コピーを保持する必要がある。 •使用する保存方法で、必要なときにドキュメントを効率的に取得できるかどうかを確認する。
3.	**Expectation　期待** All records should be protected from damage or destruction by: - fire; - liquids (e.g. water, solvents and buffer solution); - rodents; - humidity etc; and. - unauthorised personnel access, who may attempt to amend, destroy or replace records. すべての記録は、次の方法で損傷または破壊から保護する必要がある。 - 火; -液体（例：水、溶剤、緩衝液）; -げっ歯類;

	-湿度など; そして。 -記録の修正、破棄、または置き換えを試みる可能性のある、許可されていない人員のアクセス。
	Specific elements that should be checked when reviewing records: **記録を確認するときにチェックする必要がある特定の要素：** • Check if there are systems in place to protect records (e.g. pest control and sprinklers). • 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. • Check for appropriate access controls for records. •記録を保護するためのシステムが整っているかどうかを確認する（害虫駆除やスプリンクラーなど)。 •注：スプリンクラーシステムは、地域の安全要件に従って実装する必要がある。 ただし、ドキュメントが水から保護されるなど、文書の損傷を防ぐために設計する必要がある。 •記録の適切なアクセス制御を確認する。

8.11 Disposal of original records or true copies 元の記録または真のコピーの廃棄

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.)

記録の廃棄に関する文書化されたプロセスは、定義された保存期間の後に正しい元のレコードまたは真のコピーが破棄されるようにするために、適切な場所に配置する必要がある。 システムは、現在の記録が誤って破壊されないようにし、履歴記録が誤って現在の記録ストリームに戻らないようにする必要がある（たとえば、履歴記録が既存の記録と混同/混合されている)。

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.

記録/登録簿は、地域の方針に従って、廃止された記録の適切かつタイムリーなアーカイブまたは破棄を実証するために利用可能である必要がある。

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.

間違った文書を削除するリスクを減らすための対策を講じる必要がある。 記録の廃棄を許可するアクセス権

は管理され、少数の人に制限されるべきである。

9. SPECIFIC DATA INTEGRITY CONSIDERATIONS FOR COMPUTERISED SYSTEMS コンピュータ化されたシステムに関する特定のデータインテグリティに関する考慮事項

9.1 Structure of the Pharmaceutical Quality System and control of computerised systems 医薬品品質システムの構造とコンピュータ化されたシステムの管理

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.

企業は、多様なコンピュータ化されたシステムを使用して、多数の運用活動を支援している。 これらは、単純なスタンドアロンから大規模な統合された複雑なシステムにまでおよび、その多くは製造される製品の品質に影響を与える。 すべてのコンピュータ化されたシステムを完全に評価およびコントロールし、GMP および GDP 要件に従ってそれらを管理することは、各規制対象者の責任である。

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.

組織は、使用されるコンピュータ化されたシステムの性質と範囲を十分に認識し、各システム、その使用目的と機能、および操作の影響を受けやすい可能性のあるデータインテグリティのリスクまたは脆弱性を説明する評価を実施する必要がある。 製品の品質に関して、コンピュータ化されたシステムおよび関連データの重要性を判断することに特に重点を置く必要がある。

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.

製品の品質に影響を与える可能性のあるすべてのコンピュータ化されたシステムは、データの品質とインテグリティに影響を与える可能性のある偶発的または意図的な操作、変更、またはその他の活動からシステムを保護するように設計された医薬品品質システムの下で効果的に管理する必要がある。

9.1.4

---

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

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

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.

コンピュータ化されたシステムの設計、評価、および選択のプロセスには、システムのデータマネジメントとインテグリティの側面を適切に考慮する必要がある。 規制対象のユーザは、システムのベンダーが GMP/GDP とデータインテグリティの要件を十分に理解していること、および新しいシステムに効果的なデータマネジメントを確実にするための適切なコントロールが含まれていることを確認する必要がある。 レガシーシステムは、同じ基本要件を満たすことが期待されている。 ただし、完全に準拠するには、管理手順または補足のセキュリティハードウェア/ソフトウェアをサポートする等、追加のコントロールの使用が必要になる場合がある。

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:

規制対象のユーザは、コンピュータ化されたシステムによって生成されるデータの範囲と性質を完全に理解する必要があり、データのリスクと重要度（メタデータを含む）および生成されたデータの管理に必要な後続のコントロールを決定するためにリスクベースのアプローチを採用する必要がある。 例えば：

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.

生データを処理する場合、通常、製造イベントまたは分析を再構築するために、生データの完全なキャプチャと保持が必要になる。

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.

メタデータを処理する際、一部のメタデータはイベントの再構築に重要であり（ユーザの識別、時間、重要なプロセスパラメータ、測定単位など)、完全にキャプチャして管理する必要がある「関連メタデータ」と見なされる。 ただし、システムエラーログや重要でないシステムチェックなどの重要でないメタデータは、リスクマネジメントを使用して正当化される場合、完全なキャプチャと管理を必要としない場合がある。

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.

データの脆弱性とリスクを判断するときは、コンピュータ化されたシステムをビジネスプロセス内での使用との関連で考慮することが重要である。 たとえば、統合されたコンピュータインターフェースを利用した分析方法によって生成された結果のインテグリティは、サンプルの準備、システムへのサンプルの重みの入力、データを生成するためのシステムの使用、およびそのデータを使用した最終結果の処理/記録によって影響を受ける。 データフローマップの作成と評価は、コンピュータ化されたシステム、特にインターフェースされたシステムのリスクと脆弱性を理解するのに役立つ場合がある。

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.

システムやソフトウェアに組み込まれている固有のデータインテグリティ制御、特に最新のデータマネジメント要件を満たすように設計された最新のシステムよりもエクスプロイトに対して脆弱である可能性のあるコントロールを考慮する必要がある。 脆弱性をもつシステムの例としては、手動記録システム、旧式のセキュリティ対策を備えた古い電子システム、ネットワーク化されていない電子システム、ファイアウォールと侵入検知または防御システムを使用してネットワークセキュリティを必強化する必要があるシステムなどがある。

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.

コンピュータ化されたシステムの査察中、査察官は評価中に企業の専門知識を利用することを推奨する。 アクセスとナビゲーションを容易にするように企業の担当者に依頼して指示することは、システムの査察に役立つ。

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).

ここでのガイダンスは、コンピュータ化されたシステムのコンテキストでのデータインテグリティに関する特定の考慮事項を提供することを目的としている。 コンピュータ化されたシステムの適切な実践に関する詳

細なガイダンスは、『PIC/S Good Practices for Computerised Systems in Regulated“GxP” Environments（PI011)』に記載されている。

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.

ここでの原則は、コンピュータ化されたシステムの提供が外部委託されている状況にも同様に適用される。このような場合、規制対象のエンティティは、アウトソーシングされたサービスが GMP/GDP 要件に従って管理および評価され、適切なデータマネジメントとインテグリティのコントロールが両当事者によって理解され、効果的に実装されることを保証する責任を保持する。

9.2 Qualification and validation of computerised systems コンピュータ化されたシステムの適格性とバリデーション

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.

コンピュータ化されたシステムの適格性とバリデーションは、関連する GMP/GDP ガイドラインに従って実行する必要がある。 以下の表は、コンピュータ化されたシステムの適正なデータガバナンス実践を確保するための具体的な期待に関する明確化を示している。

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.

バリデーションだけでは、生成された記録が必ずしも適切に保護されていることを必ずしも保証するものではなく、バリデーションシステムは、偶発的または悪意のある手段による損失や改ざんに対して脆弱である可能性がある。 したがって、バリデーションは、適切な管理上および物理的な制御、およびユーザのトレーニングによって補完する必要がある。

9.3 Validation and Maintenance　バリデーションとメンテナンス

Item 項目	System Validation & Maintenance　システムのバリデーションとメンテナンス

1.	**Expectation　期待** 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. 規制対象企業は、システム調達の初期段階およびシステムおよびデータのライフサイクル全体において、データマネジメントおよびインテグリティの要件を考慮するために、適切な制御を文書化し、実装する必要がある。 規制対象のユーザの場合、機能仕様（FS）および/またはユーザ要件仕様（URS）は、データマネジメントおよびインテグリティの要件に適切に対応する必要がある。 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. GMP/GDP の重要な機器の購入には、購入前にシステムのデータインテグリティ制御が適切に評価されるようにするため、特に注意する必要がある。 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. レガシーシステム（使用中の既存のシステム）を評価して、既存のシステム構成と機能が、適切なデータマネジメントおよびインテグリティの実践に従ってデータの適切な制御を可能にするかどうかを判断する必要がある。 これらのシステムのシステム機能または設計が適切なレベルの制御を提供しない場合は、追加の制御を検討して実装する必要がある。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** • Inadequate consideration of DI requirements may result in the purchase of software systems that do not include the basic functionality required to meet data management and integrity expectations. • Inspectors should verify that the implementation of new systems followed a process that gave adequate consideration to DI principles. • Some legacy systems may not include appropriate controls for data management, which may allow the manipulation of data with a low probability of detection. • Assessments of existing systems should be available and provide an overview of any vulnerabilities and list any additional controls implemented to assure data integrity.

	Additional controls should be appropriately validated and may include: o 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; o Configuring operating system file/folder permissions to prevent modification/deletion of files when the PI 041-1 34 of 63 1 July 2021 modification/deletion of data files cannot be controlled by system software; or o Implementation of hybrid or manual systems to provide control of data generated. •DI 要件を十分に考慮しないと、データマネジメントおよびインテグリティの期待に応えるために必要な基本機能を含まないソフトウェアシステムを購入する可能性がある。 •査察官は、新しいシステムの実装が DI の原則を十分に考慮したプロセスに従っていることを確認する必要がある。 •一部のレガシーシステムには、データマネジメントに適したコントロールが含まれていない場合があり、検出の可能性が低いデータの操作が可能になる場合がある。 •既存のシステムの評価が利用可能であり、脆弱性の概要を提供し、データインテグリティを保証するために実装された追加のコントロールをリストする必要がある。追加のコントロールは適切にバリデートする必要があり、以下が含まれる場合がある。 o オペレーティングシステムの機能（Windows Active Directory グループなど）を使用して、ユーザとそのアクセス権限を割り当てる場合。システムソフトウェアには、ユーザ権限を制御するための管理コントロールが含まれていない。 o PI 041-1 34 of 63 2021 年 7 月 1 日データファイルの変更/削除をシステムソフトウェアで制御できない場合にファイルの変更/削除を防ぐためのオペレーティングシステムファイル/フォルダーのアクセス許可を設定する。または o 生成されたデータの制御を提供するためのハイブリッドまたは手動システムの実装。
2.	**Expectation　期待** Regulated users should have an inventory of all computerised systems in use. The list should include reference to: - The name, location and primary function of each computerised system; - Assessments of the function and criticality of the system and associated data; (e.g. direct GMP/GDP impact, indirect impact, none) - The current validation status of each system and reference to existing validation documents. 規制対象のユーザは、使用中のすべてのコンピュータ化されたシステムのインベントリを持っている必要がある。 リストには、以下への参照を含める必要がある。 -各コンピュータ化されたシステムの名前、場所、および主な機能。 -システムおよび関連データの機能と重要度の評価。(例：直接的な GMP/GDP の影響、間接的な影響、なし) -各システムの現在のバリデーションのステータスと既存のバリデードキュメントへの参

