管理番号: BZLib-119

改訂番号: 1.2

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

ページ数: 全 109ページ

PHARMACEUTICAL INSPECTION CONVENTION
PHARMACEUTICAL INSPECTION CO-OPERATION SCHEME

PI 041-1
1 July 2021

PIC/S GUIDANCE

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

Editor: PIC/S Secretariat

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

株式会社文善

改 1.2　**2024 年 1 月 30 日**

管理番号: BZLib-119

改訂番号: 1.2

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

ページ数: 全 109ページ

【注記】

本書は、Pharmaceutical Inspection Convention (PIC) の発行した英語原文を株式会社文善にて和文翻訳したものです。

翻訳文はできるだけ英語原文に忠実になるよう努めましたが、あくまでも英語原文を正とするものです。本書は規制の理解を補助する目的で作成したものであり、株式会社文善は翻訳文に誤りがないことについて保証いたしません。

原文の内容をご自身で必ず確認してください。株式会社文善は、本書を利用したことに起因して、何らかの損害が生じたとしても、これについては一切の責任を負いません。

本書に含まれる内容は、予告なしに変更されることがあります。

本書を含め、株式会社文善のサイト (https://bunzen.co.jp) では、電磁的記録・電子署名等に関する規制やガイダンスの翻訳を掲載しています。

本書、株式会社文善のサービス等への質問、コメント等は info1@bunzen.co.jp にお寄せください。

【本書の表記について】

文脈に応じ言葉を補足した場合、〔 〕内にそれを記述しています。

【訳注】には、訳又は内容についての説明を記載しています。1 つの段落中に 2 箇所以上の訳注挿入があった場合、【訳注 [1]】のように段落内のみの通し番号を付け、段落末尾に【訳注 [1]：】と番号を対応させて記述しています。

目次

1. DOCUMENT HISTORY

1. 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

2. はじめに

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 に参加する各当局機関は、医薬品有効成分 (API) や医薬品の製造業者や販売業者に対して、GMP (Good Manufacturing Practice) や GDP (Good Distribution Practice) の原則への適合レベルを判断するために、定期的に査察を行っている。これらの査察は、通常はオンサイトで行われるが、証拠書類の評価をリモート又はオフサイトで行うこともあり、その場合にはデータをリモートでレビューすること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.	査察プロセスの有効性は、査察官に提供される証拠書類の信頼性、つまり元となるデータのインテグリティによって決まる。査察プロセスでは、査察官が、提示された証拠書類や記録の正確性及び完全性を判断し、それらに全幅の信頼を寄せられることが非常に重要である。
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は、データを取り扱う際に実施されるすべての活動に関連するものであり、データポリシー、文書化、品質、セキュリティ等が含まれる。グッドデータマネジメントプラクティスは、製造業者により生成・記録されるすべてのデータ品質に影響を与える。グッドデータマネジメントプラクティスにより、データの帰属性、判読性、同時記録性、原本性、正確性、完全性、一貫性、永続性、可用性を確実にする必要がある。本書の主眼は GMP/GDP の期待に関連したものであるが、本書の原則は、グッドデータマネジメントプラクティスとして、 (API 及び製剤を管理するための戦略・仕様のベースとなる登録申請書類に含まれるデータ等を含め) もっと広い範囲でも考慮されるべきである。

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.	グッドデータマネジメントプラクティスは、医薬品品質システムのすべての要素に適用される。そして、ここに記載されている原則は、電子システム及び紙ベースシステムで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「データが完全であり、一貫性があり、正確であり、信用でき、信頼でき、かつデータのこれらの特性がデータのライフサイクルを通して維持される程度」と定義されている[1]。医薬品品質システムは、医薬品の品質を確実にするためのものであるが、データインテグリティは、効果的な医薬品品質システムの基本的な要件である。お粗末なデータインテグリティプラクティスや脆弱性は、記録や証拠の質を低下させ、結果的には医薬品の品質を低下させる可能性がある。
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及びデータインテグリティに関するグッドプラクティスの責任は、査察を受ける製造業者又は販売業者にある。製造業者又は販売業者はデータマネジメントシステムに潜在的な脆弱性がないかどうかをアセスメントし、データインテグリティを確実に維持するためのグッドデータガバナンスプラクティスを設計し、実施するための手段を講じる全責任と義務がある。

3. PURPOSE

3. 目的

3.1	This document was written with the aim of:	本書は、以下を目的として作成された：
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.	グッドデータマネジメントに関連するGMP/GDP要件の解釈、及び査察の実施について、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,	〔本書は〕リスクベースのコントロール戦略に関する統合的で説明的なガイダンスを提供するとともに、データが有効で、完全で、信

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

	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.	頼できること、という (GMP[2] 及び GDP[3] の PIC/S ガイダンスに記載されている) 以前からある要件を、最新の業界慣行やグローバル化したサプライチェーンの中で実現できるようにするものである。
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.	〔本書は〕日常的な GMP/GDP 査察の計画と実施に、グッドデータマネジメントの要素を、効果的に導入できるようにし、GMP/GDP 査察の調和に資するツールを提供し、データインテグリティの期待についての査察の品質を確保するためのものである。
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.	本書は、aide memoire【訳注】等の査察用リソースと一緒に、査察官が査察時間を最適に活用し、査察中にデータインテグリティの要素を最適に評価できるようにするものである。 【訳注：査察官用の手引き。https://picscheme.org/en/publications に掲載されている。】
3.3	Guidance herein should assist the Inspectorate in planning a risk-based inspection relating to good data management practices.	ここに記載されているガイダンスは、査察官がグッドデータマネジメントプラクティスについてリスクベース査察を計画する際に助けとなるものである。
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.	グッドデータマネジメントは、常に、GMP/GDP の不可欠な要素と考えられてきた。したがって、本書は、規制対象会社に新たな規制上の負担を課すものではなく、むしろ最新の業界のデータマネジメントプラクティスに照らして、以前からある GMP/GDP 要件を解釈するためのガイダンスを提供することを意図している。
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	データマネジメントとデータインテグリティの原則は、紙ベースのシステム、コンピュータ化システム、ハイブリッドシステムに等しく適用されるものであり、新しい概念や技術

[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

	Q10 principles, this guide should facilitate the adoption of innovative technologies through continual improvement.	の開発や採用を妨げるものであってはらならない。本書は、ICH Q10 の原則に従って、継続的改善による革新的な技術の採用を支援するものである。
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.	本書では、「医薬品品質システム」という用語を頻繁に使っているが、これは品質目標を管理し、達成するために使用される品質管理システムを意味する。GMP 規制対象会社では「医薬品品質システム」という用語を主に使用しているが、本書では、GDP 規制対象会社が使用している「品質システム」と同義とみなすものとする。
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.	本書は、強制ではなく、法律に基づいて執行されるものではない。本書は、医薬品及び活性物質 (すなわち API) の製造業者及び販売業者の行動を制限したり、データインテグリティの要件に関する各国の国内法を代替することを意図していない。データインテグリティの欠陥を指摘する場合は、国内法又は PIC/S の GMP ガイダンス又は GDP ガイダンスの関連パラグラフを参照すべきである。

4. SCOPE

4. 適用範囲

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.	本書は、製造 (GMP) 活動及び流通 (GDP) 活動を行う拠点へのオンサイト査察で利用するために作成された。本書に記載されている原則は、製品ライフサイクルのすべての段階に適用される。本書は、査察時に考慮すべき領域をすべて網羅しているわけではないことに留意すること。
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.	本書は、製造 (GMP) 活動及び流通 (GDP) 活動を行っている拠点へのリモート (デスクトップ) 査察にも利用できるが、それはデータガバナンスシステムのアセスメントに限定される。データの検証や、業務が手順に適合していることの証拠〔の確認〕には、通常オンサイトアセスメントが必要となる。

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.	本書は上記の適用範囲で作成されているが、ここに記載されているグッドデータマネジメントプラクティスの多くの原則は、規制下の医薬品及びヘルスケア産業の他の領域にも適用できる。
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.	本書は、フォレンジックの専門技術【訳注】が必要となるような重大なデータインテグリティの脆弱性が検出された後に行われる「for-cause」査察 (追加査察) についての具体的な指針を提供するものではない。 【訳注：メディアに保存されたファイルを法的な証拠として利用する技術。】

5. DATA GOVERNANCE SYSTEM

5. データガバナンスシステム

5.1 What is data governance?

5.1 データガバナンスとは？

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.	データガバナンスとは、データインテグリティを保証するために実施する準備事項の総体である。これらの準備事項を経て、データが、生成・記録・処理・保管・検索・使用される際のプロセス、フォーマット、技術にかかわらず、データライフサイクルを通して、確実に、帰属性・判読性・同時記録性・原本性・正確性・完全性・一貫性・永続性・可用性のある記録となる。「データガバナンスシステム」を実現することは法的要件ではないが、このシステムを確立することで、製造業者は、データインテグリティのリスクマネジメント活動を首尾一貫した方法で定義し、優先順位をつけ、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と、データインテグリティシステム間の調整が取れず、コントロール方策に隙間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	データライフサイクルは、データがどのように生成され、処理され、報告され、チェックされ、意思決定に使用され、保存され、最終的に保存期間終了時に廃棄されるか、を示すものである。製品やプロセスに関連するデー

	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).	タは、そのライフサイクルの中で様々な境界を越える場合がある。これには、紙ベースのシステムとコンピュータ化システムとの間のデータ転送や、社内 (例えば、製造、QC、QA の間等) 及び社外 (例えば、サービスプロバイダーの間、契約委託者と受託者の間等) の異なる組織の境界をまたいだデータ転送が含まれる。

5.2 Data governance systems

5.2 データガバナンスシステム

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 の GMP/GDP ガイダンスに記載されている医薬品品質システムに不可欠なものである。データガバナンスシステムにより、ライフサイクルを通してデータオーナーシップを明らかにするとともに、データインテグリティの原則に適合するように、プロセス及びシステムの設計・運用・監視を検討する。データインテグリティの原則には、情報を意図的又は誤って変更・削除しないようにするためのコントロールが含まれる。
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には、適切に設計されたシステム、技術の利用、及びデータセキュリティ対策を取り込むことが不可欠であり、そこにデータマネジメント及びデータインテグリティの効果的なコントロールを確実にする専門技術を組み合わせる。規制対象会社は、適切なリソースを用意し、データガバナンスシステムの設計・開発・運用・監視に活用するための手段を講じるべきである。データガバナンスシステムは、システム、業務の複雑さ、データ重要度及びデータリスクに見合ったものとする。
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: • Organisational - procedures, e.g. instructions for completion of records and retention of completed records;	データガバナンスシステムにより、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に対するコントロールを確実にすべきである。コントロールの例を以下に挙げる： • 組織的〔コントロール〕 - 手順。例えば、記録の記入方法や記入

	- 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. • Technical - computerised system validation, qualification and control; automation; or - the use of technologies that provide greater controls for data management and integrity.	した記録の保管方法等。 - データの生成と承認についてのスタッフへのトレーニング、及び文書化された許可。 - データガバナンスシステムの設計。どのようにデータが生成・記録・処理・保管・使用されるか、また、どのようにリスクや脆弱性が効果的にコントロールされるかを考慮する。 - 日常的なデータ検証 (例えば、日ごと、バッチごと、アクティビティごと等) 。 - 定期的な監視。例えば、データガバナンスシステムの有効性を検証するための自己点検プロセス等。 - データマネジメント及びデータインテグリティに関する専門技術を有する社員の活用。データセキュリティ対策の専門技術を含む。 • 技術的〔コントロール〕 - コンピュータ化システムバリデーション、適格性評価、コントロール、オートメーション。 - データマネジメント及びデータインテグリティのコントロールを強化する技術の利用。
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では、効果的なデータガバナンスプラクティス (適切な組織文化と行動 (第 6 章参照) に、データ重要度、データリスク及びデータライフサイクルの理解を組み合わせることの必要性を含む) に対する上級管理職の理解及びコミットメントが示されるものである。また、組織内のすべてのレベルの社員に、〔会社が〕期待することを伝えた証拠が必要である。これは、失敗や改善の機会を報告するエンパワーメントを確実にするような方法で行われる。こういったことにより、データを改ざん・変更・削除する動機が減少する。

5.2.5	The organisation's arrangements for data governance should be documented within their Pharmaceutical Quality System and regularly reviewed.	組織のデータガバナンスに関する準備事項は、医薬品品質システムの中で文書化し、定期的に見直すべきである。

5.3 Risk management approach to data governance

5.3 データガバナンス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、システム及び手順を導入し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とともに、ICH Q9 の原則を用いて残存リスクを特定する責任を負う。契約委託者は、〔自社の〕ベンダー保証プログラムの一環として、契約受託者のデータマネジメント方針及びコントロール戦略をレビューすべきである。このようなレビューの頻度は、リスクマネジメントの原則 (第 10 章参照) を用いて、契約受託者が提供するサービスの重要度に基づいて決定すべきである。
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る労力と資源は、製品品質へのリスクに見合うものとし、他の品質資源の需要とのバランスをとる必要がある。GMP/GDP の原則により規制されるすべての事業者 (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た許容可能なコントロール状態をもたらし、裏付けとなる根拠とともに文書化されるようなシステムを設計し、運用すべきである。
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.	望ましいコントロール状態を達成するための長期的措置が特定された場合、暫定措置を実施し、リスクを低減するとともに、その有効性を監視する必要がある。暫定措置やリスクの優先順位付けが必要になるときは、残存データインテグリティリスクを上級管理職に伝え、常にレビューすべきである。自動化システム及びコンピュータ化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〔自動化の流れに〕逆行するアプローチは、業務管理上の負担とデータリスクを増大させ、第 3.5 章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高い。

5.3.4	Not all data or processing steps have the same importance to product quality and patient safety. Risk management should be utilised to determine the importance of each data/processing step. An effective risk management approach to data governance will consider: • Data criticality (impact to decision making and product quality) and • Data risk (opportunity for data alteration and deletion, and likelihood of detection / visibility of changes by the manufacturer's routine review processes). From this information, risk proportionate control measures can be implemented. 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.	すべてのデータや処理ステップが製品の品質や患者の安全に同じ重要性を持つわけではない。それぞれのデータや処理ステップの重要性を判断するために、リスクマネジメントを活用すべきである。データガバナンスに対する効果的なリスクマネジメントアプローチは以下を考慮する： • データ重要度 (意思決定や製品品質への影響) 。 • データリスク (データの改ざんや削除の機会、製造業者における定期的なレビュープロセスにより変更を検出・可視化できる可能性) 。この情報から、リスクに比例したコントロール方策を実装することができる。本書のこの後の章で、リスクマネジメントアプローチに言及しているが、「リスク」とは、データリスクの概念とデータ重要度の概念の組み合わせを指している。

5.4 Data criticality

5.4 データ重要度

5.4.1	The decision that data influences may differ in importance and the impact of the data to a decision may also vary. Points to consider regarding data criticality include: • Which decision does the data influence? For example: when making a batch release decision, data which determines compliance with critical quality attributes is normally of greater importance than warehouse cleaning records. • What is the impact of the data to product quality or safety? For example: for an oral tablet, API assay data is of generally greater impact to product quality and safety than tablet friability data.	データが影響を与える意思決定の重要性は個々に異なり、またデータが意思決定に与える影響の程度も異なる。データ重要度について考慮すべき点は以下の通りである： • そのデータはどのような意思決定に影響を与えるのか？ 例えば、一般的には、バッチリリースを判断する際の重大な品質属性への適合を決定するためのデータは、倉庫の清掃記録よりも大事である。 • データは、製品の品質や安全性にどのような影響があるか？ 例えば、経口錠剤についていえば、一般的には、原薬の分析データは、錠剤の破砕性データよりも製品の品質と安全性に大きな影響がある。