	照。 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. システムごとにリスク評価を実施する必要がある。具体的には、データインテグリティを確保するために必要な管理を評価する。データインテグリティのコントロールのバリデーションのレベルと範囲は、システムとプロセスの重要性、および製品品質に対する潜在的なリスクに基づいて決定する必要がある。 バッチリリースデータを生成または制御するプロセスまたはシステムは、一般に、重要度の低いデータまたはプロセスを管理するシステムよりも高度な制御を必要とする。 Consideration should also be given to those systems with higher potential for disaster, malfunction or situations in which the system becomes inoperative. 災害、誤動作、またはシステムが動作不能になる可能性が高いシステムについても考慮する必要がある。 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. 評価では、重要な構成設定またはデータの操作に対する不注意または不正な変更に対するシステムの脆弱性も確認する必要がある。 すべてのコントロールを文書化し、その有効性を検証する必要がある。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** • Companies that do not have adequate visibility of all computerised systems in place may overlook the criticality of systems and may thus create vulnerabilities within the data lifecycle. • An inventory list serves to clearly communicate all systems in place and their criticality, ensuring that any changes or modifications to these systems are controlled. • Verify that risk assessments are in place for critical processing equipment and data acquisition systems. A lack of thorough assessment of system impact may lead to a lack of appropriate validation and system control. Examples of critical systems to review include: o systems used to control the purchasing and status of products and materials; o systems for the control and data acquisition for critical manufacturing processes; o systems that generate, store or process data that is used to determine batch quality; o systems that generate data that is included in the batch processing or packaging

	records; and o systems used in the decision process for the release of products. •すべてのコンピュータ化されたシステムを適切に把握していない企業は、システムの重要性を見落とし、データライフサイクル内に脆弱性を生み出す可能性がある。 •インベントリリストは、配置されているすべてのシステムとその重要性を明確に伝達し、これらのシステムへの変更や修正が確実にコントロールされるようにする。 •重要な処理装置とデータ取得システムのリスク評価が実施されていることを確認する。システムへの影響を徹底的に評価しないと、適切なバリデーションとシステムコントロールが欠如する可能性がある。レビュする重要なシステムの例は次のとおりである。 o 製品および材料の購入とステコントロールおよびデータ取得のためのシステム。 o バッチ品質を決定するために使用されるデータを生成、保存、または処理するシステム。 o バッチ処理またはパッケージング記録に含まれるデータを生成するシステム。そして o 製品のリリースの決定プロセスで使用されるシステム。
3.	**Expectation　期待** 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: - Critical system configuration details and controls for restricting access to configuration and any changes (change management). - A list of all currently approved normal and administrative users specifying the username and the role of the user. - requency of review of audit trails and system logs. - Procedures for: o creating new system user; o modifying or changing privileges for an existing user; o defining the combination or format of passwords for each system o reviewing and deleting users; o back-up processes and frequency; o disaster recovery; o data archiving (processes and responsibilities), including procedures for accessing and reading archived data; o approving locations for data storage. - The report should explain how the original data are retained with relevant metadata in a form that permits the reconstruction of the manufacturing process or the analytical activity. 新しいシステムの場合、各コンピュータ化されたシステムのバリデーション要約レポート（付録 15 の要件に従って作成および承認されたもの）を用意し、少なくとも次の項目

	を記載（または参照を提供）する必要がある。 -構成および変更へのアクセスを制限するための重要なシステム構成の詳細とコントロール（変更管理)。 -ユーザ名とユーザの役割を指定する、現在承認されているすべての通常ユーザと管理ユーザのリスト。 -監査証跡とシステムログのレビュの頻度。 -以下の手順： o 新しいシステムユーザの作成。 o 既存のユーザの特権の修正または変更。 o 各システムのパスワードの組み合わせまたは形式の定義 o ユーザの確認および削除。 o バックアッププロセスと頻度。 o 災害復旧。 o アーカイブされたデータにアクセスして読み取るための手順を含む、データのアーカイブ（プロセスと責任)。 o データストレージの場所を承認。 -レポートでは、製造プロセスまたは分析アクティビティの再構築を可能にする形式で、元のデータが関連するメタデータとともにどのように保持されるかを説明する必要がある。 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. 既存のシステムの場合、上記の要件を指定するドキュメントが利用可能である必要がある。 ただし、バリデーションの概要レポートにコンパイルする必要はない。 これらの文書は、規制対象のユーザが必要に応じて維持および更新する必要がある。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** • Check that validation systems and reports specifically address data integrity requirements following GMP/GDP requirements and considering ALCOA principles. • System configuration and segregation of duties (e.g. authorisation to generate data should be separate to authorisation to verify data) should be defined prior to validation, and verified as effective during testing. • Check the procedures for system access to ensure modifications or changes to systems are restricted and subject to change control management. • Ensure that system administrator access is restricted to authorised persons and is not used for routine operations. • Check the procedures for granting, modifying and removing access to computerised systems to ensure these activities are controlled. Check the currency of user access logs and privilege levels, there should be no unauthorised users to the system and access accounts

	should be kept up to date. • There should also be restrictions to prevent users from amending audit trail functions and from changing any pre-defined directory paths where data files are to be stored. •GMP/GDP 要件に従い、ALCOA の原則を考慮して、データインテグリティ要件に特に対応するバリデーションシステムとレポートを確認する。 •システム構成と職務の分離（たとえば、データを生成するための承認は、データを検証するための承認とは別にする必要がある） 検証前に定義し、テスト中に有効であると検証する必要がある。 •システムアクセスの手順をチェックして、システムへの変更または変更が制限され、変更コントロール管理の対象であることを確認する。 •システム管理者のアクセスが許可された人に制限されており、日常の操作に使用されていないことを確認すること。 •コンピュータ化されたシステムへのアクセスを許可、変更、および削除する手順を確認し、これらのアクティビティが制御されていることを確認する。ユーザクセスログと特権レベルの最新性を確認し、システムへの不正なユーザが存在しないようにし、アクセスアカウントを最新の状態に保つ必要がある。 •ユーザが監査証跡機能を修正したり、データファイルが保存される事前定義されたディレクトリパスを変更できないようにするための制限も必要である。
4.	**Expectation　期待** 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. 企業は、コンピュータ化されたシステムの特定のポリシーとバリデーション要件、およびそのようなシステムと関連データのインテグリティを含むバリデーションマスタープランを実施する必要がある。 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. コンピュータ化されたシステムのバリデーションの範囲は、リスクに基づいて決定する必要がある。 コンピュータ化されたシステムのバリデーション要件の評価に関する詳細なガイダンスは、PI011 を参照すること。 Before a system is put into routine use, it should be challenged with defined tests for conformance with the acceptance criteria. システムを日常的に使用する前に、受け入れ基準に準拠しているかどうかを定義したテストでチャレンジする必要がある。 It would be expected that a prospective validation for computerised systems is conducted.

	Appropriate validation data should be available for systems already in-use. コンピュータ化されたシステムの将来のバリデーション要件が行われることが期待される。 すでに使用されているシステムについては、適切なバリデーション要件データが利用可能である必要がある。 Computerised system validation should be designed according to GMP Annex 15 with URS, DQ, FAT, SAT, IQ, OQ and PQ tests as necessary. コンピュータ化されたシステム検証は、必要に応じて URS、DQ、FAT、SAT、IQ、OQ、および PQ テストを備えた GMP Annex15 に従って設計する必要がある。 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. 適格性テストのアプローチは、バリデーション中の特定のシステムに合わせて調整する必要があり、規制対象のユーザによって正当化される必要がある。適格性には、設計時適格性評価（DQ）が含まれる場合がある。据え付け時適格性確認（IQ）；稼働性能適格性確認（OQ）；および稼働性能適格性確認（PQ)。 特に、データの品質やインテグリティが危険にさらされている領域にチャンレンジするために、特定のテストを設計する必要がある。 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. 企業は、コンピュータ化されたシステムが意図された用途に適していることを確認する必要がある。 したがって、企業はベンダー認定パッケージのみに依存するべきではない。 バリデーション演習には、通常の使用目的を反映した操作中にデータインテグリティが維持されることを確認するための特定のテストを含める必要がある。 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. テストの数はリスク評価によって導かれる必要があるが、重要な機能は少なくとも特定され、テストされる必要がある。たとえば、基本的なアルゴリズムまたは論理セットに基づく特定の PLC およびシステム、機能テストはコンピュータ化されたシステムの信頼性の適切な保証を提供する場合がある 。重要なシステムやより複雑なシステムの場合、

	IQ、OQ、および PQ の段階で詳細な検証テストが必要である。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** • Check that validation documents include specific provisions for data integrity; validation reports should specifically address data integrity principles and demonstrate through design and testing that adequate controls are in place. • Unvalidated systems may present a significant vulnerability regarding data integrity as user access and system configuration may allow data amendment. • Check that end-user testing includes test-scripts designed to demonstrate that software not only meets the requirements of the vendor, but is fit for its intended use. •バリデーションドキュメントにデータインテグリティに関する特定の規定が含まれていることを確認する。バリデーションレポートは、データインテグリティの原則に具体的に対処し、設計とテストを通じて適切な管理が行われていることを実証する必要がある。 •バリデーションされていないシステムは、ユーザクセスとシステム構成によってデータの修正が可能になる可能性があるため、データインテグリティに関して重大な脆弱性を示す可能性がある。 •エンドユーザのテストに、ソフトウェアがベンダーの要件を満たしているだけでなく、その使用目的に適合していることを示すように設計されたテストスクリプトが含まれていることを確認する。
5.	**Expectation　期待** Periodic System Evaluation　　定期的なシステム評価 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. データインテグリティ制御に関する継続的なコンプライアンスを確保するために、コンピュータ化されたシステムを定期的に評価する必要がある。 評価には、逸脱、変更（変更の累積的な影響を含む)、アップグレード履歴、パフォーマンス、およびメンテナンスを含め、これらの変更がデータマネジメントおよびインテグリティのコントロールに悪影響を及ぼしたかどうかを評価する必要がある。 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. 再評価の頻度は、前回のレビュ以降のシステムへの変更の累積的な影響を考慮した、コンピュータ化されたシステムの重要度に応じたリスク評価に基づく必要がある。 実行さ

	れた評価は文書化する必要がある。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** • Check that re-validation reviews for computerised systems are outlined within validation schedules. • Verify that systems have been subject to periodic review, particularly with respect to any potential vulnerabilities regarding data integrity. • Any issues identified, such as limitations of current software/hardware should be addressed in a timely manner and corrective and preventive actions, and interim controls should be available and implemented to manage any identified risks. •コンピュータ化されたシステムの再バリデーションレビュがバリデーションスケジュール内に概説されていることを確認する。 •特にデータインテグリティに関する潜在的な脆弱性に関して、システムが定期的なレビュの対象になっていることを確認する。 •現在のソフトウェア/ハードウェアの制限など、特定された問題はタイムリーに対処し、是正措置と予防措置を講じる必要がある。また、特定されたリスクを管理するための暫定的なコントロールを利用して実装する必要がある。
6.	**Expectation　期待** 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. オペレーティングシステムとネットワークコンポーネント（ハードウェアを含む）は、ベンダーの推奨事項に従ってタイムリーに更新する必要があり、古いプラットフォームから新しいプラットフォームへのアプリケーションの移行は、システムによって生成されたデータのマネジメントおよびインテグリティに影響する可能性のある、サポートされていない状態に達する前に、事前に計画および実行する必要がある。 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. オペレーティングシステムとネットワークコンポーネントのセキュリティパッチは、データのセキュリティを維持するために、ベンダーの推奨事項に従って、制御されたタイムリーな方法で適用する必要がある。 セキュリティパッチの適用は、変更管理の原則に従って実行する必要がある。 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. サポートされていないオペレーティングシステムが維持されている場合、すなわち、ベンダーによるサポートがなくなった後でも古いオペレーティングシステムが使用されている場合、またはサポートされているバージョンにセキュリティパッチが適用されていない場合、システム（サーバー）はネットワークの他の部分から可能な限り分離する必要がある。 サポートされていないオペレーティングシステムによって引き起こされる脆弱性の悪用を防ぐために、残りのインターフェースと他の機器との間のデータ転送は、慎重に設計、構成、および適格化する必要がある。 Remote access to unsupported systems should be carefully evaluated due to inherent vulnerability risks. サポートされていないシステムへのリモートアクセスは、固有の脆弱性リスクがあるため、慎重に評価する必要がある。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** • 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. •システムの更新がコントロールされたタイムリーな方法で実行されていることを確認する。 古いシステムを批判的にレビュして、適切なデータインテグリティコントロールが統合されているかどうか、または（統合のコントロールが不可能な場合）適切な管理コントロールが実装されており、効果的であるかどうかを判断する必要がある。

9.4 Data Transfer　データ転送

Item 項目	Data transfer and migration　データの転送と移行
1.	**Expectation　期待** Interfaces should be assessed and addressed during validation to ensure the correct and complete transfer of data. データが正しく完全に転送されるように、バリデーション中にインターフェースを評価して対処する必要がある。 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:

	o Secure transfer o Encryption o Checksums データインテグリティのリスクを最小限に抑えるために、インターフェースには、データの正確で安全な入力と処理のための適切な組み込みチェックを含める必要がある。 検証方法には、以下の使用が含まれる場合がある。 o 安全な転送 o 暗号化 o チェックサム Where applicable, interfaces between systems should be designed and qualified to include an automated transfer of GMP/GDP data. 該当する場合、システム間のインターフェースは、GMP/GDP データの自動転送を含むように設計および認定する必要がある。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** • Interfaces between computerised systems present a risk whereby data may be inadvertently lost, amended or transcribed incorrectly during the transfer process. • Ensure data is transferred directly to the secure location/database and not simply copied from the local drive (where it may have the potential to be altered). • Temporary data storage on local computerised systems (e.g. instrument computer) before transfer to final storage or data processing location creates an opportunity for data to be deleted or manipulated. This is a particular risk in the case of 'standalone' (non-networked) systems. Ensure the environment that initially stores the data has appropriate DI controls in place. • Well designed and qualified automated data transfer is much more reliable than any manual data transfer conducted by humans. •コンピュータ化されたシステム間のインターフェースには、転送プロセス中にデータが誤って失われたり、修正されたり、誤って転記されたりするリスクがある。 •データがローカルドライブ（変更される可能性がある場所）から単にコピーされるのではなく、安全な場所/データベースに直接転送されることを確認する。 •最終的なストレージまたはデータ処理場所に転送する前に、ローカルのコンピュータ化されたシステム（機器コンピュータなど）に一時的にデータを保存した場合、データを削除または操作する機会が生まれる。 これは、「スタンドアロン」（ネットワーク化されていない）システムの場合に特に発生するリスクである。 データを最初に保存する環境に適切な DI 制御が設定されていることを確認する。 •適切に設計され、認定された自動データ転送は、人間が手動で行うデータ転送よりもはるかに信頼性が高くなる。
2.	**Expectation　期待**

	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. システムソフトウェア（オペレーティングシステムを含む）がインストールまたは更新されている場合、ユーザは既存およびアーカイブされたデータが新しいソフトウェアで読み取り可能であることを確認する必要がある。 必要に応じて、既存のアーカイブデータを新しい形式に変換する必要がある場合がある。 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. 新しいソフトウェアの新しいデータ形式への変換が不可能な場合は、古いソフトウェアを維持する必要がある。 1台のコンピュータまたは他の技術ソリューションにインストールされ、調査の際にアーカイブされたデータを読み取る機会を得るためのバックアップメディアとしても利用できる。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** • 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. • 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. •データはデータライフサイクル全体を通じて元の形式で読み取り可能であることが重要である。したがって、ユーザはデータの可読性を維持する必要があり、置き換えられたソフトウェアへのアクセスを維持する必要がある場合がある。 •あるシステムから別のシステムへのデータの移行は、文書化されたプロトコルに従ってコントロールされた方法で実行する必要があり、データの完全な移行の適切な検証を含める必要がある。
3.	**Expectation　期待** 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. レガシーシステムソフトウェアをサポートできなくなった場合は、データのアクセス可能性を目的としてソフトウェアを維持することを検討する必要がある（特定の保持要件に応じて可能な限り長い期間)。 これは、ソフトウェアを仮想環境で維持することによって実現できる。

	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. レガシーデータの経過時間が増加すると、データの「真のコピー」属性を可能な限り保持する代替ファイル形式への移行が必要になる場合がある。 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. 元のデータ機能を完全に使用する移行が技術的に不可能な場合は、リスクと時間の経過に伴うデータの重要性に基づいてオプションを評価する必要がある。移行ファイルの形式は、長期的なアクセス可能性と動的データ機能の低下の可能性（データの取り調べ、傾向分析、再処理など）の間のリスクのバランスを考慮して選択する必要がある。また、リスク評価では、重要な構成設定またはデータの操作に対する不注意または不正な変更に対するシステムの脆弱性も確認する必要がある。リスクを軽減するためのすべてのコントロールを文書化し、その有効性を検証する必要がある。アクセス可能性を維持する必要がある場合、一部の属性や動的データ機能を失うファイル形式への移行が必要になる場合があることが認識されている。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** • 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. •ソフトウェアが仮想環境で保守されている場合は、ソフトウェアを制御するための適切な手段（バリデーションステータス、許可された人によるアクセス制御など）が実施されていることを確認する。 すべてのコントロールを文書化し、その有効性を検証する必要がある。

9.5 System security for computerised systems　コンピュータ化されたシステムのシステムセキュリティ

Item 項目	System security　システムセキュリティ

1.	**Expectation　期待** 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: ユーザクセス制御は、データへの不正アクセス、データへの変更、およびデータの削除を禁止するように構成および実施されるものとする。 セキュリティコントロールの範囲は、コンピュータ化されたシステムの重要度に依存する。 例えば： - 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. - 特定の電子システムにアクセスして利用する必要があるすべてのスタッフに対して、個別のログイン ID とパスワードを設定して割り当てる必要がある。 共有ログイン認証情報では、アクティビティを実行した個人を追跡することはできない。このため、経済的な節約の理由であっても、共有パスワードは禁止する必要がある。ログインプロファイル、構成、およびパスワード形式が明確に定義され、意図したとおりに機能することを確認するために、電子システムのバリデーション中にログインパラメータを検証する必要がある。 - 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. - データの入力およびコンピュータ化された記録への変更は、許可された担当者のみが行う必要がある。 企業は、使用中の各電子システムについて、許可された個人とそのアクセス権限のリストを維持する必要がある。 - Appropriate controls should be in place regarding the format and use of passwords, to ensure that systems are effectively secured. - システムが効果的に保護されるように、パスワードの形式と使用に関して適切なコントロールを行う必要がある。 - Upon initially having been granted system access, a system should allow the user to create a new password, following the normal password rules. - 最初にシステムアクセスが許可されると、システムは、通常のパスワード規則に従って、ユーザが新しいパスワードを作成できるようにする必要がある。 - 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. - システムは異なるユーザクセスロール（レベル）をサポートする必要があり、ロールの割り当ては最小特権ルールに従う必要がある。すなわち、職務に必要な最小限のアクセスレベルを割り当てる必要がある。 少なくとも、単純なシステムには通常のユーザと管理者ユーザが必要であるが、複雑なシステムでは通常、アクセスコントロールを効果的にサポートするために、より多くのレベルのユーザ（階層など）が必要になる。 - 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) - GMP/GDP の重要なアプリケーションの実行に使用されるコンピュータ化されたシステムおよびインフラストラクチャへの管理者アクセス権の付与は、厳密に制御する必要がある。 システム上の通常のユーザに管理者のアクセス権を付与しないこと（すなわち、職務分掌） - Normal users should not have access to critical aspects of the computerised system, e.g. system clocks, file deletion functions, etc. - 通常のユーザは、コンピュータ化されたシステムの重要な側面にアクセスできないようにする必要がある。 システムクロック、ファイル削除機能など。 - 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. - システムは、ユーザ ID や役割など、システムに実際にアクセスできるユーザのリストを生成できる必要がある。 ユーザリストには、特定の個人の識別を可能にする名前または一意の識別子を含める必要がある。 このリストは、定期的なユーザレビュー中に使用する必要がある。 - Systems should be able to generate a list of successful and unsuccessful login attempts, including: o User identification o User access role o Date and time of the attempted login, either in local time or traceable to local time o Session length, in the case of successful logins -システムは、次のような成功および失敗したログイン試行のリストを生成できる必要がある。 o ユーザ ID o ユーザアクセスロール o ログインが試行された日時（現地時間または現地時間まで追跡可能） o ログインに成功した場合のセッションの長さ

	- 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. - ユーザアクセスコントロールは、職務の厳密な分離を保証する必要がある（すなわち、通常の作業タスクを実行しているシステム上のすべてのユーザは、通常のアクセス権のみを持つ必要がある)。 通常、アクセス権が昇格されているユーザ（admin など）は、システムで通常の作業タスクを実行しないこと。 - 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. - システム管理者は通常、タスクを実行するユーザから独立し、電子システムで生成または利用可能なデータの結果に関与または関心を持たないようにする必要がある。 たとえば、QC スーパーバイザーおよびマネージャーは、ラボ内の電子システム（HPLC、GC、UV-Vis など）のシステム管理者として割り当てられないようにする必要がある。 通常、品質および生産組織の外部の個人（情報技術管理者など）は、システム管理者として機能し、強化されたアクセス許可レベルを持っている必要がある。 - 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. - 小規模な組織の場合、品質部門または生産部門の指名された人がシステム管理者としてアクセスを保持することが許可される場合がある。 ただし、これらの場合、管理者アクセスを使用して通常の操作を実行することはできない。そしてユーザは、通常の操作を実行するために 2 番目の制限付きアクセスを保持する必要がある。 このような場合、実施されたすべての管理者の活動は、品質システム内で記録および承認される必要がある。 - 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. - 新規ユーザに対する要求、ユーザの新しい特権は、適切な担当者（ラインマネージャーやシステム所有者など）によって承認され、標準的な手順に従って追跡可能な方法でシステム管理者に転送される必要がある。

	- 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. - GMP/GDP の重要なデータまたは操作へのアクセスを提供するコンピュータ化されたシステムには、非アクティブログアウトが必要である。これは、アプリケーションレベルまたはオペレーティングシステムレベルで、事前定義された時間より長く非アクティブになっているユーザをログアウトする。 時間は長くするのではなく短くする必要があり、通常はシステムへの不正アクセスを防ぐために設定する必要がある。 非アクティブログアウトをアクティブにした場合、システムはユーザに通常の認証手順を実行して再度ログインするように要求する必要がある。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** • 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. •使用中のコンピュータ化されたシステムが保護され、意図的または不注意による変更から保護されるように、会社が合理的な措置を講じていることを確認する。 • 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. •物理的および管理的に保護されていないシステムは、データインテグリティの問題に対して脆弱である。 査察官は、システムのセキュリティを管理する検証済みの手順が存在することを確認し、コンピュータ化されたシステムが検証済みの状態に維持され、操作から保護されていることを確認する必要がある。 • 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. •個々のユーザのログイン ID が使用されていることを確認する。 システム構成で個々のユーザログイン ID の使用が許可されている場合は、これらを使用する必要がある。 • 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. •一部の従来のコンピュータ化されたシステムは、単一のユーザログインまたは限られた数のユーザログインしかサポートされていないものがある。 適切な代替のコンピュータ化されたシステムが利用できない場合、同等のコントロールは、サードパーティのソフ