5.5 Data risk

5.5 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の要件はすべての GMP/GDP データに関連しているが、データ重要度をアセスメントすることは、組織がデータガバナンスの取り組みに優先順位をつける際に役立つ。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されるべきである。
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.	データリスクアセスメントでは、過失による変更・削除・ (事故又はセキュリティ障害による) 消失・再作成・意図的な改ざんに対するデータの脆弱性、及びそういった行為の発見しやすさを考慮する。また、災害時に、確実に、完全かつタイムリーにデータを回復できるか、も考慮する。許可のない活動を防止し、可視性・検出性を高めるようなコントロール方策をリスク低減措置として利用できるであろう。
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くする要因は、例えば、プロセスが複雑又は一貫性がなく、その結果がオープンエンドで、〔判断が〕主観的である場合である。一貫性があり、明確に定義され、客観的なタスクで構成されるシンプルなプロセスは、リスクの低減につながる。
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: • 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);	リスクアセスメントは、ビジネスプロセス (例：製造、QC) に焦点を当て、データの流れやデータの生成・処理方法を評価するものであり、IT システムの機能や複雑さだけを考慮するものではない。考慮すべき要素は以下の通りである： • プロセスの複雑さ (例：多段階にわたるプロセス、プロセス又はシステム間のデータ転送〔の有無〕、複雑なデータ処理) 。 • データを生成・処理・格納・アーカイブする方法、及びデータ品質とデータインテグリティを保証する能力。 • プロセスの一貫性 (例：生物学的生産プロセスや分析試験は、低分子化学に比べ

	• 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.	て、より高い変動性を示す可能性がある)。 • オートメーションの程度、人間の関与する程度 • 最終状態・結果〔を記録する際〕の主観性 (すなわち、プロセスがオープンエンドであるか、又は明確に定義されているか)。 • 電子システムのデータと手作業で記録されたイベントを比較した結果 (例：分析レポートと生データ取得の間に明らかな時間差がある)。 • システム又はソフトウェアにもともと組み込まれているデータインテグリティコントロール。
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.	コンピュータ化システムのリスクアセスメントプロセスでは、IT システムと手作業のインターフェイスを考慮する必要がある。コンピュータ化システムバリデーションだけではデータインテグリティのリスクを下げることにはならないかもしれない。特に、バリデートされたシステムのデータを報告する際にユーザーが〔その内容に〕手を加えることができる場合や、システムが本書の第 9 章に概説されている基本要件に沿ってバリデートされていない場合である。完全に自動化され、バリデートされたプロセスは、人の介入を許さないか最小限に抑えるように構成設定されていれば、データインテグリティリスクを下げる設計であるといえ、より好ましい。技術的な理由でコントロールを統合できない場合は、適切な手順的コントロールを導入し、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.	査察官は、批判的思考スキルを用いて、〔会社の〕コントロールとレビュー手順により望ましい結果が効果的に達成されているか判断する必要がある。データガバナンスの成熟度を示す 1 つの指標は、残存リスクを組織として理解し、受け入れているかどうかであり、それに基づいてアクションの優先順位が決定される。データインテグリティ障害の「リス

	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.	クなし」と信じている組織は、データライフサイクルに内在するリスクを適切にアセスメントしていない可能性が高い。したがって、データライフサイクル、データ重要性及びデータリスクをアセスメントするアプローチを詳細に調べる必要がある。これにより、査察中に調査すべき潜在的な問題が見つかることもある。

5.6 Data governance system review

5.6 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.	自己点検 (内部監査) 等の定期的なレビュープロセスにより、データインテグリティコントロール方策の有効性を定期的にアセスメントすべきである。これにより、データライフサイクル全体にわたるコントロールが意図したとおりに機能することを確実にする。
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: • A check of continued personnel understanding of good data management practice in the context of protecting of the patient, and ensuring the maintenance of a working environment which is focussed on quality and open reporting of issues (e.g. by review of continued training in good data management principles and expectations). • A review for consistency of reported data/outcomes against raw 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. • 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	自己点検では、日常的なデータ検証チェック (例：日ごと、バッチごと、アクティビティごと) に加えて、さらに広範にコントロール方策をレビューすべきである。そのようなレビューには以下が含まれる： • 社員のグッドデータマネジメントプラクティスの理解度についての継続的チェック。患者を保護し、(例えば、グッドデータマネジメントの原則と期待についての継続的なトレーニングをレビューすることで) 品質及びオープンな問題の報告に焦点を当てた職場環境を確実に維持するという観点で実施される。 • 報告されたデータ・結果と生データの整合性のレビュー。日常的プロセスの継続的な有効性を確実にするために、(リスクに基づいた合理的な理由により) 定期的なデータ検証チェックの対象となっていないデータ、及び (又は) 以前に検証されたデータサンプルをレビューしてもよい。 • コンピュータ化システムのログ・監査証跡のリスクベースのサンプル。これは、GMP/GDP 活動に関連する情報が正確に報告されることを確実にするために行

	validated 'exception report'[4]. • A review of quality system metrics (i.e. trending) that may also be indicators of data governance effectiveness.	う。これは、日常的なコンピュータ化システムのデータを手作業又はバリデートされた「例外報告書」[4]によりレビューしている状況で有効である。 • データガバナンスの有効性の指標としても使える品質システムメトリクス (すなわち、傾向) のレビュー。
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ー〔が実施されていること〕は、会社の〔組織〕行動と組織的・技術的コントロールとの相互作用の重要性が理解されていることの証左となるものである。そのレビュー結果は、上級管理職に伝えられるとともに、データインテグリティの残存リスクのアセスメントに使用されるべきである。

6. ORGANISATIONAL INFLUENCES ON SUCCESSFUL DATA INTEGRITY MANAGEMENT

6. データインテグリティマネジメントを成功させるための組織の影響力

6.1 General

6.1 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.	査察で、組織の行動に関する欠陥を報告することは適切ではない、又は可能ではないかもしれない。〔組織の〕行動が、(i)データを修正・削除・改ざんする動機、及び(ii)データインテグリティを確実にするために設計された手順的コントロールの有効性、に与える影響を理解することで、さらに調査すべきリスクが分かってくるであろう。
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	査察官は、文化が組織の行動に与える影響を敏感に察知し、本書のこの章に記載されている原則を適切に適用すべきである。何が効果的な「品質文化」やデータガバナンスなのかは、場所ごとに実施方法が異なるかもしれな

[4] An 'exception report' is a validated search tool that identifies and documents predetermined 'abnormal' data or actions, which requires further attention or investigation by the data reviewer.
[4]「例外報告書」とは、バリデートされた検索ツールであり、事前に設定された「異常」なデータやアクションを特定し文書化する。これにより、データレビュー担当者は、注意を促され、調査を行う。

	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.	いが、文化的側面が明らかにデータインテグリティの懸念につながっている場合、査察官は、これらの懸念を組織に効果的かつ客観的に報告し、正させるようにすべきである。
6.1.3	Depending on culture, an organisation's control measures may be: • 'open' (where hierarchy can be challenged by subordinates, and full reporting of a systemic or individual failure is a business expectation) • 'closed' (where reporting failure or challenging a hierarchy is culturally more difficult)	〔組織〕文化により、組織のコントロール方策は以下のいずれかとなる： • 「オープン」 (組織上位者に対して部下が異議を唱えることができ、組織又は個人の失敗を包み隠さず報告することがビジネス上の期待事項である) • 「閉鎖的」 (失敗を報告したり、組織上位者に挑戦することが文化的に困難である)
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」な文化を持つ組織のグッドデータガバナンスは、医薬品品質システムを通して問題を特定し、報告するといった、従業員のエンパワーメントにより促進される。一方、「閉鎖的」な文化を持つ組織では、望ましくない情報を伝えることが社会的な障壁となるため、同等のコントロールレベルを達成するためには、監視や二次レビューをより重視する必要があるであろう。このような状況では、上級管理職への秘密のエスカレーションプロセスを設けることも重要であり、そういった準備事項より上級管理職が報告することを積極的にサポートし、奨励していることを明確に示すべきである。
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管理職の知識と理解の程度は、組織のデータインテグリティマネジメントの成功に影響を与える。管理職は、データインテグリティ違反の発生を防ぎ、万一発生した場合にはそれを検出するといった法的及び道徳的な義務 (すなわち職務と権限) があることを認識する必要がある。経営者は、紙〔ベース〕とコンピュータ化された (ハイブリッドと電子の両方) ワークフローについて、データインテグリティのリスクを十分に可視化し、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	データインテグリティ違反は、不正行為や改ざんに限らない。意図しないものであっても

	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.	リスクとなり得る。データの信頼性が損なわれる可能性のあるものはすべてリスクであり、適切なコントロールを行うために、それらを洗い出し、理解すべきである (第 5.3～5.5 章を参照)。直接的コントロールは通常、文書化された方針及び手順といった形をとるが、従業員の行動への間接的な影響 (不当な圧力、プロセス能力を超える生産性へのインセンティブ、データを改ざんする機会、従業員による違反行動の正当化等) についても理解し、対応する必要がある。
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違反は、いつでも、どの従業員によっても引き起こされる可能性がある。そのため、管理職は、問題を検出するための注意を怠らず、違反が見つかった場合には、違反が起きた理由を理解する必要がある。これにより、問題を調査し、是正・予防措置を実施できるようになる。
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違反は、結果的に、さまざまな利害関係者 (患者・規制当局・顧客) に影響が及ぶことになり、患者の安全性に直接影響したり、組織や製品に対する信頼を損なったりする。このような結果を従業員が認識し、理解することで、品質を優先する環境が醸成される。
6.1.9	Management should establish controls to prevent, detect, assess and correct data integrity breaches, as well as verify those controls are performing as intended to assure data integrity. Sections 6.2 to 6.7 outline the key items that Management should address to achieve success with data integrity.	管理職は、データインテグリティ違反を予防・検出・アセスメント・是正するためのコントロールを確立するとともに、それらのコントロールが意図通りに機能し、データインテグリティを保証できているか検証すべきである。第 6.2 章から第 6.7 章では、データインテグリティを成功させるために管理職が取り組むべき主要な項目を概説する。
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	上級管理職は、効果的なデータガバナンスプラクティス (適切な組織文化と行動 (第 6 章参照) に、データ重要度、データリスク及びデータライフサイクルの理解を組み合わせることの必要性を含む) に対する適切なレベルの理解とコミットメントを持つ必要がある。組織内のすべてのレベルの社員に対して、失敗や改善の機会を報告するエンパワーメントを

	which ensures empowerment to report failures and opportunities for improvement. This reduces the incentive to falsify, alter or delete data.	確実にするような方法で、社員への期待を伝えたという証拠が必要である。これにより、データを改ざん・変更・削除する動機が減少する。

6.2 Policies related to organisational values, quality, staff conduct and ethics

6.2 組織の価値観、品質、スタッフの行為 及び倫理に関する方針

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、品質へのコミットメント、組織の価値及び倫理についての適切な期待を、組織全体へ明確に伝えるべきであり、適切な品質文化を実現し、維持するための方針を提供するべきである。方針は、管理職の品質についての考えを反映するとともに、(すべての個人が患者の安全と製品の品質を確実にすることに責任を負い、説明責任を持つような) 信頼関係のある環境を構築することを意図して作成すべきである。
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.	管理職は、データ品質を確保する上での社員の役割の重要性とともに、社員の活動がどのように製品の品質、患者の安全の確保に影響するのかを社員に認識させるべきである。
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.	方針では、正直さ等の倫理的行動の期待を明確に定義する必要がある。方針は、すべての社員に伝えられ、十分に理解される必要がある。その際には、要件を知らせるだけにとどまらず、なぜその要件が設けられたのか、要件を満たさなかった場合はどうなるか、も併せて伝えるべきである。
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、許可のない変更、データの破壊、その他データ品質を損なう行為等の望ましくない行動には、速やかに対処する必要がある。会社の方針に、望ましくない行動や態度の例を文書化すべきである。望ましくない行動に対するアクションを文書化すべきであるが、 (懲戒処分等の) アクションが、特定されたデータインテグリティの問題についての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、厳しい懲罰により、他のスタッフが調査に価値のある情報を開示しなくなるかもしれない。

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データインテグリティに関するグッドプラクティスに沿った行動を目にしたときは、積極的に奨励し、適切に認知すべきである。
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.	会社の方針と手順に支えられた秘密のエスカレーションプログラムを設けるべきである。これにより、社員は、方針への違反の可能性がある事例を、不利益を被ることなく、上級管理職に知らせやすくなる。上級管理職が方針違反する可能性を認識しておくべきであり、そのような場合のための適切な報告メカニズムが用意されるべきである。
6.2.7	Where possible, management should implement systems with controls that by default, uphold the intent and requirements of company policies.	可能であれば、管理職は、会社の方針の意図と要件を満たすコントロールを最初から備えているシステムを導入すべきである。

6.3 Quality culture

6.3 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.	管理職は、透明でオープンな職場環境 (すなわち品質文化) の構築を目指すべきである。そのような環境では、社員がデータの信頼性に関する潜在的な問題を含め、失敗やミスを自由に伝えるよう奨励されており、そこから是正・予防措置を講じることができる。組織体制は、すべてのレベルの社員の間で情報が流れるようなものとすべきである。
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.	それ〔品質文化〕は、管理職、チームリーダー、品質部門の社員、及びデータ品質とデータインテグリティを確保するための品質文化の構築に貢献するすべての社員により一貫して示される価値観・信念・考え方・行動の総体である。
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	管理職は、以下の方法で品質文化を醸成することができる： • 〔会社が〕期待すること (例えば、価値・倫理規範、行動規範等) を確実に認識、理解させる。 • 模範を示す。管理職は〔会社が〕期待す

	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.	る行動をやってみせるべきである。 • 行動や決定に説明責任を持つ。特に委譲した活動。 • 事業の運営に継続的かつ積極的に関与する。 • 実現可能な期待レベルを設定する。従業員にプレッシャーを与える制約を考慮する。 • 業務の要求と期待に応えるために、適切な技術的リソース及び人的リソースを割り当てる。 • データインテグリティを確実にするために、よい文化に沿った態度を奨励するような、公平で公正な結果と報酬を実現する。 • 規制の動向を把握し、「学んだ教訓」を組織に適用する。

6.4 Modernising the Pharmaceutical Quality System

6.4 医薬品品質システムの最新化

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.	現行の医薬品品質システムに、最新の品質リスクマネジメントの原則とグッドデータマネジメントプラクティスを適用することで、システムを最新化し、複雑なデータの生成に伴う困難に対応できるようになる。
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: • Quality Risk Management, • Investigation programs, • Data review practices (section 9), • Computerised system validation,	会社における医薬品品質システムは、データインテグリティ違反につながりそうなシステム又はプロセスの弱点を予防・検出・是正できるようなものとする。会社は、データのライフサイクルを把握し、生成されるデータが有効で、完全で、信頼できるものとなるように、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、そのようなコントロールや手順の変更は以下の領域で行われる： • 品質リスクマネジメント • 調査プログラム • データレビューの実施 (第 9 章)