	トウェア、またはトレーサビリティを提供する紙ベースの方法（バージョン管理を伴う）によって提供される場合がある。 代替システムの適合性は正当化され、文書化されるべきである。 ハイブリッドシステムでは、データレビュの強化が必要になる可能性がある。 • 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. •査察官は、システムが適切なパスワードルールを適用し、強力なパスワードを要求するように、パスワード ポリシーが設定されていることを確認する必要がある。重要なデータを生成または処理するシステムには、より強力なパスワードを使用することを検討する必要がある。 • 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. •ユーザが新しいパスワードを変更できないが、管理者のみが作成できるシステムは、パスワードの機密性を維持できないため、データインテグリティと互換性がない。 • 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. •ユーザクセスレベルが適切に定義され、文書化され、コントロールされていることを確認する。システムではシングルユーザクセスレベルを使用し、すべてのユーザにこのロール（定義上は管理者ロール）を割り当てることはできない。 • 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. •システムが権限チェックを使用し、許可された個人のみがシステムの使用、記録への電子署名、操作またはコンピュータ化されたシステム入力または出力デバイスへのアクセス、記録の変更、または手元の操作の実行ができることを確認する。
2.	**Expectation　期待** 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: コンピュータ化されたシステムは、偶発的な変更や意図的な操作から保護する必要がある。 企業は、システムとその設計を評価し、最終的にデータインテグリティに影響を与える可能性のあるバリデートされた設定への不正な変更を防ぐ必要がある。 以下を考慮する必要がある。 - The physical security of computerised system hardware: o Location of and access to servers;

	o Restricting access to PLC modules, e.g. by locking access panels. o Physical access to computers, servers and media should be restricted to authorised individuals. Users on a system should not normally have access to servers and media. -コンピュータ化されたシステムハードウェアの物理的セキュリティ： o サーバーの場所とアクセス。 o PLC モジュールへのアクセスを制限する。 例、アクセスパネルをロックするなど。 o コンピュータ、サーバー、およびメディアへの物理的なアクセスは、許可された個人に制限する必要がある。 システム上のユーザは通常、サーバーやメディアにアクセスできないようにする必要がある。 - Vulnerability of networked systems from local and external attack; -ローカルおよび外部の攻撃によるネットワークシステムの脆弱性。 - Remote network updates, e.g. automated updating of networked systems by the vendor. -リモートネットワークの更新（： ベンダーによるネットワークシステムの自動更新。 - 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. -システム設定、構成、および主要データのセキュリティ。 システムの重要なデータ/動作パラメータへのアクセスは適切に制限され、設定/構成への変更は、許可された担当者による変更管理プロセスを通じてコントロールされる必要がある。 - The operating system clock should be synchronized with the clock of connected systems and access to all clocks restricted to authorised personnel. -オペレーティングシステムのクロックは、接続されているシステムのクロックと同期し、許可された担当者に制限されているすべてのクロックにアクセスする必要がある。 - Appropriate network security measures should be applied, including intrusion prevention and detection systems. -侵入防止および検出システムを含む、適切なネットワークセキュリティ対策を適用する必要がある。 - 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. -ファイアウォールは、重要なデータと操作を保護するように設定する必要がある。 ポートの開口部（ファイアウォールルール）は、最小特権ポリシーに基づいて、ファイアウォールルールを可能な限り厳しくし、それによってトラフィックのみを許可する必要がある。 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. 規制対象のユーザは、ネットワークセキュリティ対策の継続的な適切性と有効性を定期

	的にレビュし（たとえば、IT インフラストラクチャのネットワーク脆弱性スキャンを使用して潜在的なセキュリティの弱点を特定することにより)、オペレーティングシステムが現在のセキュリティ対策で維持されていることを確認する必要がある。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** • Check that access to hardware and software is appropriately secured, and restricted to authorised personnel. • Verify that suitable authentication methods are implemented. These methods should include user IDs and passwords but other methods are possible and may be required. However, it is essential that users are positively identifiable. • 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. • 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. •ハードウェアとソフトウェアへのアクセスが適切に保護され、許可された担当者に制限されていることを確認する。 •適切な認証方法が実装されていることを確認する。 これらの方法にはユーザ ID とパスワードを含める必要があるが、他の方法も可能であり、必要になる場合がある。ただし、ユーザを明確に識別できることが不可欠である。 •インターネット経由で利用可能な重要なデータを含むシステムへのリモート認証のため、 パスコードトークンや生体認証の使用など、追加の認証技術が採用されていることを確認する。 •システムの主要な運用パラメータへのアクセスが適切に制御されていること、および必要に応じて、システムが GMP/GDP ステップの重要なシーケンスでイベントとパラメータの正しい順序を適用していることを確認する。
3.	**Expectation　期待** Network protection　ネットワーク保護 Network system security should include appropriate methods to detect and prevent potential threats to data. ネットワークシステムのセキュリティには、データに対する潜在的な脅威を検出して防止するための適切な方法を含める必要がある。 The level of network protection implemented should be based on an assessment of data risk. 実装されるネットワーク保護のレベルは、データリスクの評価に基づく必要がある。 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. ファイアウォールは、不正アクセスを防止するために使用する必要がある。また、そのルールは、許可されたトラフィックのみを許可し、必要に応じて制限されるように設定するために、仕様に対する定期的なレビュを受ける必要がある。レビュは文書化する必要がある。 Firewalls should be supplemented with appropriate virus-protection or intrusion prevention/detection systems to protect data and computerised systems from attempted attacks and malware. ファイアウォールは、攻撃やマルウェアの試みからデータとコンピュータ化されたシステムを保護するために、適切なウイルス対策または侵入防止/検出システムで補完する必要がある。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** •Inadequate network security presents risks associated with vulnerability of systems from unauthorised access, misuse or modification. •Check that appropriate measures to control network access are in place. Processes should be in place for the authorisation, monitoring and removal of access. •Systems should be designed to prevent threats and detect attempted intrusions to the network and these measures should be installed, monitored and maintained. •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 rulesmay become obsolete permitting unwanted traffic or intrusions. •不十分なネットワークセキュリティは、不正アクセス、誤用、または変更によるシステムの脆弱性に関連するリスクをもたらす。 •ネットワークアクセスをコントロールするための適切な対策が講じられていることを確認する。アクセスの承認、モニタリング、および削除のためのプロセスを実施する必要がある。 •システムは、脅威を防止し、ネットワークへの侵入の試みを検出するように設計する必要があり、これらの対策をインストール、モニタリング、および維持する必要がある。 •ファイアウォールルールは通常、サーバーなどのメンテナンスによるポートの一時的な開放など、時間の経過とともに変更される可能性がある。確認を行わない場合、ファイアウォールルールが廃止され、不要なトラフィックや侵入が許可される可能性がある。

4.	**Expectation　期待** 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). 手書きの署名の代わりに使用される電子署名には、記録に電子署名した特定の人物に対する信頼性とトレーサビリティを確保するための適切なコントロールが必要である。 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. 電子署名は、それぞれの記録に永続的にリンクする必要がある。たとえば、署名された記録に後で変更が加えられた場合、 記録は修正を示し、符号なしとして表示される必要がある。 Where used, electronic signature functionality should automatically log the date and time when a signature was applied. 使用する場合、電子署名機能は、署名が適用された日時を自動的にログに記録する必要がある。 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. 高度な形式の電子署名の使用がより一般的になりつつある（たとえば、バイオメトリクスの使用が企業によってより普及している)。 高度な形式の電子署名の使用を推奨する必要がある。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** •Check that electronic signatures are appropriately validated, their issue to staff is controlled and that at all times, electronic signatures are readily attributable to an individual. •Any changes to data after an electronic signature has been assigned should invalidate the signature until the data has been reviewed again and re-signed. •電子署名が適切にバリデートされ、スタッフへの発行がコントロールされていること、および電子署名が常に個人に帰属していることを確認する。 •電子署名が割り当てられた後のデータへの変更は、データが再確認されて再署名されるまで署名を無効にする必要がある。

5.	**Expectation　期待** Restrictions on use of USB devices　USB デバイスの使用に関する制限 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. システムのセキュリティ上の理由から、コンピュータ化されたシステムは、GMP/GDP の重要なデータをホストするコンピュータクライアントおよびサーバーで USB メモリスティックおよびストレージデバイスを使用することによる脆弱性を防ぐように構成する必要がある。 必要に応じて、承認された目的でのみポートを開き、使用する前にすべての USB デバイスを適切にスキャンする必要がある。 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. セキュリティ侵害を防止するために GMP/GDP データをホストする企業のコンピュータクライアントおよびサーバーでのプライベート USB デバイス（フラッシュドライブ、カメラ、スマートフォン、キーボードなど）の使用、またはプライベートコンピュータでの企業の USB デバイスの使用をコントロールする必要がある。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** •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. •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. •これは、USB デバイスが別の外部デバイス(キーボードなど)を装ってコンピュータをだますことを可能にするオペレーティングシステムの脆弱性が知られている場合に特に重要であり、実行可能コードを含んで開始することができる。 •そのようなデバイスの使用を許可されたユーザに制限するコントロールを講じ、使用前に USB デバイスをスクリーニングするための措置を講じる必要がある。

9.6　Audit trails for computerised systems　コンピュータ化されたシステムの監査証跡

Item 項目	Audit Trails　監査証跡
1.	**Expectation　期待** 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. コンピュータ化されたシステムを購入して実装する時には、データマネジメントおよびインテグリティの要件を考慮する必要がある。 企業は、適切な電子監査証跡機能を含むソフトウェアを選択する必要がある。 Companies should endeavour to purchase and upgrade older systems to implement software that includes electronic audit trail functionality. 企業は、電子監査証跡機能を含むソフトウェアを実装するために、古いシステムの購入およびアップグレードを行う必要がある。 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. 一部の非常に単純なシステムには適切な監査証跡がないことが認められている。 ただし、、データの真実性を検証するための代替の取り決めとして、例えば、管理手順、二次的なチェックおよびコントロールを実施する必要がある。ハイブリッドシステムに関する追加のガイダンスは、セクション 9.10 に記載されている。 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. システムの検証中に監査証跡機能を検証して、各手動アクティビティに関連する重要なデータのすべての変更と削除が記録され、ALCOA +の原則を満たしていることを確認する必要がある。 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: 規制対象のユーザは、システム内の監査証跡の性質と機能を理解し、適格性確認中に異なる監査証跡の評価を実行し、各監査証跡の GMP/GDP 関連性を判断し、重要な GMP/GDP 関連データの監査証跡の正しい管理と構成を確保する必要がある。 この演習は、定義された頻度でレビュするために、どの特定のトレイルとトレイル内のどのエントリが重要であるかを判断する上で重要である。 たとえば、このような評価監査証跡のレビュに続いて、以下に焦点を当てることができる。 - Identifying and reviewing entries/data that relate to changes or modification of data. - Review by exception – focusing on anomalous or unauthoried activities. - Systems with limitations that allow change of parameters/data or where activities are left open to modification - 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 -データの変更または修正に関連するエントリ/データを特定して確認する。 -例外によるレビュ–異常または非承認のアクテビティに焦点を当てる。 -パラメータ/データの変更を許可する制限があるシステム、またはアクティビティが変更可能なままになっているシステム -注：パラメータ/データの変更を防止する権限設定を備えた、または構成設定の変更を防止するアクセス制限を備えた適切に設計されたシステムでは、関連する監査証跡を詳細に調べる必要がない場合がある。 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. 監査証跡機能は常に有効にしてロックする必要があり、機能を非アクティブ化、削除、または変更できないようにする必要がある。 管理ユーザが監査証跡機能を非アクティブ化、削除、または変更できる場合は、監査証跡に自動エントリを作成し、このことが発生したことを示す必要がある。 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. 企業は、ポリシーとプロセスの概要を説明する手順を実装し、監査証跡に必要なデータを決定し、リクマネジメントの原則に従って監査証跡を確認する必要がある。各操作に関連する重要な監査証跡は、重要なデータとその変更が受け入れられることを確認するために、操作に関連する他のすべての記録とともに、操作の完了（たとえば、バッチリリースの前に）を確認する前に、個別に確認する必要がある。このレビュは、元の部門が実行する必要があり、必要に応じて自己点検または調査活動中に品質部門によって検証される必要がある。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** •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. •Verify that audit trails are regularly reviewed (in accordance with quality risk management principles) and that discrepancies are investigated. •If no electronic audit trail system exists a paper based record to demonstrate changes to

	data may be acceptable until a fully audit trailed (integrated system or independent audit software using a validated interface) system becomes available. These hybrid systems are permitted, where they achieve equivalence to integrated audit trail, such as described in Annex 11 of the PIC/S GMP Guide. •Failure to adequately review audit trails may allow manipulated or erroneous data to be inadvertently accepted by the Quality Unit and/or Authorised Person. •Clear details of which data are critical, and which changes and deletions should be recorded (audit trail) should be documented. •バリデーション文書は、監査証跡が機能していること、およびシステム内のすべてのアクティビティ、変更、およびその他のトランザクションが、関連するすべてのメタデータとともに記録されていることを実証する必要がある。 •監査証跡が定期的にレビュされ（品質リスクマネジメントの原則に従って)、不一致が調査されていることを確認する。 •電子監査証跡システムが存在しない場合、完全な監査証跡（統合システムまたはバリデートされた済みインターフェースを使用する独立した監査ソフトウェア）システムが利用可能になるまで、データの変更を示す紙ベースの記録が受け入れられる場合がある。これらのハイブリッドシステムは。PIC/S GMP ガイドの付録 11 に記載されているように、統合された監査証跡と同等性を達成する場合に許可されている。 •監査証跡を適切にレビュしない場合、操作されたデータや誤ったデータが品質部門や権限のある人物によって誤って受け入れられる可能性がある。 •重要なデータ、および記録する変更と削除（監査証跡）の詳細を明確に文書化する必要がある。
2.	**Expectation　期待** 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. 可能な場合は、電子ベースのシステムの監査証跡機能を適切に評価および構成し、監査目的でのデータの取得、削除、上書き、および変更に関連する重要なアクティビティを把握する必要がある。 Audit trails should be configured to record all manually initiated processes related to critical data. 監査証跡は、重要なデータに関連する手動で開始されたすべてのプロセスを記録するように構成する必要がある。 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. システムは、電子記録を作成、変更、または削除するエントリとアクションの日時を個別に記録するために、安全なコンピュータ生成のタイムスタンプ付き監査証跡を提供する必要がある。

	The audit trail should include the following parameters: - details of the user that undertook the action; - what action occurred, was changed, incl. old and new values; - when the action was taken, incl. date and time ; - why the action was taken (reason); and - in the case of changes or modifications to data, the name of any person authorising the change. 監査証跡には、次のパラメータを含める必要がある。 -アクションを実行したユーザの詳細。 -どのようなアクションが発生し、変更されたか。 古い値と新しい値を含む。 -アクションが実行されたとき。日時を含む ; -なぜアクションが実行されたか（理由）; そして -データの変更または修正の場合、変更を承認した人の名前。 The audit trail should allow for reconstruction of the course of events relating to the creation, modification, or deletion of an electronic record. 監査証跡は、電子記録の作成、変更、または削除に関連する一連のイベントの再構築を可能にする必要がある。 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. システムは、監査証跡の電子コピーを印刷して提供できる必要があり、、システムでオンラインまたはハードコピーで表示する場合でも、監査証跡は意味のある形式で使用できる必要がある。 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). 可能であれば、監査証跡は、コンピュータ化されたシステムに見られる動的な機能（たとえば、検索機能やスプレッドシートなどにデータをエクスポートする機能）を保持する必要がある。 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：監査証跡を、PQS の下で適切にコントロールおよび承認するために変更が必要になる可能性がある変更管理システムと混同しないこと。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** •Verify the format of audit trails to ensure that all critical and relevant information is captured. •The audit trail should include all previous values and record changes should not overwrite or obscure previously recorded information. •Audit trail entries should be recorded in true time and reflect the actual time of activities.

	Systems recording the same time for a number of sequential interactions, or which only make an entry in the audit trail, once all interactions have been completed, may not 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. •監査証跡の形式を確認して、重要で関連性のあるすべての情報が確実に取得されるようにする。 •監査証跡には以前のすべての値が含まれている必要があり、記録の変更によって以前に記録された情報が上書きまたは不明瞭にならないようにする必要がある。 •監査証跡のエントリは、実際の時間に記録され、実際の活動時間を反映する必要がある。多数の連続したインタラクションを同時に記録するシステム、またはすべてのインタラクションが完了後に監査証跡にのみエントリを作成するシステムは、例えば 混合容器へ 4 つの原材料を追加する電子記録のために、各個別の相互作用または配列が重要な場合、データインテグリティに対する期待に準拠していない可能性がある。追加の順序が重要なプロセス パラメータ（CPP）である場合は、各追加をタイムスタンプと共に個別に記録する必要がある。

9.7 Data capture/entry for computerised systems コンピュータ化されたシステムのデータキャプチャ/入力

Item 項目	Data capture/entry データキャプチャ/入力
1.	**Expectation 期待** Systems should be designed for the correct capture of data whether acquired through manual or automated means. システムは、手動または自動のいずれの方法で取得した場合でも、データを正しくキャプチャできるように設計する必要がある。 For manual entry: - The entry of critical data should only be made by authorised individuals and the system should record details of the entry, the individual making the entry and when the entry was made. - Data should be entered in a specified format that is controlled by the software, validation activities should verify that invalid data formats are not accepted by the system. - All manual data entries of critical data should be verified, either by a second operator, or by a validated computerised means. - Changes to entries should be captured in the audit trail and reviewed by an appropriately authorised and independent person. 手動入力の場合： -重要なデータの入力は、許可された個人のみが行う必要があり、システムは、入力の詳

	細、入力を行った個人、および入力が行われた日時を記録する必要がある。 -データは、ソフトウェアによって制御される指定された形式で入力する必要があるバリデーションアクティビティでは、無効なデータ形式がシステムによって受け入れられないを確認する必要がある。 -重要なデータの手動データ入力はすべて、2 番目のオペレーター、またはバリデート済のコンピュータ化された手段のいずれかによって検証する必要がある。 -エントリへの変更は、監査証跡に記録され、適切に権限を与えられた独立した人物によってレビュされる必要がある。 For automated data capture: (refer also to table 9.3) - The interface between the originating system, data acquisition and recording systems should be validated to ensure the accuracy of data. - Data captured by the system should be saved into memory in a format that is not vulnerable to manipulation, loss or change. - The system software should incorporate validated checks to ensure the completeness of data acquired, as well as any relevant metadata associated with the data. 自動データキャプチャの場合:(表 9.3 も参照) -データの正確性を確保するために、元のシステム、データ取得、および記録システム間のインターフェースを検証する必要がある。 -システムによってキャプチャされたデータは、操作、損失、または変更に対して脆弱ではない形式でメモリに保存する必要がある。 -システムソフトウェアには、取得したデータインテグリティと、データに関連付けられた関連メタデータを確認するためのバリデート済みチェックを組み込む必要がある。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** •Ensure that manual entries of critical data made into computerised systems are subject to an appropriate secondary check. •Validation records should be reviewed for systems using automated data capture to ensure that data verification and integrity measures are implemented and effective, e.g. verify whether an auto save function was validated and, therefore, users have no ability to disable it and potentially generate unreported data. •コンピュータ化されたシステムに作成された重要なデータの手動入力が適切な二次チェックの対象となることを確認する。 •自動データキャプチャを使用するシステムのバリデーション記録を確認して、データの検証とインテグリティの測定が実装され、効果的であることを確認する必要がある。例えば、自動保存機能が検証されているかどうかを確認し、それにより、ユーザが自動保存機能を無効にし、レポートされないデータを生成することができなくなる。
2.	**Expectation　期待** Any necessary changes to data should be authorised and controlled in accordance with

	approved procedures. データに必要な変更はすべて、承認された手順に従って承認およびコントロールする必要がある。 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. たとえば、手動による統合と査察結果の再処理は、承認されコントロールされた方法で実行する必要がある。 企業の品質部門は、データの変更が必要な場合にのみ、指定された個人によって実行されるようにするための対策を確立する必要がある。 元の（変更されていない）データは、元のコンテキストで保持する必要がある。 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. 生データに対するすべての変更および修正は完全に文書化され、少なくとも 1 人の適切な訓練を受けた資格のある個人によってレビュおよび承認される必要がある。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** •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. •データの修正または再処理をコントロールするための適切な手順が存在することを確認する。 証拠は、提案された変更、コントロール/制限/定義された変更、および行われた変更の正式なレビュに対する正式な承認の適切なプロセスを実証する必要がある。

9.8 Review of data within computerised systems　コンピュータ化されたシステム内のデータのレビュ

Item 項目	Review of electronic data　電子データのレビュ
1.	**Expectation　期待** 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. 規制対象のユーザは、コンピュータ化されたシステムによって生成されたすべての GMP/GDP 関連の電子データ、およびデータの重要性を特定するために、リスク評価を実行する必要がある。特定された重要なデータは、規制対象のユーザが監査し、操作が

	正しく実行され、電子記録の元の情報に対して変更（変更、削除、上書き）が行われたかどうか、または関連する未報告のデータが生成されたかどうかを確認する必要がある。すべての変更は正式に承認されている必要がある。 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 は、2 番目のオペレーターがデータをチェックするプロセスを説明する必要がある。 これらの SOP は、レビュされる重要な生データ、データ要約のレビュ、関連するログブックとハードコピー記録のレビュの概要を示し、レビュがどのように実行、記録、承認されるかを説明する必要がある。 The review of audit trails should be part of the routine data review within the approval process. 監査証跡のレビュは、承認プロセス内の定期的なデータレビュの一部である必要がある。 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. 監査証跡レビュの頻度、役割、および責任は、コンピュータ化されたシステムに記録されたデータの GMP/GDP 関連値に従ったリスク評価に基づく必要がある。 たとえば、医薬品の品質に直接影響を与える可能性のある電子データの変更については、データが重要な決定を行うために信頼されるポイントの前に、監査証跡を確認することが期待される。 例えば、バッチリリース。 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. 規制対象のユーザは、監査証跡のレビュ方法、検索対象、検索の実行方法などを詳細に説明する SOP を確立する必要がある。本手順では、監査証跡レビュの担当者が従う必要のあるプロセスを詳細に決定する必要がある。 監査証跡のレビュ活動は文書化して記録する必要がある。 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. 監査証跡のレビュ中に見つかった予想結果からの大幅な変動は、完全に調査して記録する必要がある。 手順では、監査証跡のレビュにより、医薬品の品質またはデータのインテグリティに影響を与える可能性のある重大な問題が特定された場合に実行するアクシ

	ョンを説明する必要がある。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** •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. •Where data summaries are used for internal or external reporting, evidence should be available to demonstrate that such summaries have been verified in accordance with raw data. •Check that 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. •Where global systems are used, it may be necessary for date and time records to include a record of the time zone to demonstrate contemporaneous recording. •Check that known changes, modifications or deletions of data are actually recorded by the audit trail functionality. •ローカルの手順をチェックして、電子データがその重要度（製品の品質や意思決定への影響）に基づいてレビュされていることを確認する。 各レビュの証拠は記録され、査察官が利用できるようにする必要がある。 •データの要約が内部または外部の報告に使用される場合、そのような要約が生データに従って検証されたことを示す証拠が利用可能である必要がある。 •規制対象の当事者が、二次レビュと監査証跡レビュを実行する方法の手順と、レビュの過程で問題が見つかった場合に実行する手順の概要を示す詳細な SOP を持っていることを確認する。 •グローバルシステムが使用されている場合、同時記録を示すために、日付と時刻の記録にタイムゾーンの記録を含める必要がある場合がある。 •データの既知の変更、修正、または削除が実際に監査証跡機能によって記録されていることを確認する。
2.	**Expectation　期待** 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. 企業の品質部門は、現在のコントロールの効果的な実装を検証し、潜在的な非準拠の問題を検出するために、重要度とシステムの複雑さに基づいて監査証跡の継続的なレビュを実施するプログラムとスケジュールを確立する必要がある。 これらのレビュは、企業の自己点検プログラムに組み込む必要がある。 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. 必要に応じて上級経営陣および国内当局に通知するためのエスカレーションプロセスを含む、監査証跡の不一致に対処および調査するための手順を実施する必要がある。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** •Verify that self-inspection programs incorporate checks of audit trails, with the intent to verify the effectiveness of existing controls and compliance with internal procedures regarding the review of data. •Audit trail reviews should be both random (selected based on chance) and targeted (selected based on criticality or risk). •自己点検プログラムに監査証跡のチェックが組み込まれていることを確認する。これは、既存のコントロールの有効性と、データのレビュに関する内部手順への準拠を確認することを目的としている。 •監査証跡のレビュは、ランダム（偶然に基づいて選択）とターゲット（重要度またはリスクに基づいて選択）の両方である必要がある。