	• 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.	• コンピュータ化システムバリデーション • IT インフラ、サービス、セキュリティ (物理的及び仮想的) • ベンダー・契約者の管理 • トレーニングプログラム。会社のデータガバナンスへの取り組みとデータガバナンス SOP を含む。 • 完成した記録の保存・処理・転送・検索。分散型・クラウド型のデータ保存・処理・転送に係る活動を含む。 • データインテグリティの期待に応えるための要件、例えばユーザー要求仕様書等 (第 9.2 章参照) を実現する、GMP/GDP に不可欠な機器及び IT インフラを購入する際の適切な監督 • 自己点検プログラム。データ品質とデータインテグリティを含む。 • パフォーマンス指標 (品質メトリクス) と上級管理職への報告

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

6.5 定期的なパフォーマンス指標 (品質メトリクスを含む) のマネジメントレビュー

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.	定期的にパフォーマンス指標 (データインテグリティに関連するものを含む) のマネジメントレビューを行い、重要な問題を特定し、タイムリーにエスカレートし、対処すべきである。重要パフォーマンス指標 (KPI) を選択する際は十分注意し、意図に反してデータインテグリティを軽視する文化が出来上がってしまったということのないようすべきである。
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.	品質部門の責任者から上級管理職に直接リスクを伝えるルートを確保すべきであり、上級管理職があらゆる問題を認識し、対応するために資源を割り当てられるようにする。
6.5.3	Management can have an independent expert periodically verify the effectiveness of their systems and controls.	管理職は、独立した専門家に自社のシステムとコントロールの有効性を定期的に検証させてもよい。

6.6 Resource allocation

6.6 資源の割り当て

6.6.1	Management should allocate appropriate resources to support and sustain good data integrity management such that the workload and pressures on those responsible for data generation and record keeping do not increase the likelihood of errors or the opportunity to deliberately compromise data integrity.	管理職は、グッドデータインテグリティマネジメントを支援・維持するために、適切な資源を割り当てる必要がある。それにより、データ生成や記録保管を行う者への過大な負荷やプレッシャーによる作業ミスの可能性やデータインテグリティを意図的に損なう機会を増大させないようにする。
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.	組織の業務に見合った、品質及びマネジメントの観点からの監督、IT サポート、調査の実施、トレーニングプログラムの管理を行うためには十分な人数の社員が必要である。
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	取り扱うデータの重要度に応じて、ニーズに合った機器・ソフトウェア・ハードウェアを購入するための規定が必要である。会社は、ALCOA+[5] の原則への適合状況の改善につながり、その結果、データ品質とデータインテグリティに関する弱点を減らすような技術的

	compliance with ALCOA+[5] principles and thus mitigate weaknesses in relation to data quality and integrity.	ソリューションを導入すべきである。
6.6.4	Personnel should be qualified and trained for their specific duties, with appropriate segregation of duties, including the importance of good documentation practices (GdocPs). There should be evidence of the effectiveness of training on critical procedures, such as electronic data review. The concept of good data management practices applies to all functional departments that play a role in GMP/GDP, including areas such as IT and engineering.	社員は、それぞれの職務に対して適格で、トレーニングされるべきである。また適切な職務分離を行うべきである。トレーニングにはグッドドキュメンテーションプラクティス (GdocPs) の重要性も含まれる。また、電子データのレビュー等の重大な手順については、トレーニングの有効性を示す証拠が必要である。グッドデータマネジメントプラクティスの概念は GMP/GDP で何らかの役割を果たす、すべての機能部門 (IT やエンジニアリング等の領域を含む) 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.	データ品質とデータインテグリティは全員が知っているべきであるが、様々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) を集め、一致協力して調査を実施・支援し、システムギャップを特定し、改善策の実施を推進してもらってもよい。
6.6.6	Introduction of new roles in an organisation relating to good data management such as a data custodian might be considered.	組織に、データ管理人等の、グッドデータマネジメントに関連する新しい役割の導入を検討してもよいであろう。

6.7 Dealing with data integrity issues found internally

6.7 社内で発見されたデータインテグリティ問題への対応

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違反が見つかったときは、医薬品品質システムにおける逸脱行為と同様に対処すべきである。問題の広がりとその根本原因を特定し、その問題を全面的に是正し、予防措置を実施することが重要である。さらなる専門技術知識や見解を得るために第三者を利用することも含まれ、システムの弱点を特定するためにギャップアセスメントを行う場合もある。
6.7.2	When considering the impact on patient safety and product quality, any conclusions drawn	患者の安全や製品の品質への影響を考慮する

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

	should be supported by sound scientific evidence.	ときは、導き出す結論は健全な科学的証拠によって裏付けられている必要がある。
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.	〔問題の〕修正には、製品の回収、顧客への通知及び規制当局への報告等が含まれる。修正及び是正措置の計画とその実施状況は、記録し、監視すべきである。
6.7.4	Further guidance may be found in section 12 of this guide.	本書、第 12 章にさらなる詳細のガイダンスを掲載する。

7. GENERAL DATA INTEGRITY PRINCIPLES AND ENABLERS

7. データインテグリティの一般原則と実現手段

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、原薬と医薬品のライフサイクルの様々な段階を通して実施すべきであり、科学的かつリスクに基づいたアプローチの利用を奨励すべきである。
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).	十分な情報をもとに意思決定することを確実にし、またその情報の信頼性を検証するためには、その意思決定に使われる情報の元となるイベントやアクションを十分に文書化する必要がある。このように、GdocPs は、データインテグリティを確実にする上で重要であり、適切に設計された医薬品品質システム (第 6 章参照) には不可欠な要素である。
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.	GdocPs をどのように適用するかは、データを記録する媒体 (すなわち、物理的な記録か、電子的な記録か) によって異なるが、その原則はどちらにも適用される。この章では重要な原則を紹介し、次の章 (第 8 章と第 9 章) で、紙ベースの記録保管と電子ベースの記録保管のそれぞれの文書化について原則を深堀りする。
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	いくつかの GdocPs の重要な概念は、ALCOA という頭字語でまとめられる。すなわち帰属性 (Attributable) 、判読性 (Legible) , 同時記録性 (Contemporaneous) 、 原本性 (Original) 及び正確性 (Accurate) である。 これに完全性

	(ALCOA+[6]). Together, these expectations ensure that events are properly documented and the data can be used to support informed decisions.	(Complete) 、 (一貫性) (Consistent) 、永続性 (Enduring) 及び 可用性 (Available) といった属性を加えることがある (ALCOA+[6])。これらの期待に応えることで、イベントが適切に文書化され、そのデータをもとに、十分な情報に基づく意思決定が行われる。
7.5	Basic data integrity principles applicable to both paper and electronic systems (i.e. ALCOA +):	紙媒体と電子システムの両方に適用されるデータインテグリティの基本原則 (すなわち ALCOA+) を以下に示す：

Data Integrity Attribute	**Requirement**	**要件**
Attributable 帰属性	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.	タスクを実行し記録を残した個人又はコンピュータ化システムを特定するとともに、そのタスクをいつ実行したかも特定できるようにする必要がある。これは、誰が、いつ、何のために変えたのかを知ることが重要な場合、記録に加えられるすべての変更 (修正・削除・変更等) にも当てはまる。
Legible 判読性	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.	すべての記録には判読性が必要である、すなわち情報を理解し、利用するためには、読むことができ、かつ明瞭であることが必要である。これは、「完全性」を満たす必要のあるすべての情報 (「原本性」のある記録や入力を含む) に適用される。電子データの「動的」な性質 (検索、クエリ、傾向分析等ができるか) が記録の内容と意味に重要な場合、適切なアプリケーションを使用してデータを対話形式で操作できることは、記録の「可用性」を満たすために重要である。

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

Data Integrity Attribute	**Requirement**	**要件**
Contempo-raneous 同時記録性	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、意思決定の証拠は、それらが行われると同時に記録されるべきである。このような文書化により、何が行われたか、又はどのような理由で何が決定されたか (すなわちその時の決定に何が影響したか) を正確に立証することができる。
Original 原本性	The original record can be described as the first-capture of information, whether recorded on paper (static) or electronically (usually dynamic, depending on the complexity of the system). Information that is originally captured in a dynamic state should remain available in that state.	原本記録とは、紙に記録されている (静的) か、電子的に記録されている (システムの複雑さにもよるが、通常は動的) かを問わず、情報を最初の取得したものである。動的な状態で最初に取得された情報は、その状態のまま利用可能にしておくべきである。
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.	正確性を持つためには、記録は事実を忠実に表現する必要がある。強固な医薬品品質システムの多くの要素を用いて記録の正確性を確実にすることができる。これらの要素には以下がある： • 機器に関連する要因。例えば、適格性評価、キャリブレーション、メンテナンス、コンピュータ〔化システム〕バリデーション等。 • アクションと行動をコントロールするための方針と手順。手順的要件の遵守を検証するデータレビュー手順を含む。 • 逸脱管理。根本原因の分析、影響アセスメント、CAPA を含む。 • 訓練を受けた適格な社員。確立された手順に従うことの重要性、及び自らのアクションや意思決定を文書化することの重要性を理解している。 これらの要素を組み合わせて (製品品質についての重要な意志決定に用いられる科学的データ等の) 情報の正確性を確実にする。

Data Integrity Attribute	**Requirement**	**要件**
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).	あるイベントを理解しようとするときには、そのイベントを再現するために不可欠となるすべての情報が重要である。情報が消失したり削除されたりしないようにすることが大事である。一連の情報が完全性を満たすために必要とされる詳細レベルは、情報の重要度 (第 5.4 章のデータ重要度を参照) によって異なる。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 (第 9 章参照) 。
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、一貫性のある、論理的な方法で作成・処理・保存されるべきである。その方法には、データのコントロールや標準化に役立つポリシーや手順が含まれる (例えば、時系列の順序、日付のフォーマット、測定単位、数値の丸め方、有効桁数等) 。
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、必要とされる可能性のある全期間にわたって存在するように保管されるべきである。すなわち、保存期間中、消えない/継続して残る【訳注】記録として、変わることなく、アクセスでき続ける必要がある。 【訳注：不揮発性の記憶媒体等。】
Available 可用性	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、必要とされる保存期間を通して常時利用可能であるべきであり、日常的なリリースの決定・調査・傾向把握・年次報告・監査・査察等の目的を問わず、レビューに責任を持つすべての該当する社員が見読性のあるフォーマット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	これらの要素が、GMP 及び GDP に関連する活動のすべての領域に適切に適用され、医薬品品質システムの他の支援要素とともに適用されるならば、医薬品に関する重大な決定を

	regarding drug products should be adequately assured.	行うための情報の信頼性は十分に保証されるはずである。

7.7 True copies

7.7 真正コピー

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).	一般的に、紙の原本記録 (例えば、分析サマリレポート、バリデーション報告書等) のコピーは、 (例えば、別の場所で操業する会社間の) 連絡に用いるうえで非常に便利である。これらの記録はライフサイクルを通してコントロールし、他施設 (グループ会社、請負業者等) から受け取ったデータを必要に応じて「真正コピー」として維持管理すべきである。また、 (複雑な分析データのサマリ等のように) 〔データが〕「真正コピー」の要件を満たさない場合は、「サマリレポート」として用いる。
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.	静的な記録において原本データのインテグリティが保たれていることを合理的に説明できる場合には、電子的手段で生成された生データを、許容可能な紙又は PDF 形式で保管することが考えられる。ただし、データ保管プロセスは、医薬品の品質のすべての側面に直接的又は間接的に影響するすべての活動に関するすべてのデータ (メタデータを含む) を記録すべきである。 (例えば、分析の記録には、生データ・メタデータ・関連する監査証跡及び結果ファイル・各分析実行に固有のソフトウェア/システム構成設定・所定の生データセットの再現に必要なすべてのデータ処理実行 (メソド及び監査証跡を含む) が含まれる) 。印刷された記録が〔生データの〕正確な表現であったことを検証するための文書化された手段も必要となるであろう。このアプローチは、記録を GMP/GDP に適合させるためには、業務管理的負担が大きくなる可能性が高い。
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	多くの電子記録は、データとの対話ができるように、動的な形式で保管することが重要である。データインテグリティのため、又は後で検証するために不可欠であれば、データを動的な形式で保管すべきである。リスクマネジメントの原則を活用し、データを動的な形

	long data should be stored in a dynamic format.	式で格納する必要性及び〔動的な形式で保管する〕期間の判断を合理的に説明できるようにすべきである。
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.	記録を受け取る拠点では、これらの記録 (真正コピー) を、紙又は電子形式 (例：PDF) のいずれかで管理し、承認された QA 手順に従ってコントロールする必要がある。
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.	万全の注意を払い、文書が「真正コピー」であることを確実に証明できるようにすべきである。これは、文書の真正性を容易に検証できる方法 (手書き署名又は電子署名を使用する、又は真正コピーを作成するためのバリデートされたプロセスに従って〔真正コピーを〕生成する等) で行う。

Item:	**How should the “true copy” be issued and controlled?**	**「真正コピー」はどのように発行し、コントロールすべきか？**
1.	**Creating a “true copy” of a paper document.** At the company who issues the true copy: - Obtain the original of the document to be copied - Photocopy the original document ensuring that no information from the original copy is lost; - Verify the authenticity of the copied document and sign and date the new hardcopy as a “true copy”; The “True Copy” may now be sent to the intended recipient. **Creating a “true copy” of a electronic document.** A ‘true copy’ of an electronic record should be created by electronic means (electronic file copy), including all required metadata. Creating pdf versions of electronic data should be prohibited, where there is the potential for loss of metadata. The “True Copy” may now be sent to the intended	**紙の文書の「真正コピー」を作成する。** 真正コピーを発行する会社において： - コピーする文書の原本を入手する。 - 原本の情報が失われないように、原本のコピーを取る。 - コピーされた文書の真正性を検証し、新しいハードコピーに「真正コピー」として署名と日付を記入する。 これで「真正コピー」を受領者に送ることができる。 **電子文書の「真正コピー」を作成する。** 電子記録の「真正コピー」は、電子的手段 (電子的なファイルコピー) で作成し、必要なメタデータをすべて含むべきである。メタデータが失われる可能性がある場合、電子データの PDF 版の作成は禁止すべきである。 これで「真正コピー」を受領者に送ることができる。

	recipient. A distribution list of all issued "true copies" (soft/hard) should be maintained.	発行されたすべての (ソフト/ハードの)「真正コピー」の配布先リストを維持管理する必要がある。
	Specific elements that should be checked when reviewing records: • Verify the procedure for the generation of true copies, and ensure that the generation method is controlled appropriately. • Check that true copies issued are identical (complete and accurate) to original records. Copied records should be checked against the original document records to make sure there is no tampering of the scanned image. • Check that scanned or saved records are protected to ensure data integrity. • After scanning paper records and verifying creation of a 'true copy': - 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.	**記録をレビューする際にチェックすべき具体的事項：** • 真正コピーを生成する手順を検証し、生成方法が適切にコントロールされていることを確認する。 • 発行された真正コピーが原本の記録と同一 (完全かつ正確) であることをチェックする。コピーされた記録を、原本の文書記録と照合し、スキャンされたイメージが変更されていないことをチェックする。 • データインテグリティを確実にするためにスキャンした記録や保存した記録を保護していることをチェックする。 • 紙の記録をスキャンし、「真正コピー」の作成を検証した後： - (顧客に送付する等) 配布の目的で真正コピーを作成する場合は、記録のオーナーはスキャンイメージの元となった原本文書をそれぞれの保存期間に合わせて保管する必要がある【訳注】。 【訳注：原文では 誤って "Where ～ from which the" が 2 回繰り返されている。】 - 文書保管の目的で真正コピーを作成する場合は、スキャンイメージの元となった原本の記録文書の代わりにコピーを保管してもよい。
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. The document should clearly indicate that it is a true copy and not an original record.	真正コピーを受け取った会社において： - 紙のバージョン、スキャンしたコピー、又は電子ファイルは、レビューし、GdocPs に従ってファイリングする必要がある。 文書には、それが原本の記録ではなく、真正コピーであることを明確に示す必要がある。

	Specific elements that should be checked when reviewing records: • 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.	**記録をレビューする際にチェックすべき具体的事項：** • 受け取った記録を確認し、適切に保管していることをチェックする。 • 署名者の正しさの検証等により「真正コピー」の真正性を検証するシステムが設けられていること。

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.	品質合意書を締結し、「真正コピー」の生成・転送に関する責任及びデータインテグリティのコントロールの責任を定める必要がある。契約委託者及び受託者は「真正コピー」を発行及びコントロールするシステムを監査し、そのプロセスが堅牢であり、データインテグリティの原則を満たしていることを確実にすべきである。

7.8 Limitations of remote review of summary reports

7.8 サマリレポートのリモートレビューの限界

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.	一般的にサマリレポート内のデータをリモートレビューすることは必要であるが、データインテグリティの適切なコントロールを実現するためには、リモートデータレビューの限界を十分に理解しておく必要がある。
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.	データのサマリレポートは、物理的に離れた場所にある製造拠点、製造販売業者、その他の関係者の間でやりとりされることが多い。しかし、サマリレポートには、重大なサポートデータやメタデータが含まれていないことが多く、したがって原本データをレビューすることにならない。この点で、本質的に限界が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、サマリレポートはデータ転送プロセスの一部にすぎないと考え、利害関係者や査察者は、サマリレポートのデータのみに依存しないようにすることが重要である。
7.8.4	Prior to acceptance of summary data, an evaluation of the supplier's quality system and	サマリデータを受け入れる前に、提供する側の品質システムとデータインテグリティの原

	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.	則への 適合性についての評価を確立しておく必要がある。データインテグリティの原則への適合性を机上やそれに類するアセスメントで判断することは、一般的に許容されるものではなく、また不可能であろう。
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.	外部組織の場合、これ〔データインテグリティの原則への適合性〕が品質リスクマネジメントの観点から重要と考えられる場合には、オンサイト監査により判断すべきである。監査では、その会社により生成されたデータの信憑性を確認するとともに、サマリデータやサマリレポートの作成・配布に用いられている仕組みのレビューを行うべきである。
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.).	サマリデータが同一組織の異なる拠点間で配布されている場合、提供する側となる拠点の適合性の評価は、別の手段 (例：会社の手順に対する適合性の証拠、内部監査報告書等) によって判断することができる。
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.	サマリデータは、原本を持つ拠点の許可されたスタッフが、合意された手順に従って用意し、レビュー・承認すべきである。サマリには、Authorized Person により署名された、サマリの真正性及び正確性を示す宣言書を添付すべきである。サマリレポートの作成・転送・検証に関する取り決めは、品質/技術合意書に盛り込むべきである。

8. SPECIFIC DATA INTEGRITY CONSIDERATIONS FOR PAPER- BASED SYSTEMS

8. 紙ベースのシステムにおけるデータインテグリティに関する具体的な検討事項

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

8.1 医薬品品質システムの構造とブランクのフォーム/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.	紙ベースの文書を効果的に管理することは、GMP/GDP の重要な要素である。したがって、文書システムは、GMP/GDP の要件を満たすように設計し、文書及び記録が効果的にコントロールされ、インテグリティが確実に維持されるようにすべきである。
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.	紙の記録をコントロールし、データライフサイクルを通して、帰属性・判読性・同時記録性・原本性・正確性・完全性・一貫性・永続性 (消えない/継続して残る) ・可用性 (ALCOA+) を維持する必要がある。
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: • 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	医薬品品質システムの枠組みの中で、GdocPs 及び文書コントロールの取り決めを概説した手順書を用意すべきである。手順書には、データライフサイクルを通してどのようにデータインテグリティを維持するかを明記すべきであり、以下が含まれる： • マスターとなる文書及び手順の作成・レビュー・承認。 • データ (マスターデータ、ログデータ等) を記録するためのテンプレートの生成・配布・コントロール。 • 記録に関する検索及び災害復旧のプロセス。 • 日常的に使用するための文書の作業用コピーの作成。 (SOP やブランクフォーム等の) 文書のコピーが、コントロールされた、追跡可能な方法で発行し、利用後の照合を行うことに特に重点を置く。 • 紙ベースの文書の完成。個々のオペレーターを識別方法するか、データ入力フォーマット、記録の修正、及び日常的な正確性・真正性・完全性のレビューついて

	disposal of records.	定める。 • 記録のファイリング・検索・保管・アーカイブ・廃棄。

8.2 Importance of controlling records

8.2 記録をコントロールすることの重要性

8.2.1	Records are critical to GMP/GDP operations and thus control is necessary to ensure: • 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.	記録は GMP/GDP 業務に不可欠であり、以下を確実にコントロールする必要がある： • 実行した活動の証拠。 • GMP/GDP 要件及び会社の方針・手順・作業指示書への適合性を示す証拠。 • 医薬品品質システムの有効性。 • トレーサビリティ。 • プロセスの真正性と一貫性。 • 製造された医薬品がグッドクオリティ属性を持つことの証拠。 • 苦情やリコールが発生した場合、記録は調査に使用される可能性がある。 • 逸脱や検査不合格の場合、記録は、調査を効果的に完遂するために重要である。

8.3 Generation, distribution and control of template records

8.3 テンプレート記録の作成、配布、コントロール

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).	マスター文書を管理及びコントロールすることは、誰かが「通常の手段」で (すなわち、専門的な不正行為の技術を使わずに) 記録を不適切に使用及び(又は) 改ざんするリスク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。品質リスクマネジメントアプローチを用いて以下の期待事項を、記録されたデータリスクとデータ重要度 (第 5.4 章、第 5.5 章参照) を考慮し、実施すべきである。

8.4 Expectations for the generation, distribution and control of records

8.4 記録の作成、配布、コントロールに関する期待事項

Item:	Generation	作成
1.	**Expectation** All documents should have a unique identifier (including the version number) and should be checked, approved, signed and dated. The use of uncontrolled documents should be prohibited by local procedures. The use of temporary recording practices, e.g. scraps of paper should be prohibited.	**期待事項** すべての文書には一意の識別子 (バージョン番号を含む) を付け、チェック及び承認し、日付を入れて署名する必要がある。 コントロールされていない文書の使用は、ローカル手順により禁止すべきである。紙の切れ端等に一時的に記録するようなやり方は禁止すべきである。
	Potential risk of not meeting expectations/items to be checked • Uncontrolled documents increase the potential for omission or loss of critical data as these documents may be discarded or destroyed without traceability. In addition, uncontrolled records may not be designed to correctly record critical data. • It 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.	**期待事項を満たさない場合の潜在的なリスク/チェックすべき項目** • コントロールされていない文書は、廃棄・破棄されても追跡できない場合があり、重要なデータが欠けたり、消失してしまう可能性が高くなる。また、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かもしれない。 • コントロールされていない記録の方が、改ざんしやすいかもしれない。 • 一時的に記録するやり方を用いることでデータの漏れが発生するかもしれない。また、一時的な記録を原本保管するよう定めていないかもしれない。 • 記録の生成及びアクセスがコントロールされていない場合、イベントが発生した時点で記録していないかもしれない。 • バージョンや発行をコントロールしていない場合、古いフォームを使用してしまうリスクがある。
2.	**Expectation** The document design should provide sufficient space for manual data entries.	**期待事項** 文書には、手書きでデータ入力するための十分な記入スペースを確保するよう設計する必要がある。

	Potential risk of not meeting expectations/items to be checked • 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.	**期待事項を満たさない場合の潜在的なリスク/チェックすべき項目** • データ入力用の記入スペースが十分に確保されていないと、手書きのデータは明瞭でなくなり、判読できなくなる可能性がある。 • 文書は、コメントのための十分な記入スペースを設けるように設計すべきである。例えば、転写エラーの場合、オペレーターが、間違った箇所に取り消し線を引き、イニシャルと日付を記入し、求められている説明を記録するための十分な記入スペースが必要である。 • 文書を完成させるために文書にページを追加する場合は、追加したページの数と参照を本体の記録に明確に記載し、署名する必要がある。 • 文書フォーマットには、必要なすべてのデータを追記するための十分な記入スペースを設ける必要がある。ところかまわず、データを記録すべきではない。例えば、記録用に意図されていない、印刷ページの裏面には記録しないようにする。
3.	**Expectation** The document design should make it clear what data is to be provided in entries.	**期待事項** 文書は、どのようなデータを入力すべきかを明確にするよう設計する必要がある。
	Potential risks of not meeting expectations/items to be checked • 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.	**期待事項を満たさない場合の潜在的なリスク/チェックすべき項目** • 曖昧な指示により、一貫性・正確性のないデータが記録されるかもしれない。 • 適切に設計されれば、すべての重要なデータが確実に記録され、また入力し完成した記録の明瞭性・同時記録性・永続性(消えない/継続して残る) が確実になる。 • 重要なデータをうっかり記録し忘れるリスクを最小限にするために、運用プロセスや関連する SOP と同じ順序で情報を記録するように文書を構成すべきであ

		る。
4.	**Expectation** Documents should be stored in a manner which ensures appropriate version control. 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. Master documents (in electronic form) should be prevented from unauthorised or inadvertent changes. E.g.: For the template records stored electronically, the following precautions should be in place: - access to master templates should be controlled; - process controls for creating and updating versions should be clear and practically applied/verified; and - master documents should be stored in a manner which prevents unauthorised changes.	**期待事項** 文書は、適切なバージョンコントロールが確実に行われるような方法で保存すべきである。 マスター文書には、コピーと区別するための明確なマーキングを施すべきである。例えば、誤って使用されないよう、色付きの紙やインクを使用する。 (電子形式の) マスター文書への、許可のない又は不注意による変更を防止すべきである。 例：電子的に保存されているテンプレート記録については、以下のような用心が必要である： - マスターテンプレートへのアクセスがコントロールされている。 - 〔テンプレート記録を〕作成し、バージョンを更新するためのプロセスコントロールは明確であり、実際に適用/検証されている。 - マスター文書が、無許可の変更を防ぐような方法で保存されている。
	Potential risk of not meeting expectations/items to be checked • 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.	**期待事項を満たさない場合の潜在的なリスク/チェックすべき項目** • 保存条件が不適切だと、文書が許可なく変更されたり、期限切れの文書及び (又は) ドラフト文書が使用されたりするかもしれない。またマスター文書の消失を引き起こすかもしれない。 • 実施するためのプロセスと、必要に応じて実施前に行う適切なトレーニングによる効果的なコミュニケーションは、文書と同様に重要である。

Item:	Distribution and Control	配布とコントロール
1.	**Expectations** Updated versions should be distributed in a timely manner. Obsolete master documents and files should be archived and their access restricted. Any issued and unused physical documents should be retrieved and reconciled. Where authorised by Quality, recovered copies of documents may be destroyed. However, master copies of authorised documents should be preserved.	**期待事項** 最新版は、タイムリーに配布すべきである。 旧版のマスター文書やファイルはアーカイブし、そのアクセスを制限すべきである。 発行済みの未使用の物理的文書は、すべて回収し、照合する必要がある。 品質〔部門〕が許可している場合は、回収したコピーを破棄してもよい。ただし、承認された文書のマスターコピーは保管すべきである。
	Potential risk of not meeting expectations/items to be checked • There may be a risk that obsolete versions can be used by mistake if available for use.	**期待事項を満たさない場合の潜在的なリスク/チェックすべき項目** • 旧版が利用可能な状態にあると、誤って使用してしまう危険性がある。
2.	**Expectation** 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	**期待事項** 文書の発行は、書面による手順に従ってコントロールすべきである。そこには以下のコントロールが含まれる： • 誰が、いつコピーを発行したかの詳細。 • 文書の承認されたコピーを区別する明確な手段。例えば、セキュリティスタンプ、作業エリアにはない紙の色、又は他の適切なシステムの使用。 • 最新の承認版のみが利用可能となることを確実にする。 • 発行した各ブランク文書に一意の識別子を割り振り、各文書の発行を登録簿に記録する。 • 配布されたコピーに番号 (例：コピー2 の 2) を付け、発行されたページは束ねて製本し、連番を付ける。 • ブランクテンプレートのコピーを追加で再発行する必要がある場合は、コントロールされた再発行プロセスに従うべきで

	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.	ある。そのプロセスには、配布済みのすべてのコピーを管理し、追加コピー要求の合理性と承認を記録する必要がある。例：「原本のテンプレート記録が破損した。」 • 重要な GMP/GDP のブランクフォーム (例：ワークシート、ラボノート、バッチ記録、コントロール記録) は、使用後に照合し、記録の正確性と完全性を確認すべきである。 • (手順書等の) 記録以外の文書のコピーを参照用にのみ印刷する場合、照合を行う必要はない。ただし、文書の生成時にタイムスタンプが付され、短期間でのみ有効である旨が文書に記されることを条件とする。
	Potential risk of not meeting expectations/items to be checked • 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.	**期待事項を満たさない場合の潜在的なリスク/チェックすべき項目** • セキュリティ対策がないと、ユーザーがテンプレートをコピー又はスキャンして (テンプレートのコピーをもう一つ使えるようにして) データの書き換えや改ざんを行うリスクがある。 • 旧版が、意図的又は誤って使用される可能性がある。 • 異常なデータが入力された記録が、書き直されたテンプレートで置き換えられる可能性がある。 • 未使用のフォームは員数を明らかにし、使用できないようにして破棄するか、回収して安全にファイリングする。 • 文書の参照用コピーが使用されている場合は、その文書に生成日、有効期間、及び参照用であって正式なコピーではない旨を示す明確な記載 (例：「印刷版はコントロール外」) があるかチェックする。

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.).	医薬品品質システムの枠組みで、承認されたすべてのマスター文書 (SOP・フォーム・テンプレート・記録) のインデックスを維持管理すべきである。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こと：文書名、版番号を含む識別子、場所 (例：文書データベース) 【訳注】、発効日、次回レビュー日等)。 【訳注：原文で誤っていると思われる括弧の位置を正した。】