9.9 Storage, archival and disposal of electronic data 電子データの保存、アーカイブ、廃棄

Item 項目	Storage, archival and disposal of electronic data 電子データの保存、アーカイブ、廃棄
1.	**Expectation 期待** Storage of data should include the entire original data and all relevant metadata, including audit trails, using a secure and validated process. データの保存には、安全でバリデートされたプロセスを使用して、元のデータ全体と、監査証跡を含むすべての関連メタデータを含める必要がある。 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: -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. -Stored data should be accessible in a fully readable format. Companies may need to maintain suitable software and hardware to access electronically stored data backups or copies during the retention period -Routine backup copies should be stored in a remote location (physically separated) in the event of disasters. -Back-up data should be readable for all the period of the defined regulatory retention period, even if a new version of the software has been updated or substituted for one with better performance. -Systems should allow backup and restoration of all data, including meta-data and audit trails. データがバックアップ、またはコピーが作成される場合、データへの不正アクセス、データの変更、削除、またはそれらの変更を禁止するために、バックアップとコピーにも同じ適切なレベルのコントロールが必要である。たとえば、ポータブルハードドライブにデータをバックアップする企業は、ハードドライブからデータを削除する機能を禁止する必要がある。データの保存とバックアップに関するその他の考慮事項は次のとおりである。 -動的電子レコードの真のコピーは、コンテンツ全体(すべてのデータとすべての関連メタデータが含まれている)と元のレコードの意味が保持されることを期待して、作成することができる。 -保存されたデータは、完全に読み取り可能な形式でアクセスできる必要がある。企業は、保存期間中に電子的に保存されたデータのバックアップまたはコピーにアクセスするために、適切なソフトウェアとハードウェアを維持する必要がある場合がある -災害が発生した場合に備えて、定期的なバックアップコピーを離れた場所（物理的に分離した場所）に保存する必要がある。 -バックアップデータは、ソフトウェアの新しいバージョンが更新された場合や、パフォーマンスが向上したものに置き換えられた場合でも、定義された規制保持期間のすべての期間にわたり読み取り可能である必要がある。 -システムは、メタデータと監査証跡を含むすべてのデータのバックアップと復元が可能である必要がある。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** •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. •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. •Check that data associated with superseded or upgraded systems is managed appropriately

	and is accessible. •データストレージ、バックアップ、およびアーカイブシステムが、すべてのデータと関連するメタデータをキャプチャするように設計されていることを確認する。これらのシステムがバリデートされ、検証されたという証拠を文書化する必要がある。 •キャプチャされるメタデータの範囲はリスクマネジメントの原則に基づく必要があり、ユーザはアクティビティまたはプロセスの再構築に重要なすべてのメタデータがキャプチャされるようにする必要がある。 •置き換えられたまたはアップグレードされたシステムに関連するデータが適切に管理され、アクセス可能であることを確認する。
2.	**Expectation　期待** 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. 記録保持手順には、メタデータを保持するための規定を含める必要がある。 これにより、将来のクエリまたは調査で、バッチに関連して発生したアクティビティを再構築できる。
3.	**Expectation　期待** 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. データは定期的にバックアップし、書面による手順に従ってアーカイブする必要がある。アーカイブコピーは、バックアップおよび元のデータが保存されている場所とは別の離れた場所に物理的に（または関連する場合は仮想的に）保護する必要がある。 The data should be accessible and readable and its integrity maintained for all the period of archiving. データはアクセス可能で読み取り可能であり、アーカイブのすべての期間にわたってそのインテグリティが維持されている必要がある。 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. 調査が必要な場合に備えて、アーカイブされたデータを復元するための手順を用意する必要がある。 アーカイブされたデータを復元するための手順は、定期的にテストする必要がある。 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. アーカイブプロセスに施設が必要な場合は、意図的または不注意による変更や損失から記録を確実に保護するために、特定の環境管理と許可された担当者のアクセスのみを実装する必要がある。 データへの長期アクセスの問題が想定されるために、施設内のシステムを廃止する必要がある場合、手順はアーカイブされたデータの継続的な可読性を保証する必要がある。 たとえば、データを別のシステムに転送するように設定できる。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** •There is a risk with archived data that access and readability of the data may be lost due to software application updates or superseded equipment. Verify that the company has access to archived data, and that they maintain access to the necessary software to enable review of the archived data. •Where external or third party facilities are utilised for the archiving of data, these service providers should be subject to 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. •アーカイブされたデータには、ソフトウェアアプリケーションの更新や機器の置き換えにより、データへのアクセスと可読性が失われるリスクがある。企業がアーカイブデータにアクセスできること、およびアーカイブデータのレビュを可能にするために必要なソフトウェアへのアクセスを維持していることを確認する。 •外部またはサードパーティの施設がデータのアーカイブに利用される場合、これらのサービスプロバイダーは評価の対象となり、すべての責任は品質技術協定に記録される。契約書と評価記録をチェックして、アーカイブされた記録のインテグリティを確保するために十分な考慮が払われていることを確認する。
4.	**Expectation　期待** It should be possible to print out a legible and meaningful record of all the data generated by a computerised system (including metadata). コンピュータ化されたシステムによって生成されたすべてのデータ（メタデータを含む）の読みやすく意味のある記録を印刷できるはずである。 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. 記録に変更が加えられた場合、記録の変更も印刷し、元のデータがいつどのように変更されたかを示す必要がある。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** •Check validation documentation for systems to ensure that systems have been validated for the generation of legible and complete records. •Samples of print-outs may be verified. •システムのバリデーションドキュメントを調べ、読みやすく完全な記録の生成について

	システムがバリデートされていることを確認する。 •プリントアウトのサンプルが検証される場合がある。
5.	**Expectation　期待** 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. 電子的に保存されたデータの廃棄プロセスを説明する手順を実施する必要がある。 これらの手順では、データの評価と保存期間の割り当てに関するガイダンスを提供し、不要になったデータの廃棄について説明する必要がある。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** •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. •手順でデータの廃棄条件が明確に規定され、ライフサイクル中に必要なデータが誤って廃棄されないように注意が払われていることを確認すること。

9.10　Management of Hybrid Systems　ハイブリッドシステムの管理

Item 項目	Management of Hybrid Systems　ハイブリッドシステムの管理
1.	**Expectation　期待** 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. ハイブリッドシステムは、その複雑さとデータ操作に対する潜在的な脆弱性の増加を反映して、特定の追加のコントロールを必要とする。 このため、ハイブリッドシステムの使用は推奨されておらず、そのようなシステムは可能な限り交換する必要がある。 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. ハイブリッドシステムの各要素は、上記で指定された手動およびコンピュータ化されたシステムに関連するガイダンスに従って適格化およびコントロールする必要がある。 Appropriate quality risk management principles should be followed when assessing, defining, and demonstrating the effectiveness of control measures applied to the system. システムに適用されるコントロール手段の有効性を評価、定義、および実証するときは、適切な品質リスクマネジメントの原則に従う必要がある。 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.

	システム全体の詳細なシステム記述では、システムのすべての主要コンポーネント、各コンポーネントの機能、データマネジメントとインテグリティのコントロール、およびシステムコンポーネントが相互作用する方法を概説する必要がある。 Procedures and records should be available to manage and appropriately control the interface between manual and automated systems, particularly steps associated with: -manual input of manually generated data into computerised systems; -transcription (including manual) of data generated by automated systems onto paper records; and -automated detection and transcription of printed data into computerised systems. 手動システムと自動システムの間のインターフェース、特に以下に関連するステップを管理および適切にコントロールするための手順と記録が利用可能である必要がある。 -手動で生成されたデータをコンピュータ化されたシステムに手動で入力する。 -自動システムによって生成されたデータの書き起こし（手動を含む）を紙の記録へ転記する。および -印刷データを自動検出し、コンピュータ化されたシステムへ転記する。
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** •Check that hybrid systems are clearly defined and identified, and that each contributing element of the system is validated. •Attention should be paid to the interface between the manual and computerised system. Inspectors should verify that adequate controls and secondary checks are in place where manual transcription between systems takes place. •Original data should be retained following transcription and processing. •Hybrid systems commonly consist of a combination of computerised and manual systems. Particular attention should be paid to verifying: o The extent of qualification and/or validation of the computerised system; and, o 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. •ハイブリッドシステムが明確に定義および特定されており、システムの各要素がバリデートされていることを確認する。 •手動システムとコンピュータ化されたシステムの間のインターフェースに注意を払う必要がある。 査察官は、システム間の手動転記が行われる場所で、適切なコントロールと二次チェックが実施されていることを確認する必要がある。 •元のデータは、転記および処理後に保持する必要がある。 •ハイブリッドシステムは通常、コンピュータ化されたシステムと手動のシステムの組み合わせで構成される。 以下の検証には特に注意を払う必要がある。 o コンピュータ化されたシステムの適格性および/またはバリデーションの範囲。 および、 o 手動プロセスの一貫した適用が困難なため、ハイブリッドシステムの手動要素の管理に適用されるコントロールの堅牢性。

2.	**Expectation　期待** 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: -Instructions for how electronic data and paper-based data is correlated to form a complete record. -Expectations for approval of data outputs for each system. -Risks identified with hybrid systems, with a focus on verification of the effective application of controls 電子データおよび紙ベースのデータの評価と承認のプロセスを明確に概説する、ハイブリッドシステムによって生成されたデータのレビュを管理するための手順を実施する必要がある。 手順の概要は次のとおりである。 -完全な記録を形成するために電子データと紙ベースのデータをどのように関連付けるかについての指示。 -各システムのデータ出力の承認への期待。 -制御の効果的な適用の検証に焦点を当てた、ハイブリッドシステムで特定されたリスク
	Potential risk of not meeting expectations/items to be checked **期待/チェックすべき項目を満たさない潜在的なリスク** •Verify that instructions for the review of hybrid system data is in place. •ハイブリッドシステムデータのレビュ手順が整っていることを確認する。

10. DATA INTEGRITY CONSIDERATIONS FOR OUTSOURCED ACTIVITIES
外部委託された活動に関するデータインテグリティに関する考慮事項

10.1 General supply chain considerations　一般的なサプライチェーンの考慮事項

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.

現代のサプライチェーンは、多くの場合、医薬品の安全で継続的な供給を確保するために協力する複数のパートナー企業で構成されている。 一般的なサプライチェーンでは、API 生産者、剤形製造業者、分析研究所、卸売業者および流通組織の関与が必要であり、多くの場合、さまざまな組織や場所からの関与が必要である。 これらのサプライチェーンは、多くの場合、外部委託サービス、IT サービスとインフラストラクチャ、専門知識、またはコンサルティングサービスを提供する追加の組織によってサポートされている。

10.1.2

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.

データインテグリティは、サプライチェーンのセキュリティとインテグリティを確保する上で重要な役割を果たす。委託者によるデータガバナンス対策は、サプライチェーンパートナーが提供さする信頼性の低いまたは偽造されたデータまたは資料によって大幅に弱体化する可能性がある。 この原則は、原材料のサプライヤ、委託製造業者、分析サービス、卸売業者、委託サービスプロバイダー、コンサルタントを含むすべての外部委託活動に適用される。

10.1.3

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

サプライチェーンパートナーとアウトソーシング活動の初期および定期的な再認定には、データインテグリティリスクと適切なコントロール措置の考慮を含める必要がある。

10.1.4

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.