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

8.5 使用場所における記録〔用紙〕の使用と管理

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〔用紙〕は、オペレーターの使用場所で用意しておくようにし、これらの記録〔用紙〕を管理するために適切なコントロールを設けるべきである。これらのコントロールを実施し、記録の損傷や消失のリスクを最小限に抑え、データインテグリティを確実にすべきである。必要に応じて、記録〔用紙〕が汚れる (例：水に濡れる、物質で汚れる等) ことのないように保護する手段を講じるべきである。
8.5.2	Records should be appropriately controlled in these areas by designated persons or processes in accordance with written procedures.	記録〔用紙〕は、これらの場所において、指名された者又はプロセスにより、書面による手順に基づいて適切にコントロールされるべきである。

8.6 Filling out records

8.6 記録〔用紙〕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.	記録〔用紙〕に適切に記入されることを確実にするために、下表の項目をコントロールする必要がある。

Item:	Completion of records	記録の完成
1.	**Expectations** Handwritten entries should be made by the person who executed the task[7]. Unused, blank fields within documents should be voided (e.g. crossed-out), dated and signed. Handwritten entries should be made in clear and legible writing. 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.	**期待事項** 手書きでの入力は、そのタスクを実行した者が行うべきである [7]。 文書内の未使用のブランク欄は、無効にし (例：クロスアウト) 、日付を入れて署名する。 手書きの場合は、はっきりと読みやすい文字で記入する。 日付欄の入力は、拠点で定義された、曖昧さのない形式を使う必要がある。例えば dd/mm/yyyy 又は mm/dd/yyyy。
	Potential risk of not meeting expectations/items to be checked • 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.	**期待事項を満たさない場合の潜在的なリスク /チェックすべき項目** • 同一者による入力は、筆跡に一貫性があることをチェックする。 • 入力内容が判読でき、明瞭である (すなわち、曖昧さがない) こと、及び未知の記号や略語 (例えば、同上を示す記号 (〃)の使用) が使用されていないことをチェックする。 • 記録されたデータが完全であるかどうかチェックする。 • 記録に正しくページが振られ、すべてのページが揃っていることをチェックする。
2.	**Expectation** Records relating to operations should be completed contemporaneously[8].	**期待事項** 操作に関する記録は、〔操作と〕同時に完成させる必要がある [8]。
	Potential risk of not meeting expectations/items	**期待事項を満たさない場合の潜在的なリスク**

[7] Scribes may only be used in exceptional circumstances, refer footnote 8.
[7] 記録者は、例外的な状況下でのみ使用することができる。脚注 8 を参照のこと。
[8] The use of scribes (second person) to record activity on behalf of another operator should be considered ‘exceptional’, and only take place where: …
【訳注：脚注が長いため、本書末尾に移しました。】

	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.	**/チェックすべき項目** • 記録〔用紙〕が使用場所のすぐ近くに用意されていることを検証する。すなわち、査察官は、操作の行われている現場で連続的に記録できるようになっているかどうかを見るべきである。使用場所でフォームが用意されていないと、オペレーターが〔イベント〕発生時に記録〔用紙〕に入力することができない。
3.	**Expectation** Records should be enduring (indelible).	**期待事項** 記録は永続性を持つ (消せない) べきである。
	Potential risk of not meeting expectations/items to be checked • 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.	**期待事項を満たさない場合の潜在的なリスク /チェックすべき項目** • 記入した内容は、インクで書かれており、消せない、及び(又は) (保存期間中に) 汚れたり消えたりしないことをチェックする。 • 鉛筆で記入した上から、ペンでなぞって (上書き) いないことをチェックする。 • システムからのプリントアウトは、感熱紙等時間の経過とともに色あせてしまうものもあることに注意する。このような場合、署名と日付の入った鮮明な真正コピーを作成し、保管する必要がある。
4.	**Expectation** Records should be signed and dated using a unique identifier that is attributable to the author.	**期待事項** 記録には、記入者に帰属するユニークな識別子を用いて署名し、日付を記入する必要がある。
	Potential risk of not meeting expectations/items to be checked • Check that there are signature and initials logs, that are controlled and current and that demonstrate the use of unique examples, not just standardized printed letters. • Ensure that all key entries are signed & dated, particularly if steps occur over time, i.e. not just signed at the end of the page	**期待事項を満たさない場合の潜在的なリスク /チェックすべき項目** • 署名やイニシャルのログがあることをチェックする。そのログはコントロールされ、最新であり、標準的な印刷活字だけでなく〔署名者を特定できる〕ユニークな例の使用が示されていること。 • すべての重要な入力箇所に署名と日付が

	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.	入っていることを確認する。特に、時間をかけて実行されるステップでは、ページ及び (又は) プロセスの最後に署名するだけでは不十分である。 • 印鑑の使用は一般的に推奨されていない。使用する場合は、アクセス管理する必要がある。個人と印鑑の間を明確に関連づけるログが必要である。印鑑の使用を受け入れるためには、印鑑を使用した際に (〔印鑑の〕所有者が) 日付を記入する必要がある。

8.7 Making corrections on records

8.7 記録の修正

	Corrections to the records should be made in such way that full traceability is maintained.	記録の修正は、トレーサビリティが完全に維持されるような方法で行う必要がある。

Item:	How should records be corrected?	記録の修正はどのように行うか？
1.	**Expectation** Cross out what is to be changed with a single line. Where appropriate, the reason for the correction should be clearly recorded and verified if critical. Initial and date the change made.	**期待事項** 変更したい部分に一本線で取り消し線を引く。 必要に応じて、修正理由を明記し、重要な場合は検証すべきである。 変更した箇所にイニシャルと日付を入れる。
	Specific elements that should be checked when reviewing records: • 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.	**記録をレビューする際にチェックすべき具体的事項：** • 原本データが読めること、隠されていないことをチェックする。(例：修正液によって隠されていない。〔元のデータの上への〕重ね書きは許されない。) • 重要な入力データに変更が加えられている場合、変更の正当な理由が記録され、変更を裏付ける証拠が用意されていることを検証する。 • 記録の中に説明のない記号や入力がない

		ことをチェックする。
2.	**Expectation** Corrections should be made in indelible ink.	**期待事項** 訂正は消えないインクで行う。
	Specific elements that should be checked when reviewing records: • 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).	**記録をレビューする際にチェックすべき具体的事項:** • 記入は、インクで行われており、消せない、及び (又は) (保存期間中に) 汚れたり消えたりしないことをチェックする。 • 鉛筆で記入した上からペンでなぞって (上書き)いないことをチェックする。

8.8 Verification of records (secondary checks)

8.8 記録の検証 (二次チェック)

Item:	When and who should verify the records?	いつ、誰が記録を検証すべきか？
1.	**Expectation** 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. Batch production records of non-critical process steps is generally reviewed by production personnel according to an approved procedure. 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.	**期待事項** 重要なプロセスステップ (例：バッチ記録内の重要なステップ) は以下のように検証すべきである： • 操作が行われる時点で、独立した、指名された社員がレビュー/立ち会いを行う。 • 品質部門に送付する前に、製造部門内の許可された者がレビューする。 • 製造されたバッチをリリース又は配送する前に、品質部門 (例：Authorised Person、Qualified Person) がレビューし、承認する。 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って生産部門の社員がレビューする。 ラボにおける試験実施手順の記録は、試験完了後、指名された社員 (例：第二分析者) がレビューすべきである。レビュー者は、すべての記入事項や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

	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. This verification should be conducted after performing production-related tasks and activities and be signed or initialled and dated by the appropriate persons. Local SOPs should be in place to describe the process for review of written documents.	の信頼性について適切なアセスメントを行うことが期待されている。 重要なテストの解釈 (例：寒天培地上の微生物コロニーの記録) をただ一人で行う場合には、追加のコントロールを設けることを検討すべきである。リスクマネジメントの原則に基づき、二次レビューが必要かもしれない。場合によっては、このレビューをリアルタイムで行う必要がある。〔レビューの〕代わりに、保存用のデータの写真画像を撮影する等、重要なデータを適切な電子的手段を使って検証してもよい。 この検証は、製造に関連するタスクや活動を行った後に実施し、適切な者が署名するかイニシャルを記して、日付を記入する必要がある。 作成された文書をレビューするプロセスを記述したローカル SOP を設ける必要がある。
	Specific elements that should be checked when reviewing records: • 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.	**記録をレビューする際にチェックすべき具体的事項：** • 処理が行われている場所における製造記録の取り扱いプロセスを検証し、記録に関連する活動を実行する時に、適切な社員が〔製造記録を〕すぐに利用できるようになっていることを確認する。 • 処理中に行われたすべての二次チェックが、製造監督者や QA 等、適切な資格を持った独立した社員により行われたことを検証する。 • 操作が終了した後で、まず生産〔部門〕の社員、続いて品質保証〔部門〕の社員が文書をレビューしていることをチェックする。

Item:	How should records be verified?	記録はどのように検証すべきか？
2.	**Expectation** Check that all the fields have been completed correctly using the current (approved) templates, and that the data was critically compared to the acceptance criteria. Check items 1, 2, 3, and 4 of section 8.6 and Items 1 and 2 of section 8.7	**期待事項** 最新の (承認された) テンプレートを使って、すべての欄が正しく埋められていることをチェックする。またデータの受入基準との比較を批判的に行っていることをチェックする。 第 8.6 章の項番 1、2、3、4 と第 8.7 章の項番 1、2 をチェックする。
	Specific elements that should be checked when reviewing records: • 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.	**記録をレビューする際にチェックすべき具体的事項：** • 査察官は、手作業データのレビューに関する会社の手順をレビューし、プロセスの妥当性を判断すべきである。 • 二次チェックの必要性とその程度は、生成されたデータの重要度に応じたものとし、品質リスクマネジメントの原則に基づいて行われるべきである。 • 使用された計算の検証が、データの二次レビューに含まれていることをチェックする。 • (可能な場合) 原本データを見て、計算のために正しいデータが転記されていることを確認する。

8.9 Direct print-outs from electronic systems

8.9 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.	非常に単純な電子システム (例：天秤、pH メーター、データを保存しない単純な処理装置) は直接印刷される紙の記録を生成する。このようなタイプのシステム及び記録では、(再) 処理や電子的な日付・タイムスタンプの変更によりデータ表記に影響を与える機会は限られている。このような場合には、記録原本に、記録を作成した者の署名と日付を入れ、サンプル ID、バッチ番号等のトレーサビリティを確保するための情報を記録すべきである。これらの原本記録は、バッチ処理又はテストの記録に添付すべきである。

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性を持つことを確実にするための検討を行う必要がある (第 8.6.1 章参照) 。

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

8.10 文書保管 (記録保管と記録のアーカイブに関する要件の特定)

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.	各種の記録の保存期間は、 (最低でも) GMP/GDP の要件で規定された期間を満たすべきである。より長い保存期間を規定している可能性のある、他のローカル又は国の法律についても考慮すべきである。
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、社内で保管することもできるし、品質合意書に基づいて外部の保管サービスを利用することもできる。後者の場合、データセンターの所在地を特定しておく必要がある。リスクアセスメント〔結果〕を用意し、保管システム/施設/サービスが適切であり、残存リスクを理解していることを示せるようにしておく必要がある。

Item:	**Where and how should records be archived?**	**どこで、どのように記録を保管すべきか？**
1.	**Expectation** A system should be in place describing the different steps for archiving records (identification of archive boxes, list of records by box, retention period, archiving location, etc.). Instructions regarding the controls for storage, as well as access and recovery of records should be in place. Systems should ensure that all GMP/GDP relevant records are stored for periods that meet GMP/GDP requirements[9].	**期待事項** 記録をアーカイブするためのさまざまなステップ (アーカイブ用の箱の識別、箱ごとに含まれる記録のリスト、保存期間、アーカイブ場所等) を説明するシステムを設ける必要がある。 倉庫のコントロール、また記録のアクセス及びリカバリに関する指示が必要である。 システムは、GMP/GDP に関連するすべての記録が、GMP/GDP の要件を満たす期間、確実に保管されるようなものであること [9]。
	Specific elements that should be checked when	**記録をレビューする際にチェックすべき具体**

[9] Note that storage periods for some documents may be dictated by other local or national legislation.
[9] 文書によっては〔GMP/GDP 以外の〕他のローカルまたは国の法律によって保存期間が定められている場合がある。

	reviewing records: • 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.	**的事項**： • アーカイブされた記録を取り出すためのシステムが効果的であり、追跡可能であることをチェックする。 • 記録が整然と保管され、容易に識別できることをチェックする。 • 記録が定められた場所にあり、適切に保護されていることをチェックする。 • 保存された記録のインテグリティを確実にするために、アーカイブされた文書へのアクセスが許可された社員に制限されていることをチェックする。 • 記録へのアクセスや返却の記録が存在することをチェックする。 • 使用している保存方法は、必要なときに文書を効率的に取り出せるものであること。
2.	**Expectation** 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.	**期待事項** すべてのハードコピーの品質記録は、以下のようにアーカイブする： • 破損や消失を防ぐような安全な場所で、 • 容易に追跡でき、取り出せるような方法で、 • アーカイブ期間に渡って記録が継続して残ることを確実にするような方法で。
	Specific elements that should be checked when reviewing records: • 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.	**記録をレビューする際にチェックすべき具体的事項：** • アーカイブ業務が外部委託されている場合、品質合意書が締結され、かつ保存場所が監査されていることをチェックする。 • 全アーカイブ期間で文書の判読性/可用性が維持されることを確実にするために、何らかのアセスメントを行っていることを確認する。

	• Verify whether the storage methods used permit efficient retrieval of documents when required.	• プリントアウトが恒久的ではない (熱転写紙等) 場合は、検証された (「真正」) コピーを保管すべきである。 • 使用している保存方法が、必要なときに文書を効率的に取り出せるようになっていることを検証する。
3.	**Expectation** 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.	**期待事項** すべての記録は、以下の原因による損傷や破壊から保護する必要がある： • 火災 • 液体 (例：水、溶媒、緩衝液) • げっ歯類 • 湿度等 • 許可のない (記録の修正・破壊・置換を試みようとしている) 社員によるアクセス。
	Specific elements that should be checked when reviewing records: • 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.	**記録をレビューする際にチェックすべき具体的事項：** • 記録を保護するシステム (例：害虫コントロールやスプリンクラー) があることをチェックする。 • 注：スプリンクラーシステムは、ローカルの安全要件に従って実装すべきであるが、文書の損傷を防ぐ (例：文書を水から保護する) ように設計する必要がある。 • 記録に対する適切なアクセスコントロール〔が設けられていること〕をチェックする。

8.11 Disposal of original records or true copies

8.11 原本の記録又は真正コピーの処分

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	定められた保存期間の後に正しい原本記録又は真正コピーが確実に処分されるように、記録の廃棄に関する文書化されたプロセスを設けるべきである。このシステムは、誤って最

	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.)	新の記録が破棄されたり、過去の記録が誤って最新の記録の中に紛れ込んだりする (例：過去の記録が現在の記録と混同・混合される) ことを確実に防ぐものであること。
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.	ローカルポリシーに従って、退役した記録を適切かつタイムリーにアーカイブ、又は破棄したことを示すための記録/登録簿を用意しておく必要がある。
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.	誤った文書を削除してしまうリスクを低減するための対策を講じるべきである。記録を廃棄できるアクセス権をコントロールし、少人数に限定すべきである。

9. SPECIFIC DATA INTEGRITY CONSIDERATIONS FOR COMPUTERISED SYSTEMS

9．コンピュータ化システムにおけるデータインテグリティに関する具体的な検討事項

9.1 Structure of the Pharmaceutical Quality System and control of computerised systems

9.1 医薬品品質システムの構造とコンピュータ化システムのコントロール

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.	会社では、様々なコンピュータ化システムが使用され、非常に多くの業務活動を支援している。これらは、単純なスタンドアロンシステムから大規模な統合された複雑なシステムまで多岐にわたり、その多くが製造される製品の品質に影響する。すべてのコンピュータ化システムを十分に評価及びコントロールを行い、GMP[10] 及び GDP[11] の要件に従って管理することは、各規制対象会社の責任である。
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	各組織において、利用しているコンピュータ化システムの性質と範囲を十分に認識し、アセスメントを実施しておく必要がある。アセスメント〔記録〕には、各システムの、利用目的と機能、不正操作に対するデータインテグリティのリスクや脆弱性を記載する。特に、コンピュータ化システム及び関連データの、製品品質に対する重要度を判断すること

[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

	respect of product quality.	に重点を置く。
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.	製品品質に影響する可能性のあるすべてのコンピュータ化システムは、(システムを、偶発的又は意図的な不正操作、変更、又は他のデータ品質とデータインテグリティに影響し得る活動から確実に保護するよう設計された) 医薬品品質システムの下で効果的に管理すべきである。
9.1.4	The processes for the design, evaluation, and selection of computerised systems should include appropriate consideration of the data management and integrity aspects of the system. Regulated users should ensure that vendors of systems have an adequate understanding of GMP/GDP and data integrity requirements, and that new systems include appropriate controls to ensure effective data management. Legacy systems are expected to meet the same basic requirements; however, full compliance may necessitate the use of additional controls, e.g. supporting administrative procedures or supplementary security hardware/software.	コンピュータ化システムの設計・評価・選定のプロセスでは、システムのデータマネジメントと データインテグリティの側面を適切に検討すべきである。規制対象ユーザーは、システムベンダーが GMP/GDP 及びデータインテグリティの要件を十分に理解し、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適切なコントロールが組み込まれることを確実にすべきである。レガシーシステムも同様の基本要件を満たすことが期待されているが、完全に適合するためには追加的なコントロール (例：補助的な業務管理手順やセキュリティを強化するハードウェア/ソフトウェア) を使用する必要があるであろう。
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:	規制対象ユーザーは、コンピュータ化システムによって生成されるデータの範囲と性質を十分に理解する必要がある。また、リスクベースアプローチを採用し、データリスクとデータ重要度 (メタデータを含む) 、及び生成されたデータを管理するために必要なコントロールを決定する。
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.	生データを取り扱う上で、通常は、製造のイベントや分析を再現するために、生データを完全〔不足なく〕に取得・保管する必要がある。
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	メタデータを取り扱う上で、メタデータの中にはイベントを再現する上で重要なもの (例：ユーザーの識別、時間、重要なプロセスパラメータ、測定単位) があり、それらは完全に取得・管理すべき「関連メタデータ」とみなされる。しかし、重要でないメタデータ (例：システムのエラーログや重要でない

	management where justified using risk management.	システムチェック) は、リスクマネジメントにより合理性を説明できるならば、完全な取得・管理は不要かもしれない。
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.	データの脆弱性及びリスクを判断する際には、コンピュータ化システムをビジネスプロセスの中で使用するという観点から検討することが重要である。例えば、統合されたコンピュータインターフェイスを利用する分析メソドから生成された〔分析〕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重量の入力、データを生成するためのシステムの利用、そのデータを用いた最終結果の処理・記録〔のやり方〕に影響される。データフローマップを作成し、アセスメントを行うことにより、コンピュータ化システム、特にインターフェイスされたシステム【訳注】のリスクと脆弱性を理解することができるであろう。 【訳注：interfaced は、integrated (統合) との対比で、統合されず、単に組み合わされたという意味で用いられていると思われる。】
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.	システム及び (又は) ソフトウェアにもともと組み込まれているデータインテグリティコントロールを検討すべきである。これは現在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システムというよりも、特に不正に対して脆弱なシステムについて、より必要である。脆弱性のあるシステムの例は、手作業による記録システム、旧式のセキュリティ対策が施され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、追加的なネットワークセキュリティ保護 (例：ファイアウォールや侵入検出・防止システムの利用) を必要とするシステム等である。
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.	コンピュータ化システムの査察では、査察官はアセスメントの際に、会社の専門技術を活用するとよい。会社の対応者に、アクセスやナビゲーションを手伝ってもらうよう依頼・指示することでシステムの査察の助けになる。

9.1.9	The guidance herein is intended to provide specific considerations for data integrity in the context of computerised systems. Further guidance regarding good practices for computerised systems may be found in the PIC/S Good Practices for Computerised Systems in Regulated “GxP” Environments (PI 011)	本書におけるガイダンスは、コンピュータ化システムにおけるデータインテグリティの具体的な検討事項を提供することを目的としている。コンピュータ化システムのグッドプラクティスに関する更なるガイダンスは、PIC/S Good Practices for Computerised Systems in Regulated "GxP" Environments (PI 011) 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.	本書で述べる原則は、コンピュータ化システムの提供を外部委託する場合にも同様に適用される。このような場合、外部委託されたサービスが GMP/GDP の要件に従って管理され、アセスメントされていること、並びに適切なデータマネジメント及びデータインテグリティのコントロールが〔規制対象会社と外部委託先の〕双方で理解され、効果的に実施されることを確実にする責任は規制対象会社にある。

9.2 Qualification and validation of computerised systems

9.2 コンピュータ化システムの適格性評価とバリデーション

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.	コンピュータ化システムの適格性評価及びバリデーションは、関連する GMP/GDP ガイドラインに従って実施されるべきである。下表は、コンピュータ化システムのグッドデータガバナンスプラクティスを確実にするための特別な期待事項を明らかにするものである。
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、生成された記録が適切に保護されていることを保証できるとは限らない。バリデートされたシステムは、偶発的又は悪意のある手段による消失や改ざんに対して脆弱な場合がある。したがって、バリデーションに加えて、適切な業務管理的コントロール、物理的コントロール、及びユーザートレーニングが必要である。

9.3 Validation and Maintenance

9.3 バリデーションとメンテナンス

Item:	System Validation & Maintenance	システムバリデーションとメンテナンス
1.	**Expectation** 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. 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. 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.	**期待事項** 規制対象会社は、システム調達の初期段階、及びシステムとデータのライフサイクル全体を 通して、データマネジメント及びデータインテグリティの要件が考慮されることを確実にするために、適切なコントロールを文書化し、実施すべきである。規制対象ユーザーは、機能仕様書 (FS) 及び (又は) ユーザー要求仕様書 (URS) に、 データマネジメント及びデータインテグリティの要件を適切に盛り込むべきである。 GMP/GDP に不可欠な機器の購入に際しては、特に注意して、システムのデータインテグリティコントロールを、購入前に適切に評価することを確実にすべきである。 レガシーシステム (使用中の既存システム) を評価し、既存システムの構成設定と機能により、データをグッドデータマネジメントプラクティスとグッドデータインテグリティプラクティスに従って適切にコントロールできるか判断する必要がある。システムの機能や設計により適切なレベルのコントロールが得られない場合は、追加的なコントロールを検討し、実施する必要がある。
	Potential risk of not meeting expectations/items to be checked • 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,	**期待事項を満たさない場合の潜在的なリスク/チェックすべき項目** • DI〔データインテグリティ〕要件の検討が不十分だと、データマネジメント及びデータインテグリティの期待に応える基本機能を備えていないソフトウェアシステムを購入することになりかねない。 • 査察官は、新システムの導入が、データインテグリティの原則を十分に考慮したプロセスに沿って行われていることを検証すべきである。 • レガシーシステムの中には、データマネ

	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: - 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; - Configuring operating system file/folder permissions to prevent modification/deletion of files when the modification/deletion of data files cannot be controlled by system software; or - Implementation of hybrid or manual systems to provide control of data generated.	ジメントのための適切なコントロールが備わっておらず、データの不正操作が可能で、かつそのことを検出しにくいものがある。 • 既存システムのアセスメント〔記録〕が用意されるべきである。アセスメント〔記録〕には、あらゆる脆弱性の概要が示され、データインテグリティを確保するために実施された追加的なコントロールが列挙される。追加的なコントロールは適切にバリデートすべきであり、以下が含まれる： - システムソフトウェアがユーザー権限をコントロールするためのシステム管理のコントロールを備えていない場合、オペレーティングシステム(OS) の機能 (例：Windows Active Directory のグループ) を使用して、ユーザーとそのアクセス権限を割り当てる。 - システムソフトウェアがデータファイルの変更・削除をコントロールできない場合、OS のファイル/フォルダーのパーミッションを設定してファイルの修正・削除を防ぐ。 - 生成されたデータをコントロールするためにハイブリッドシステム又は手作業システムを導入する。
2.	**Expectation** 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. Risk assessments should be in place for each	**期待事項** 規制対象ユーザーは、使用中のすべてのコンピュータ化システムの台帳を持つべきである。この台帳には以下が含まれる： • 各コンピュータ化システムの名称、場所、主な機能。 • システム及び関連データの機能、及び重要度のアセスメント〔結果〕 (例：GMP/GDP への直接的影響、間接的影響、影響なし)。 • 各システムの現在のバリデーション状況と、既存のバリデーション文書への参

	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. Consideration should also be given to those systems with higher potential for disaster, malfunction or situations in which the system becomes inoperative. Assessments should also review the vulnerability of the system to inadvertent or unauthorised changes to critical configuration settings or manipulation of data. All controls should be documented and their effectiveness verified.	照。 各システムについてのリスクアセスメント(特に、データインテグリティを確実にするために必要となるコントロールのアセスメント)〔の記録〕を用意すべきである。データインテグリティのコントロールに対するバリデーションのレベル及び範囲は、システムやプロセスの重要度及び製品品質に対する潜在的なリスクに基づいて決定すべきである。例えば、一般的に、バッチリリースデータを生成又はコントロールするプロセスやシステムは、重要度の低いデータやプロセスを管理するシステムよりも大きなコントロールが必要であろう。 被災や故障等システムが運転できない状況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。 アセスメントでは、重要な構成設定に対する不注意による又は許可のない変更、又はデータへの不正操作に対するシステムの脆弱性についてもレビューする必要がある。すべてのコントロールを文書化し、その有効性を検証すべきである。
	Potential risk of not meeting expectations/items to be checked • Companies that do not have adequate visibility of all computerised systems in place may overlook the criticality of systems and may thus create vulnerabilities within the data lifecycle. • An inventory list serves to clearly communicate all systems in place and their criticality, ensuring that any changes or modifications to these systems are controlled. • Verify that risk assessments are in place for critical processing equipment and data acquisition systems. A lack of thorough assessment of system impact may lead to a lack of appropriate validation and system control. Examples of critical systems to review include: - systems used to control the purchasing and	**期待事項を満たさない場合の潜在的なリスク/チェックすべき項目** • すべてのコンピュータ化システムを適切に可視化できていない会社は、システムの重要度を見落とし、データライフサイクルの中で脆弱性を作り込む可能性がある。 • 台帳は、存在するすべてのシステムとその重要度を明確に伝え、システムへの変更や修正を確実にコントロールするのに役立つ。 • 重要な製造機器及びデータ収集システムについて、リスクアセスメントが実施されていることを検証する。システムの影響についての徹底的なアセスメントが行われないと、バリデーションやシステムコントロールが適切に行われない可能性がある。確認すべき重要なシステムの例

	status of products and materials; - systems for the control and data acquisition for critical manufacturing processes; - systems that generate, store or process data that is used to determine batch quality; - systems that generate data that is included in the batch processing or packaging records; and - systems used in the decision process for the release of products.	を以下に示す。 - 製品や原料の購入や状態のコントロールに用いられるシステム。 - 重要な製造プロセスのコントロールとデータ収集のためのシステム。 - バッチ品質の決定に使用されるデータを生成・保存・処理するシステム。 - バッチ処理やパッケージングの記録に含まれるデータを生成するシステム。 - 製品リリースの決定プロセスに用いられるシステム。
3.	**Expectation** 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. • Frequency of review of audit trails and system logs. • Procedures for: - creating new system user; - modifying or changing privileges for an existing user; - defining the combination or format of passwords for each system - reviewing and deleting users; - back-up processes and frequency; - disaster recovery; - data archiving (processes and responsibilities), including procedures for	**期待事項** 新しいシステムについては、各コンピュータ化システムのバリデーションサマリ報告書 (Annex 15 の要件に従って作成され、承認されたもの) を用意する必要があり、少なくとも以下の項目を記載 (又は参照)) する： • 重要なシステム構成設定の詳細。また構成設定へのアクセス及びあらゆる変更を制限するためのコントロール (変更管理) 。 • 現時点で承認されているすべての一般ユーザー及びシステム管理者のリストで、ユーザー名とユーザーの役割を示すもの。 • 監査証跡及びシステムログをレビューする頻度。 • 以下に関する手順： - 新規システムユーザーの作成。 - 既存ユーザーの権限の修正又は変更。 - 各システムのパスワードの組み合わせ又はフォーマット。 - ユーザーのレビュー及び削除。 - バックアッププロセス及び頻度。

	accessing and reading archived data; - 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. 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.	- 災害復旧。 - データアーカイブ (のプロセスと責任) 。アーカイブデータへのアクセスと読み出しの手順を含む。 - データ保存場所の承認。 • 報告書では、どのように原本データと関連メタデータが、製造プロセスや分析活動の再現を可能にするような形式で、保管されるのかを説明する必要がある。 既存システムについては、上記の要件を明記した文書を用意する必要があるが、バリデーションサマリ報告書としてまとめる必要はない。規制対象ユーザーは、これらの文書を、必要に応じて維持・更新する必要がある。
	Potential risk of not meeting expectations/items to be checked • 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	**期待事項を満たさない場合の潜在的なリスク/チェックすべき項目** • バリデーションシステムと報告書で、特に、GMP/GDP の要件に従って、ALCOA の原則を考慮したデータインテグリティの要件が記載されていることをチェックする。 • システム構成設定及び職務の分離 (例：データを生成する権限とデータを検証する権限を分ける) は、バリデーション前に定義し、テスト時に有効性を検証すべきである。 • システムアクセス手順をチェックする。システムへの修正や変更が制限され、変更管理の対象となっているか。 • システム管理者のアクセス権が、承認された者に制限され、日常業務に使用されていないことを確認する。 • コンピュータ化システムへのアクセスを許可・変更・削除するための手順をチェックし、これらの活動がコントロールされていることを確認する。ユーザーのアクセスログと権限レベルが最新であることをチェックする。システムに許可されていないユーザーが〔ログ上に〕おら

	users from amending audit trail functions and from changing any pre-defined directory paths where data files are to be stored.	ず、またアクセスアカウントが最新の状態に保たれていること。 • ユーザーが監査証跡機能を変更したり、データファイルが格納される既定のディレクトリパスを変更したりすることの制限も必要である。