組織は、サプライチェーンから取得した情報(例えば、要約記録とコピー/印刷物)のデータインテグリティの制限およびリモート監視の課題を理解することが重要である。これらの制限は、本ガイダンスのセクション 8.11 で説明されている制限と同様である。 これは、品質リスクマネジメントアプローチを使用して、データインテグリティの検証と監視にリソースを集中させるのに役立つ。

10.2 Routine document verification 定期的なドキュメントの検証

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.

サプライチェーンは、ある組織から別の組織に渡されるドキュメントとデータの使用に依存している。 委託者が報告された結果に関連するすべての生データを確認することは、多くの場合、現実的ではない。 品質リスクマネジメントの原則を使用して、外部委託業者および請負業者の堅牢な適格性プロセスに重点を置く必要がある。

10.3 Strategies for assessing data integrity in the supply chain サプライチェーンにおけるデータインテグリティを評価するための戦略

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: •The outcome of site audits, with focus on data governance measures •Demonstrated compliance with international standards or guidelines related to data integrity and security •Review of data submitted in routine reports, for example:

企業は、必要なデータインテグリティのコントロールの範囲を評価するサプライチェーンとアウトソーシング活動のリスクレビュを定期的に実施する必要がある。 このようなレビュの頻度は、リスクマネジメントの原則を使用し、契約受諾者が提供するサービスの重要度に基づく必要がある。リスクレビュ中に考慮される情報には次のものが含まれる。
•データガバナンス対策に焦点を当てたサイト監査の結果
•データインテグリティとセキュリティに関連する国際標準またはガイドラインへの準拠の実証
•定期的なレポートで提出されたデータのレビュ。例：

Area for review　レビュエリア	Rationale　理論的根拠
Comparison of analytical data reported by the contractor or supplier vs in-house data from analysis of the same material 請負業者またはサプライヤによって報告された分析データと同じ材料の分析からの社内データの比較	To look for discrepant data which may be an indicator of falsification 改ざんの指標となり得る矛盾するデータを探す

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.

材料の製造業者と供給業者、サービスプロバイダー、医薬品製造受託機関（CMO)、および（流通の場合）医薬品の供給業者の間で品質協定（または同等のもの）を締結し、サプライチェーン全体でデータインテグリティを確保するための特定の規定を設ける必要がある。 これは、データガバナンスへの期待を設定し、契約の受諾者から委託者に報告する透過的なエラー/逸脱を設定することによって達成される可能性がある。
また、契約アクセプターサイトで特定されたデータインテグリティの障害について、委託者に通知する必要がある。

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.

製造業者（または第三者が代理として）が実施する、API のサプライヤと製造業者、重要な中間サプライヤ、一次および印刷包装材料サプライヤ、委託製造業者、およびサービスプロバイダーの監査には、契約組織におけるデータインテグリティ対策の検証を含める必要がある。契約の受諾者は、監査中に契約の提供者に代わって生成されたデータへの合理的なアクセスを提供することが期待され、これにより、データインテグリティとマネジメントの原則への準拠を評価および実証できる。

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:

監査と定期的な監視には、品質リスクマネジメントアプローチを使用した、委託者の品質部門によるソース電子データとメタデータの適切な検証を含める必要がある。これは、次のような手段によって達成される可能性がある。

Site audit サイト監査	Review the contract acceptors organisational behaviour, and understanding of data governance, data lifecycle, risk and criticality. 契約アクセプターの組織行動を確認し、データガバナンス、データライフサイクル、リスク、および重要性を理解する。
Material testing vs CoA 材料試験と 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. 分析テストの結果とサプライヤが報告した CoA を比較する。精度、精度、または純度の結果の不一致を調べる。これは、材料およびサプライヤのリスクに応じて、日常的に、定期的に、または予告なしに実行される場合がある。必要に応じて、サンプルの定期的な検査（proficiency testing）を検討することができる。
Remote data review リモートデータレビュ	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. 委託者は、バッチ製造およびテストで使用するために、契約施設/サプライヤに独自のハードウェアおよびソフトウェアシステム（ワイドエリアネットワーク上に展開）の使用を提供することを検討できる。

	契約提供者は、契約施設の担当者によって生成されたデータの品質とインテグリティをリアルタイムでモニタリングできる 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. この状況では、委託者がデータをモニタリングしても、契約受諾者が生成したデータの修正が提供されないようにするために、職務を分離する必要がある。
Quality monitoring 品質モニタリング	Quality and performance monitoring may indicate incentive for data falsification (e.g. raw materials which marginally comply with specification on a frequent basis.) 品質と性能のモニタリングは、データの改ざんのインセンティブを示している可能性がある。(たとえば、仕様の準拠に対しわずかな変動が頻繁にある原材料)

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.

委託者は、契約受諾者と協力して、すべてのクライアントの機密情報がエンコードされ、クライアントの匿名化が行われるようにすることができる。 これにより、他のクライアントに対する守秘義務を破ることなく、委託者のサイトでソースの電子データとメタデータのレビュが容易になる。より大きなデータセットを確認することにより、契約受諾者のデータガバナンス対策をより堅牢に評価できるようになる。 また、繰り返されるデータセットや予期される変動性を示さないデータなど、データインテグリティ障害の指標を検索も可能である。

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.

提供された文書の真正性と正確性を確保するように注意する必要がある（セクション 8.11 を参照)。 請負業者とサプライチェーンの資格を決定する際には、「真のコピー」と「要約レポート」データのデータインテグリティとトレーサビリティのリスクの違いを考慮する必要がある。

11. REGULATORY　ACTIONS IN RESPONSE TO DATA INTEGRITY FINDINGS データインテグリテ

ィに関する調査結果に応じた規制措置

11.1 Deficiency references 欠陥の参照

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.

データインテグリティは適正製造基準の基本であり、適切なデータマネジメントの要件は、医薬品の GMP/GDP に関する現在の PIC/S ガイドに組み込まれている。 次の表は、これらの既存の要件のいくつかを強調する参照ポイントを示している。

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:
Attributable	[4.20, c & f], [4.21, c & i], [4.29 point 5]	[5.43], [6.14], [6.18], [6.52]	[2], [12.1], [12.4], [15]	[4.2.4], [4.2.5]
Legible	[4.1], [4.2], [4.7], [4.8], [4.9], [4.10]	[6.11], [6.14], [6.15], [6.50]	[4.8], [7.1], [7.2] [8.1], [9], [10], [17]	[4.2.3], [4.2.9]
Contemporaneous	[4.8]	[6.14]	[12.4], [14]	[4.1], [4.2.9]
Original	[4.9], [4.27], [Paragraph "Record"]	[6.14], [6.15], [6.16]	[8.2], [9]	[4.2.5]
Accurate	[4.1], [6.17]	[5.40], [5.42], [5.45], [5.46], [5.47], [6.6]	[Paragraph "Principles"] [4.8], [5], [6], [7.2]	[4.2.3]
Complete	[4.8]	[6.16], [6.50], [6.60], [6.61]	[4.8], [7.1], [7.2], [9]	[4.2.3], [4.2.5]
Consistent	[4.2]	[6.15], [6.50]	[4.8], [5]	[4.2.3]
Enduring	[4.1], [4.10]	[6.11], [6.12], [6.14]	[7.1], [17]	[4.2.6]
Available	[Paragraph “Principle”], [4.1]	[6.12], [6.15], [6.16]	[3.4], [7.1], [16], [17]	[4.2.1]

11.2 Classification of deficiencies 欠陥の分類

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：以下のガイダンスは、データインテグリティの欠陥の報告と分類の一貫性を支援することを目的としており、内部ポリシーまたは国の規制の枠組みに従って行動する査察機関の能力に影響を与えることを意図していない。

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.

データインテグリティの障害に関連する欠陥は、製品の品質にさまざまな影響を与える可能性がある。障害の蔓延は、単一の従業員の行動から、査察された組織全体の特有の障害まで多様である。

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".

欠陥の分類に関する PIC/S ガイダンスは次のように述べている。

「重大な欠陥とは、人間の患者または動物に有害な製品、または食品生産動物に有害な残留物をもたらす可能性のある製品のいずれかを生産した、または生産する重大なリスクにつながる慣行またはプロセスである。 重大な欠陥は、製造業者が製品またはデータの詐欺、虚偽表示、または改ざんに関与していることが観察された場合にも発生する。」

11.2.3

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

•Data integrity failure resulting from bad practice,

•Opportunity for failure (without evidence of actual failure) due to absence of the required data control measures.

詐欺、虚偽表示、または改ざんに関連する欠陥の「重大な」分類にもかかわらず、データインテグリティの欠陥は以下にも関連する可能性があると理解されている。

---

[12] PI 040 PIC/S Guidance on Classification of GMP Deficiencies

•悪い実践に起因するデータインテグリティの失敗、
•必要なデータコントロール手段がないために（実際の障害の証拠をもたない）失敗する可能性。

11.2.4

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

このような場合、以下を考慮して欠陥の分類を割り当てることが適切な場合がある（表示リストのみ）。

Impact to product with actual or potential risk to patient health: Critical deficiency: •Product failing to meet Marketing Authorisation specification at release or within shelf life. •Reporting of a 'desired' result rather than an actual out of specification result when reporting of QC tests, critical product or process parameters. •Wide-ranging 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.

患者の健康に実際のまたは潜在的なリスクを伴う製品への影響：重大な欠陥：
•製品がリリース時または保管期間内に販売承認仕様を満たしていない。
•QC テスト、重要な製品またはプロセスパラメータを報告する際に、実際の仕様外の結果ではなく、「望ましい」結果を報告する。
•上級経営陣の知識と支援の有無にかかわらず、データの広範囲にわたる虚偽表示または改ざんは、医薬品品質システムの信頼性を著しく損ない、サイトによって製造または取り扱われる医薬品の品質と安全性に対するすべての信頼を損なう。

Impact to product with no risk to patient health: Major deficiency: •Data being misreported, e.g. original results 'in specification', but altered to give a more favourable trend. •Reporting of a 'desired' result rather than an actual out of specification result when reporting of data which does not relate to QC tests, critical product or process parameters. •Failures arising from poorly designed data capture systems (e.g. using scraps of paper to record info for later transcription).

患者の健康へのリスクのない製品への影響：主要な欠陥：
•誤って報告されているデータ。 元の結果は「仕様どおり」であるが、より好ましい傾向を与えるように変更されている。
•QC テスト、重要な製品またはプロセスパラメータに関連しないデータを報告する場合、実際の仕様外の結果ではなく、「望ましい」結果を報告する。
•不十分に設計されたデータキャプチャシステムに起因する障害（たとえば、後で転記するために紙のスクラップを使用して情報を記録する）。

No impact to product; evidence of moderate failure: Major deficiency: •Bad practices and poorly designed systems which may result in opportunities for data integrity issues or loss

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

製品への影響はない; 中程度の失敗の証拠：主要な欠陥：

•不適切な実践および不十分な設計のシステムにより、データインテグリティの問題が発生し、または機能領域（QA、本番、QC など）の数が限られている場合にトレーサビリティが失われる可能性がある。それぞれがそれ自体で、製品の品質に直接的な影響を与えることはない。

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

•Bad practice or poorly designed system which result in opportunities for data integrity issues or loss of traceability in a discrete area.

•Limited failure in an otherwise acceptable system, e.g. manipulation of non-critical data by an individual.

製品への影響はない。 失敗の限られた証拠：その他の欠陥：

•不適切な実践または不十分な設計のシステムにより、データインテグリティの問題や個別の領域でのトレーサビリティの喪失の機会をもたらす、。

•他の許容できるシステムでの限定的な障害。 個人による重要でないデータの操作など。

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.

重要な要素（データガバナンスプロセス、準拠したデータの記録を容易にするシステムの設計、監査証跡の使用と検証、IT ユーザクセスなど）の適正な全体像を構築し、全社的な障害、または限られた範囲/影響の不足に関する堅牢な評価を行うことが重要である。

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.