4.	**Expectation** Companies should have a Validation Master Plan in place that includes specific policies and validation requirements for computerised systems and the integrity of such systems and associated data. The extent of validation for computerised systems should be determined based on risk. Further guidance regarding assessing validation requirements for computerised systems may be found in PI 011. Before a system is put into routine use, it should be challenged with defined tests for conformance with the acceptance criteria. It would be expected that a prospective validation for computerised systems is conducted. Appropriate validation data should be available for systems already in-use. Computerised system validation should be designed according to GMP Annex 15 with URS, DQ, FAT, SAT, IQ, OQ and PQ tests as necessary. 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. Companies should ensure that computerised systems are qualified for their intended use. Companies should therefore not place sole reliance on vendor qualification packages; validation exercises should include specific tests to ensure data integrity is maintained during operations that reflect normal and intended use. The number of tests should be guided by a risk assessment but the critical 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,	**期待事項** 会社は、バリデーションマスター計画書を用意する必要がある。そこには、コンピュータ化システム及び関連データのインテグリティに関する具体的なポリシーとバリデーション要件が記載される。 コンピュータ化システムバリデーションの範囲は、リスクに基づいて決定すべきである。コンピュータ化システムバリデーションの要件をアセスメントするための詳細なガイダンスは、PI 011 に記載されている。 システムを日常的に使用する前に、定義されたテストにより、受入基準への適合を確認する必要がある。 予測的コンピュータ化システムバリデーションを行うことが期待されている。既に使用中のシステムについて、適切なバリデーションデータを用意しておく必要がある。 コンピュータ化システムバリデーションは GMP Annex 15 に従って設計【訳注】すべきであり。必要に応じて URS、DQ、FAT、SAT、IQ、OQ、PQ テストが含まれる。 【訳注：システムの設計ではなく、バリデーションのやり方の設計を指す。】 適格性評価のテスト方法は、バリデーション対象となるシステムに合わせる必要があり、規制対象ユーザーがその合理性を判断すべきである。適格性評価には、設計適格性評価 (DQ) 、据付時適格性評価 (IQ) 、運転時適格性評価 (OQ) 、性能適格性評価 (PQ) が含まれる。特に、データ品質又はデータインテグリティにリスクがある部分を確かめるようにテストを設計する必要がある。 会社は、コンピュータ化システムが意図された用途に対して適格性評価が行われることを確実にすべきであり、ベンダーの適格性評価パッケージのみに依存すべきではない。バリデーションを実施する際には、通常の、意図された用途が反映された業務において、データインテグリティが維持されることを確かめるテストも行うべきである。

	OQ & PQ stages.	テストの数はリスクアセスメントに従うべきであるが、少なくとも重要な機能を特定し、テストすべきである。例えば、基本アルゴリズムやロジックセットに基づく PLC やシステムでは、機能テストによりコンピュータ化システムの信頼性を十分に保証できるであろう。重要なシステム及び (又は) より複雑なシステムについては、IQ、OQ、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 • 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.	**期待事項を満たさない場合の潜在的なリスク/チェックすべき項目** • バリデーション文書にデータインテグリティに関する具体的な取り決めが含まれていることをチェックする。バリデーションサマリ報告書は、特にデータインテグリティの原則に触れるべきであり、また設計とテストにより適切なコントロールがあることを示すべきである。 • バリデートされていないシステムでは、〔不適切な〕ユーザーアクセスやシステム構成設定によりデータを修正できてしまい、データの完全性に関して重大な脆弱性が生じる可能性がある。 • エンドユーザーテストには、ソフトウェアがベンダーの要件を満たすだけでなく、意図した用途に適していることを示すよう設計されたテストスクリプトが含まれていることをチェックする。
5.	**Expectation** <u>Periodic System Evaluation</u> Computerised systems should be evaluated periodically in order to ensure continued compliance with respect to data integrity controls. The evaluation should include deviations, changes (including any cumulative effect of changes), upgrade history, performance and maintenance, and assess whether these changes have had any detrimental effect on data management and integrity controls. The frequency of the re-evaluation should be based on a risk assessment depending on the criticality of the computerised systems	**期待事項** <u>定期的なシステム評価</u> コンピュータ化システムを定期的に評価し、データインテグリティコントロールへの継続的な適合を確実にすべきである。評価内容には、逸脱、変更 (変更による累積的影響を含む) 、アップグレード履歴、性能、保守を含む。また、評価では、これらの変更による、データマネジメント及びデータインテグリティのコントロールへの悪影響がないかアセスメントする。 再評価の頻度は、リスクアセスメントに基づ

	considering the cumulative effect of changes to the system since last review. The assessment performed should be documented.	き、コンピュータ化システムの重要度に応じたものとし、前回レビュー以降に行われたシステム変更の累積的な影響を考慮する。実施した評価は文書化すべきである。
	Potential risk of not meeting expectations/items to be checked • 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.	**期待事項を満たさない場合の潜在的なリスク/チェックすべき項目** • コンピュータ化システムの再バリデーションレビュー〔の予定〕がバリデーションスケジュールに記載されていることをチェックする。 • システムが定期的レビュー (特にデータインテグリティに関する潜在的な脆弱性について) の対象となっていることを検証する。 • 現在のソフトウェア/ハードウェアの限界等の問題が発見されたときは、タイムリーに対処する必要がある。発見されたリスクを管理するために、是正・予防措置及び暫定的コントロールを用意し、実施すべきである。
6.	**Expectation** 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. 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. 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	**期待事項** OS 及びネットワークコンポーネント (ハードウェアを含む) は、ベンダーの推奨に従ってタイムリーに更新すべきである。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、プラットフォームがサポートされなくなってしまう前に計画し、実施する必要がある。そうしないと、システムで生成されたデータのデータマネジメント及びデータインテグリティに影響が出るかもしれない。 データのセキュリティを維持するために、OS やネットワークコンポーネントのセキュリティパッチを、ベンダーの推奨に従って、管理された方法でタイムリーに適用すべきである。セキュリティパッチの適用は、変更管理の原則に従う。 サポートの終わった OS を維持している場合 (すなわち古い OS をベンダーサポート終了後も使用している場合、又はサポートされてい

	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. Remote access to unsupported systems should be carefully evaluated due to inherent vulnerability risks.	るバージョンであってもセキュリティパッチが適用されていない場合) 、そのシステム (サーバー) は、ネットワークの他の部分から可能な限り隔離すべきである。他の機器とのインターフェイスやデータ転送は、慎重に設計・設定・適格性評価し、サポートされていない OS に起因する脆弱性を利用した悪用を防止すべきである。 サポートの終わったシステムは、もともと脆弱性リスクがあるため、リモートアクセスを行う場合は慎重に評価すべきである。
	Potential risk of not meeting expectations/items to be checked • 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.	**期待事項を満たさない場合の潜在的なリスク/チェックすべき項目** • システム更新が、コントロールされた方法でタイムリーに行われていることを検証する。古いシステムについては、批判的にレビューされ、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、又は (コントロールを統合できない場合) 適切な業務管理的コントロールが実施され、有効であるかどうかを判断する。

9.4 Data Transfer

9.4 データ転送

Item:	Data transfer and migration	データ転送とデータ移行
1.	**Expectation** Interfaces should be assessed and addressed during validation to ensure the correct and complete transfer of data. Interfaces should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimise data integrity risks. Verification methods may include the use of: • Secure transfer • Encryption • Checksums Where applicable, interfaces between systems	**期待事項** バリデーション時にインターフェイスをアセスメントし、対応することで、データが正確かつ完全に転送されるようにすべきである。 インターフェイスには、データを正しく安全に入力・処理する適切なチェック機能を組み込み、データインテグリティに関するリスクを最小にすべきである。チェック方法として以下を利用することが考えられる： • 安全な転送 • 暗号化

	should be designed and qualified to include an automated transfer of GMP/GDP data.	• チェックサム 該当する場合、システム間のインターフェイスは、GMP/GDP データの自動転送を含むように設計し、適格性評価すべきである。
	Potential risk of not meeting expectations/items to be checked • 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.	**期待事項を満たさない場合の潜在的なリスク/チェックすべき項目** • コンピュータ化システム間のインターフェイスでは、転送プロセス中にデータが誤って失われたり、変更されたり、誤って転記されたりするリスクがある。 • データが安全な場所/データベースに直接転送されていることを確認する。 (改ざんの可能性のある) ローカルドライブからの単純なコピーではないことを確認する。 • データを、最終的に保存したりデータ処理したりする場所に転送する前に、一時的にでもローカルのコンピュータ化システム (例：装置コンピュータ) に保存すると、データが削除又は不正操作される可能性がある。これは、(ネットワークに接続されていない)「スタンドアロン型」 システムの場合には特にリスクが高い。データが最初に保存される環境に、適切な DI〔データインテグリティ〕コントロールが設けられていることを確認する。 • 適切に設計され、適格性評価された自動データ転送は、人が手作業で行うデータ転送よりもはるかに信頼性が高い。
2.	**Expectation** 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. 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	**期待事項** システムソフトウェア (OS を含む) をインストール又は更新したときは、ユーザーは、既存のデータ及びアーカイブデータが、新しいソフトウェアでも読めることを確実にすべきである。必要に応じて、既存のアーカイブデータを新しいフォーマットに変換する必要がある。 新しいソフトウェアを新しいデータフォーマ

	available as a backup media in order to have the opportunity to read the archived data in case of an investigation.	ットに変換できない場合は、調査を行う際にアーカイブデータを読み取れるように、古いソフトウェアを維持する (例：1 台のコンピュータ又は他の技術的ソリューションにインストールする) とともに、バックアップメディアでも利用可能にしておくべきである。
	Potential risk of not meeting expectations/items to be checked • 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.	**期待事項を満たさない場合の潜在的なリスク/チェックすべき項目** • データライフサイクルを通して、データが原本の〔最初に記録されたときの〕形式で読むことができることが大事であり、したがって、ユーザーはデータの見読性を維持する必要がある。そのためには過去のソフトウェアへのアクセスを維持する必要があるかもしれない。 • あるシステムから別のシステムへのデータ移行は、コントロールされた方法で、文書化されたプロトコルに従って実行すべきであり、データの完全な移行も適切に検証すべきである。
3.	**Expectation** 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. 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. 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	**期待事項** レガシーシステムのソフトウェアがサポートされなくなった場合、(保管に関する要件に従って、可能な限り長い期間にわたって) そのソフトウェアを維持することを考慮し、データにアクセスし続けられるようにする必要がある。これは、ソフトウェアを仮想環境で維持することで実現できるかもしれない。 レガシーデータが古くなるにつれ、代替のファイル形式への移行が必要になる。そのファイル形式は、データの「真正コピー」の属性をなるべく多く持つものとする。 原本データの機能を完全に保ったまま移行することが技術的に不可能な場合は、将来にわたってのデータのリスク及び重要性に基づいて選択肢をアセスメントすべきである。移行のファイル形式は、長期的にアクセスできる〔メリット〕と動的なデータ機能 (例：データ照会、トレンド、再処理等) が損なわれる〔デメリット〕のリスクバランスを考慮して選択すべきである。リスクアセスメントで

	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.	は、重要な構成設定への不注意による又は許可のない変更、又はデータの不正操作に対する脆弱性をレビューすべきである。リスクを低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べきである。継続してアクセスできるようにするために、一部の属性及び(又は)動的データ機能を欠いたファイル形式への移行もやむを得ないことは了解されている。
	Potential risk of not meeting expectations/items to be checked • 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.	**期待事項を満たさない場合の潜在的なリスク/チェックすべき項目** • ソフトウェアを仮想環境で維持する場合、ソフトウェアをコントロールするための適切な方策 (例えば、バリデーションの状態、許可された者によるアクセスコントロール等) が実施されているかどうかをチェックする。すべてのコントロールを文書化し、その有効性を検証すべきである。

9.5 System security for computerised systems

9.5 コンピュータ化システムのシステムセキュリティ

Item:	**System security**	**システムセキュリティ**
1.	**Expectation** User access controls shall be configured and enforced to prohibit unauthorised access to, changes to and deletion of data. The extent of security controls is dependent on the criticality of the computerised system. For example: • Individual Login IDs and passwords should be set up and assigned for all staff needing to access and utilise the specific electronic system. Shared login credentials do not allow for traceability to the individual who performed the activity. For this reason, shared passwords, even for reasons of financial savings, 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.	**期待事項** 許可のないデータへのアクセス・変更・削除を禁止するために、ユーザーアクセスのコントロールを構成設定し、実施する。セキュリティコントロールの程度は、コンピュータ化システムの重要度に依存する。例えば： • 電子システムにアクセスし、利用する必要のあるすべてのスタッフに、個人別のログイン ID とパスワードを設定して割り当てる。ログイン認証情報を共有すると、活動を行った個人を追跡することができなくなるため、パスワードの共有は、たとえ経済的な節約のためであっても、禁止すべきである。電子システムのバリデーションにより、ログインパラメータを検証し、ログインプロファイル、構成設定及びパスワード形式が明確に定義され、意図された通りに機能すること

	• 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. • Appropriate controls should be in place regarding the format and use of passwords, to ensure that systems are effectively secured. • Upon initially having been granted system access, a system should allow the user to create a new password, following the normal password rules. • Systems should support different user access roles (levels) and assignment of a role should follow the least-privilege rule, i.e. assigning the minimum necessary access level for any job function. As a minimum, simple systems should have normal and admin users, but complex systems will typically requires more levels of users (e.g. a hierarchy) to effectively support access control. • 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). • Normal users should not have access to critical aspects of the computerised system, e.g. system clocks, file deletion functions, etc. • Systems should be able to generate a list of users with actual access to the system, including user 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. • Systems should be able to generate a list of successful and unsuccessful login attempts, including: - User identification	を確実にすべきで ある。 • データ入力及びコンピュータ上の記録の変更は、許可された社員に限定する。会社は、使用中の電子システムごとに、権限を持つ個人のリストとそのアクセス権限を管理すべきである。 • システムが効果的に安全に保たれることを確実にするために、パスワード形式と使用について適切なコントロールを設けるべきである。 • システムは、ユーザーが最初にシステムへのアクセスを許可されたとき、通常のパスワード規則に従って、新しいパスワードを作成できるようにすべきである。 • システムは、異なるユーザーアクセスの役割 (レベル) をサポートし、役割は、最小特権ルールに従って割り当てるべきである。単純なシステムでは、最低でも一般ユーザーとシステム管理者に分けるべきであるが、複雑なシステムでは、アクセスコントロールを効果的にサポートするために、より多くのユーザーレベル (例：階層) が必要となることが多い。 • GMP/GDP に不可欠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システムやインフラに対するシステム管理者アクセス権限の付与は、厳格にコントロールすべきである。システム管理者アクセス権限は、システムの一般ユーザーに与えるべきではない (すなわち、職務の分離) 。 • 一般ユーザーには、コンピュータ化システムの重要な部分 (例：システムクロック、ファイル削除機能等) へのアクセス権を持たせるべきではない。 • システムは、実際にシステムにアクセスできるユーザーのリストを、ユーザーの識別情報と役割を含めて、生成できるべきである。ユーザーリストには、特定の個人の識別を可能にする名前又はユニークな識別子を含むものとする。定期的なユーザーレビューの際には、このリスト