個々の状況（悪化/緩和要因）も、最終的な分類または規制措置に影響を与える可能性がある。欠陥の分類およびコンプライアンス問題の当局内報告に関する詳細なガイダンスは、欠陥の分類に関する PIC/S ガイダンス PI040 で入手できる。

12. REMEDIATION OF DATA INTEGRITY FAILURES データインテグリティ障害の修復

12.1 Responding to Significant Data Integrity issues 重要なデータインテグリティの問題への対応

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:

主に、特定された当面の問題を解決し、データインテグリティの問題に関連するリスクを評価することを検

討する必要がある。 問題の企業による対応は、是正計画の一部として取られた行動の概要を示す必要がある。 関係する製造業者からの回答には、以下を含める必要がある。

•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]; •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; •An assessment of the extent of data integrity deficiencies at the facility. Identify omissions, alterations, deletions, record destruction, non-contemporaneous record completion, and other deficiencies; •Determination of the scope (data, products, processes and specific batches) and timeframe for the incident, with justification for the time-boundaries applied; •A description of all parts of the operations in which data integrity lapses occurred, additional consideration should be given to global corrective actions for multinational companies or those that operate across multiple sites; •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; •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.

•詳細な調査プロトコルと方法論。 評価の対象となるすべての研究所、製造業務、製品およびシステムの要約。 規制対象のユーザが除外することを提案する操作の任意の部分の正当性
•データの不正確さの性質、範囲、および根本原因を特定するための、現在および可能な場合は適切な元従業員へのインタビュー。これらの面接は、資格のある第三者によって実施される場合がある。
•施設でのデータインテグリティの欠陥の程度の評価。 見落とし、変更、削除、記録の破壊、非同時期の記録の完了、およびその他の欠陥を特定する。
•インシデントの範囲（データ、製品、プロセス、および特定のバッチ）と時間枠の決定、および適用される時間境界の正当化。
•データインテグリティの欠如が発生した操作のすべての部分の説明。多国籍企業または複数のサイトにまたがって操作する企業のグローバルな是正措置については、追加の考慮事項を与える必要がある。
•データインテグリティの欠陥の性質の包括的な遡及的評価、および調査プロトコルで定義されているように、是正措置および予防措置の基礎を形成する根本原因または最も可能性の高い根本原因の特定。 潜在的な違反が特定された分野で特定の専門知識を持つ資格のある第三者コンサルタントのサービスが必要になる場

[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.

合がある。
•観察された障害が関連する物質、医薬品、および製品の品質に及ぼす潜在的な影響のリスク評価。 評価には、データインテグリティの欠如によって影響を受ける製品のリリース/配布によって引き起こされる患者への潜在的なリスク、進行中の運用によってもたらされるリスク、および製品登録書類に関連するデータを含む規制当局に提出されるデータインテグリティへの影響の分析を含める必要がある。

12.1.1.2

Corrective and preventive actions taken to address the data integrity vulnerabilities and timeframe for implementation, and including: •Interim measures describing the actions to protect patients and to ensure the quality of the medicinal products, such as notifying customers, recalling product, conducting additional testing, adding lots to the stability program to assure stability, drug application actions, and enhanced complaint monitoring. Interim measures should be monitored for effectiveness and residual risks should be communicated to senior management, and kept under review. •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.

データインテグリティの脆弱性と実装の時間枠に対処するために取られた是正措置と予防措置。これには次のものが含まれる。
•顧客への通知、製品のリコール、追加のテストの実施、安定性を保証するための安定性プログラムへのロットの追加、薬物適用アクション、および強化された苦情モニタリングなど、患者を保護し、医薬品の品質を確保するためのアクションを説明する暫定措置。暫定措置は有効性をモニタリングし、残留リスクを上級経営陣に伝達し、レビュを継続する必要がある。
•データインテグリティを確保するために設計された、手順、プロセス、方法、コントロール、システム、マネジメントの監視、および人的資源（トレーニング、人員配置の改善など）の改善努力と強化を説明する長期的な措置。長期的な措置が特定される場合は、リスクを軽減するための暫定的な措置を実施する必要がある。

12.1.1.3

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

実行されたアクションによって問題が解消されたかどうかをモニタリングするために実装された CAPA 有効性チェック。

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:

•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
•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.

可能な限り、査察官は関係する企業の上級代表と会い、特定された欠陥の性質を伝え、企業が問題の包括的な調査と完全な開示およびそれらの迅速な解決にコミットしていることを書面で確認する必要がある。 グローバルな是正措置と予防措置計画の詳細を含む管理戦略を規制当局に提出する必要がある。 戦略には以下を含める必要がある。
•現在の行動計画の範囲と深さが調査とリスク評価の結果に見合っているという証拠を含む、データインテグリティの欠如の根本原因の包括的な説明。 これは、データインテグリティの欠如に責任のある個人が GMP/GDP 関連または薬剤適用データに影響を与えることができるかどうかを示す必要がある
•規制対象のユーザが、分析データ、製造記録、および所管官庁に提出または提示されたすべてのデータを含む、生成されたすべてのデータの「ALOCA +」属性（セクション 7.4 を参照）をどのように確保するかを説明する詳細な是正措置計画。

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.

査察官は、データインテグリティ違反に関連するリスクを管理および封じ込めるために、査察時に特定された重大なデータインテグリティの問題を管理するためのポリシーを実装する必要がある。

12.2 Indicators of improvement 改善の指標

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:

重大なデータインテグリティの問題に対処するために実行されたアクションの有効性を検証するために、オンサイト査察を推奨する。 効果的な改善を検証するための代替アプローチは、リスクマネジメントの原則に従って検討することができる。 改善の指標は次のとおりである。

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;

特定された問題の徹底的かつオープンな評価と、組織レベルでの是正措置および予防措置の適切な実施を含む、効果的な是正措置および予防措置の適時の実施の証拠。

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;

クライアントや他の規制当局との問題のオープンなコミュニケーションの証拠。 調査と修復の段階を通じて、透明性のあるコミュニケーションを維持する必要がある。 規制当局は、詳細な調査の結果として、さらなるデータインテグリティの障害が報告される可能性があることに注意する必要がある。 これらの通知に対する追加の反応は、継続的な報告を奨励するために、公衆衛生上のリスクに比例する必要がある。

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;

潜在的な問題と改善の機会をオープンに報告するためのプロセスを組み込み、奨励する、組織全体でのデータインテグリティの期待を伝達する証拠。

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;

規制対象のユーザは、データ操作に対する電子システムの脆弱性の適切に評価し、フォローアップアクションがすべての違反を完全に解決したことを確認する必要がある。この評価には、関連する専門知識を備えた資格のある第三者コンサルタントのサービスが必要になる場合がある。

12.2.1.5

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

本ガイドの原則に沿ったデータインテグリティポリシーの実装。

12.2.1.6

Implementation of routine data verification practices.

日常的なデータ検証手法の実装。

13. Glossary 用語集

Archiving　　アーカイブ

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

プロセスまたはアクティビティの再構築を目的として、完成したデータおよび関連するメタデータを最終的な形式で長期間永続的に保持する。

Audit Trail　監査証跡

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 監査証跡は、GMP/GDP 活動の再構築を可能にする、GMP/GDP 重要情報（GMP/GDP 関連データの作成、変更、削除など）の記録であるメタデータである。

Back-up　バックアップ

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.

災害復旧の目的で維持されている現在の（編集可能な）データ、メタデータ、およびシステム構成設定（分析実行に関連する変数設定など）のコピー。

Computerised system　コンピュータ化されたシステム

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

データの入力、電子処理、およびレポートまたは自動制御のいずれかに使用される情報の出力を含むシステム。

Data　データ

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

参照または分析のために一緒に収集された事実、数値、および統計。

Data Flow Map　データフローマップ

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

情報システムを介したデータの「流れ」のグラフィック表現

Data Governance　データガバナンス

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.

データのライフサイクル全体を通じて完全で一貫性のある正確な記録を保証するために、形式に関係なくの生成、記録、処理、保持、および使用されたデータを保証するための取り決めの合計。

Data Integrity　データインテグリティ

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.

データインテグリティ、一貫性、正確性、信用性、信頼性およびデータのこれらの特性がデータのライフサイクル全体を通じて維持される度合い。

データは安全な方法で収集および維持する必要がある。これにより、データは帰属可能、判読可能、同時性のある記録、オリジナル（または真のコピー）で正確性をもつ。 データインテグリティを保証するには、適切な品質とリスクマネジメントシステムが必要である。これには、健全な科学的原則と適正な文書化実践の順守が含まれる。 データは ALCOA +の原則に準拠している必要がある。

Data Lifecycle　データライフサイクル

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.

データ（生データを含む）の初期生成と記録から処理（変換または移行を含む)、使用、データ保持、アーカイブ/検索、破棄までのすべてのフェーズ。

Data Quality　データ品質

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

生成されたデータが、まさにまさに意図された目的に合わせて作成され、意図された目的に適合しているという保証。これには、ALCOA +の原則が組み込まれている。

Data Ownership　データの所有権

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.

特定のプロセス所有者に対するデータコントロールの責任の割り当て。 企業は、システムとそのデータに対する責任が適切に割り当てられ、責任が遂行されることを確実にするためのシステムを実装する必要がある。

Dynamic Record　ダイナミック記録

Records, such as electronic records, that allow an interactive relationship between the user and the record content.[13]

ユーザと記録の内容の間のインタラクティブな関係を可能にする電子記録などの記録。

Exception Report　例外レポート

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

[14] ‘GXP’ Data Integrity Guidance and Definitions, MHRA, March 2018

事前に決定された「異常な」データまたはアクションを特定して文書化するバリデートされた検索ツールであり、データレビュアによる深い注意や調査を必要とする。

Good Documentation Practices (GdocP)　適切な文書化の実践

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

紙であろうと電子的であろうと、文書を集合的かつ個別に保証する手段であり、データマネジメントおよびインテグリティの原則を満たしている。例、ALCOA+。

Hybrid Systems　ハイブリッドシステム

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.

データを管理およびコントロールするためのシステムであり、通常は、電子データを生成する電子システムで構成され、紙ベースの記録を常に生成する定義された手動システムによって補完される。したがって、ハイブリッドシステムの完全なデータセットは、電子データと紙のデータの両方で構成される。 ハイブリッドシステムは、両方のサブシステムの効果的な管理を使用して、正しい動作を行う。

Master Document　マスタードキュメント

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

配布または使用するためのコントロールされたコピーを作成できる、元の承認済みドキュメント。

Metadata　メタデータ

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.

他のデータの属性を記述し、コンテキストと意味を提供するファイル内データ。

通常、これらは、データの構造、データ要素、相互関係、および監査証跡などその他の特性を説明するデータである。メタデータを使用すると、データを個人に帰属させることもできる（または、自動生成された場合は、元のデータソースに帰属させることもできる)。 メタデータは、元の記録の不可欠な部分を形成する。 メタデータによって提供されるコンテキストがなければ、データは意味を持たない。

Quality Unit　品質部門

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.

特に医薬品品質システムの設計、効果的な実施、モニタリングおよび保守を含む品質の監視を担当する規制対象組織内の部門。

Raw Data　生データ

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]

生データは、紙に記録されているか電子的に記録されているかにかかわらず、情報の最初のキャプチャとして説明できる元の記録（データ）として定義される。 元々動的な状態でキャプチャされた情報は、その状態で引き続き利用できる必要がある。

Static Record　静的な記録

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]

紙や電子記録など、固定された記録形式であり、ユーザと記録コンテンツの間のやりとりをほとんどまたはまったく許可しない

Supply Chain　サプライチェーン

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.

製造サイト、卸売サイト、流通サイト間の取り決めの合計であり、販売または使用の時点までの製造および流通を通じて医薬品の品質が保証される。

System Administrator　システム管理者

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

コンピュータ化されたシステムまたは特定の電子通信サービスの運用を管理する人。

14. REVISION HISTORY　改訂履歴

Date　日付	Version Number バージョン番号	Reasons for revision　改定理由