	- User access role - Date and time of the attempted login, either in local time or traceable to local time - Session length, in the case of successful logins • User access controls should ensure strict segregation of duties (i.e. that all users on a system who are conducting normal work tasks should have only normal access rights). Normally, users with elevated access rights (e.g. admin) should not conduct normal work tasks on the system. • System administrators should normally be independent from users performing the task, and have no involvement or interest in the outcome of the data generated or available in the electronic system. For example, QC supervisors and managers should not be assigned as the system administrators for electronic systems in their laboratories (e.g. HPLC, GC, UV-Vis). Typically, individuals outside of the quality and production organisations (e.g. Information Technology administrators) should serve as the system administrators and have enhanced permission levels. • For smaller organisations, it may be permissible for a nominated person in the quality unit or production department to hold access as the system administrator; however, in these cases the administrator access should not be used for performing routine operations and the user should hold a second and restricted access for performing routine operations. In these cases all administrator activities conducted should be recorded and approved within the quality system. • Any request for new users, new privileges of users should be authorised by appropriate personnel (e.g. line manager and system owner) and forwarded to the system administrator in a traceable way in accordance with a standard procedure. • Computerised systems giving access to GMP/GDP critical data or operations should have an inactivity logout, which, either at	を使用すべきである。 • システムは、成功・失敗したログイン試行のリストを生成できるべきである。リストには以下が含まれる： - ユーザー識別子 - ユーザーアクセス役割 - (ローカル時刻による、又はローカル時刻を特定できる) ログインの試みがあった日時。 - ログインに成功した場合、セッションの長さ。 • ユーザーのアクセスコントロールにより、厳密な職務分離を確実にすべきである (すなわち、システム上で通常の作業タスクを行っているすべてのユーザーは、一般アクセス権限のみを持つことを確実にする) 。一般的に、より強いアクセス権限を持つユーザー (例：システム管理者) は、システム上で通常の作業タスクを行うべきではない。 • システム管理者は通常、タスクを実行するユーザーから独立し、電子システムで生成される利用可能なデータのもたらす結果に関与・関心を持たない者であること。例えば、QC スーパーバイザー及び QC マネージャーを、管轄するラボの電子システム (HPLC、 GC、UV-Vis 等) のシステム管理者に任命すべきではない。一般的には、品質及び製造組織の外部の個人 (例：情報技術管理者) をシステム管理者とし、強い権限レベルを持たせる。 • 小規模な組織では、品質部門又は製造部門の中で指名された者がシステム管理者アクセス権限を持つことは許される場合がある。このような場合、システム管理者としてのアクセス権限は通常業務の実行に使用すべきではなく、通常業務を行うときのために第二の、制限されたアクセス権限を持つようにすべきである。このような場合、システム管理者として実

	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.	施したすべての活動は、品質システムの枠組みで記録し、承認すべきである。 • 新ユーザーの追加やユーザーの新たな権限の要求は、適切な社員 (例：ラインマネージャーやシステムオーナー) が、標準的な手順に従って、追跡可能な方法で、承認し、システム管理者に回送すべきである。 • GMP/GDP に重要なデータや操作へのアクセスを提供するコンピュータ化システムでは、アプリケーションレベル又は OS レベルで、無操作による自動ログアウトを設けるべきである。これは、活動していない時間が事前に定められた時間を超えたときにユーザーをログアウトするものである。この時間は長めよりは、短めに設定すべきである。これは一般的にシステムへの許可のないアクセスを防ぐ目的で設定する。無操作による自動ログアウト発動時、システムはユーザーに通常の認証手続きを経て再度ログインすることを求めるべきである。
	Potential risk of not meeting expectations/items to be checked • Check that the company has taken all reasonable steps to ensure that the computerised system in use is secured, and protected from deliberate or inadvertent changes. • Systems that are not physically and administratively secured are vulnerable to data integrity issues. Inspectorates should confirm that verified procedures exist that manage system security, ensuring that computerised systems are maintained in their validated state and protected from manipulation. • 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. • It is acknowledged that some legacy computerised systems support only a single user login or limited numbers of user logins.	**期待事項を満たさない場合の潜在的なリスク/チェックすべき項目** • 会社が、使用中のコンピュータ化システムのセキュリティを確保し、意図的又は不注意による変更から保護するために、あらゆる合理的な手段を講じていることをチェックする。 • 物理的及び業務管理的なセキュリティが確保されていないシステムは、データインテグリティの問題が生じる可能性がある。査察官は、システムのセキュリティを管理するための、検証済みの手順が設けられていることを確認する。その手順は、コンピュータ化システムのバリデートされた状態の維持、及び不正操作からの保護を確実にするものであること。 • 個人別のユーザーログイン ID が使用されていることをチェックする。システム構成設定で個人別ユーザーログイン ID が使用できるのであれば、それを使用す

	Where no suitable alternative computerised system is available, equivalent control may be provided by third party software, or a paper based method of providing traceability (with version control). The suitability of alternative systems should be justified and documented. Increased data review is likely to be required for hybrid systems. • Inspectors should verify that a password policy is in place to ensure that systems enforce good password rules and require strong passwords. Consideration should be made to using stronger passwords for systems generating or processing critical data. • Systems where a new password cannot be changed by the user, but can only be created by the admin, are incompatible with data integrity, as the confidentiality of passwords cannot be maintained. • Check that user access levels are appropriately defined, documented and controlled. The use of a single user access level on a system and assigning all users this role, which per definition will be the admin role, is not acceptable. • Verify that the system uses authority checks to ensure that only 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.	べきである。 • レガシーコンピュータ化システムの中には、1 人のユーザーしかログインできないものや、限られた数のユーザーしかログインできないものがあることは了解されている。適切な代替コンピュータ化システムがない場合は、同等のコントロールを、サードパーティのソフトウェア、又はトレーサビリティ (とバージョン管理) を提供する紙ベースの方法により実現できるかもしれない。代替システムの適切さについて、その合理性を検討し、文書化する必要がある。ハイブリッドシステムの場合は、データレビューの強化が必要となるであろう。 • 査察官は、システムがグッドパスワードルールを実行し、強力なパスワードを要求することを確実にするために、パスワードポリシーが設けられていることを検証すべきである。重要なデータを生成・処理するシステムには、より強力なパスワードの使用を検討すべきである。 • 新しいパスワードをシステム管理者権限でしか作成できず、ユーザーが変更できないようなシステムは、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の考え方に反している。 • ユーザーのアクセスレベルが適切に定義され、文書化され、管理されていることをチェックする。システム上で一つのユーザーアクセスレベルのみ使用し、すべてのユーザーをこの役割 (定義上はシステム管理者の役割となる) に割り当てることは認められない。 • システムが権限チェックを使用していることを検証する。権限チェックは、システムの使用、記録への電子署名、操作〔画面〕へのアクセス、コンピュータ化システムの入力又は出力デバイスへのアクセス、記録の変更、操作の実行、が許可された個人のみに限定されることを確実にするものである。

2.	**Expectation** 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: • The physical security of computerised system hardware: - Location of and access to servers; - Restricting access to PLC modules, e.g. by locking access panels. - 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. • Vulnerability of networked systems from local and external attack; • Remote network updates, e.g. automated updating of networked systems by the vendor. • Security of system settings, configurations and key data. Access to critical data/operating parameters of systems should be appropriately restricted and any changes to settings/configuration controlled through change management processes by authorised personnel. • The operating system clock should be synchronized with the clock of connected systems and access to all clocks restricted to authorised personnel. • Appropriate network security measures should be applied, including intrusion prevention and detection systems. • 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. Regulated users should conduct periodic reviews of the continued appropriateness and effectiveness	**期待事項** コンピュータ化システムは、偶発的な変更や意図的な不正操作から保護すべきである。会社は、バリデートされた設定に対する許可のない変更 (これにより最終的にデータインテグリティが影響を受ける可能性がある) を防止するために、システムとその設計をアセスメントすべきである。以下を考慮する： • コンピュータ化システムのハードウェアの物理的セキュリティ。 - サーバーの場所とサーバーへのアクセス。 - (アクセスパネルのロック等による) PLC モジュールへのアクセスの制限。 - コンピュータ、サーバー及びメディアへの物理的なアクセスは、許可された個人に限定すべきである。一般的にはシステムのユーザーは、サーバー及びメディアにアクセスできないようにすべきである。 • ローカル及び外部からの攻撃に対するネットワークシステムの脆弱性。 • リモートネットワーク更新。例えば、ネットワーク接続されたシステムのベンダーによる自動アップデート。 • システム設定・構成設定・主要データのセキュリティ。システムの重要なデータや運転パラメータへのアクセスは適切に制限すべきであり、〔システム〕設定・構成設定の変更は、許可された社員により、変更管理プロセスに従ってコントロールすべきである。 • OS のクロックを、接続されているシステム群のクロックと同期させる。またすべてのクロックへのアクセスを許可された社員に限定する。 • 侵入防止・検出システム等の、適切なネットワークセキュリティ対策を講じるべきである。

	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.	• ファイアウォールを設定し、重要なデータや操作を保護すべきである。ポートの開放 (についてのファイアウォールのルール) は、最小特権ポリシーに基づくべきであり、ファイアウォールのルールを可能な限り厳しくし、許可されたトラフィックのみが通過できるようにする。 規制対象ユーザーは、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について定期的なレビューを行い (例えば、IT インフラに対して、セキュリティ上の潜在的な弱点を特定するネットワーク脆弱性スキャンを用いる) 、OS のセキュリティ対策が最新に維持されていることを確実にする。
	Potential risk of not meeting expectations/items to be checked • 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.	**期待事項を満たさない場合の潜在的なリスク /チェックすべき項目** • ハードウェア及びソフトウェアへのアクセスが適切に保護され、許可された社員に限定されていることをチェックする。 • 適切な認証方法が実装されていることを検証する。認証方法には、ユーザーID とパスワードが含まれるが、他の方法も可能であり、また必要となる場合もある。ただし、ユーザーの本人証明ができることが必須である。 • 重要なデータを持つシステムにインターネット経由でリモート認証する場合は、パスコードトークンやバイオメトリクス等の追加の認証技術が採用されていることを検証する。 • システムの重要な運転パラメータへのアクセスが適切にコントロールされていることを検証する。また、GMP/GDP の重要な連続作業において、必要に応じてシステムがイベントの順序及びパラメータを強制していることを検証する。

3.	**Expectation** Network protection Network system security should include appropriate methods to detect and prevent potential threats to data. The level of network protection implemented should be based on an assessment of data risk. 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. Firewalls should be supplemented with appropriate virus-protection or intrusion prevention/detection systems to protect data and computerised systems from attempted attacks and malware.	**期待事項** ネットワークの保護 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・防止するための適切な方法を含むべきである。 実装するネットワーク保護のレベルは、データリスクのアセスメントに基づくべきである。 許可のないアクセスを防ぐためにファイアウォールを使用し、そのルールを仕様に照らして定期的にレビューすべきである。これは、許可されたトラフィックのみを通過させるよう、十分に限定的に設定されていることを確実にするためである。このレビューは文書化すべきである。 データやコンピュータ化システムを、攻撃の試みやマルウェアから保護するために、適切なウイルス保護システムや侵入防止・検出システムでファイアウォールを補強すべきである。
	Potential risk of not meeting expectations/items to be checked • 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 rules may become obsolete permitting unwanted traffic or intrusions.	**期待事項を満たさない場合の潜在的なリスク/チェックすべき項目** • 不適切なネットワークセキュリティは、許可のないアクセス・誤使用・改変に対す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チェックする。アクセスを承認・監視・削除するためのプロセスがあるべきである。 • 脅威を防ぎ、ネットワークへの侵入の試みを検出するようにシステムを設計し、これらの対策を設定・監視・維持すべきである。 • ファイアウォールのルールは、(例えば、サーバーのメンテナンス等で一時的にポートが開放される等) 時間の経過とともに変わることがある。一度も見直し

		をしないと、ファイアウォールルールが古くなり、望ましくないトラフィックや侵入を許してしまう可能性がある。
4.	Electronic signatures used in the place of handwritten signatures should have appropriate controls to ensure their authenticity and traceability to the specific person who electronically signed the record(s). 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. Where used, electronic signature functionality should automatically log the date and time when a signature was applied. The use of advanced forms of electronic signatures is becoming more common (e.g. the use of biometrics is becoming more prevalent by firms). The use of advanced forms of electronic signatures should be encouraged.	手書き署名の代わりに使用される電子署名について、適切なコントロールを設け、その真正性と記録に電子署名した者へのトレーサビリティを確実にすべきである。 電子署名は、それぞれの〔署名された〕記録に恒久的にリンクすべきである。すなわち、署名後に、署名された記録に変更を加えた場合、その記録は、修正されたことが示されるとともに署名されていないように見えるべきである。 電子署名機能を使用する場合は、署名が行われた日時を自動的に記録する必要がある。 高度な形式の電子署名を使用することが一般的になってきている (例えば、バイオメトリクスの使用が会社に浸透してきている) 。高度な形式の電子署名の使用を奨励すべきである。
	Potential risk of not meeting expectations/items to be checked • 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.	**期待事項を満たさない場合の潜在的なリスク/チェックすべき項目** • 電子署名が適切にバリデートされていること、スタッフへの〔電子署名の〕発行がコントロールされていること、常に電子署名の個人への帰属性を容易に示すことができることをチェックする。 • 電子署名を行った後にデータを変更した場合は、データを再度レビューして再署名するまでは、署名を無効にすべきである。
5.	Restrictions on use of USB devices 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	USB 機器の使用制限について システムセキュリティの観点から、コンピュータ化システムを構成設定し、コンピュータクライアントや GMP/GDP に不可欠なデータを持つサーバーでは、USB メモリ・格納装置の使用による脆弱性を防ぐべきである。必要であれば、ポートを承認された目的のためにのみ開放するようにし、またすべての USB

	properly scanned before use. 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.	デバイスを使用前に適切にスキャンする。 セキュリティ違反を防止するために、会社のコンピュータクライアントや GMP/GDP データを持つサーバーで個人の USB 機器 (フラッシュドライブ、カメラ、スマートフォン、キーボード等) を使用することや、個人のコンピュータで会社の USB 機器を使用することは、コントロールすべきである。
	Potential risk of not meeting expectations/items to be checked • 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.	**期待事項を満たさない場合の潜在的なリスク /チェックすべき項目** • 〔USB 機器の使用制限〕は (USB デバイスがキーボード等の外部デバイスと偽ってコンピュータを騙すことを OS が防げず、その USB デバイスには実行可能なコードが含まれており、それを起動することができるという) OS の脆弱性が知られている状況において特に重要である。 • このようなデバイスの使用を許可されたユーザーに限定するためのコントロールを設け、USB デバイスの使用前にスクリーニングする措置を講じるべきである。

9.6 Audit trails for computerised systems

9.6 コンピュータ化システムの監査証跡

Item:	**Audit Trails**	**監査証跡**
1.	**Expectation** Consideration should be given to data management and integrity requirements when purchasing and implementing computerised systems. Companies should select software that includes appropriate electronic audit trail functionality. Companies should endeavour to purchase and upgrade older systems to implement software that includes electronic audit trail functionality. It is acknowledged that some very simple systems lack appropriate audit trails; however, alternative arrangements to verify the veracity of data should	**期待事項** コンピュータ化システムを購入し、導入する際には、データマネジメントとデータインテグリティの要件を考慮する必要がある。会社は、適切な電子的な監査証跡機能を備えるソフトウェアを選択すべきである。 会社は、電子的な監査証跡機能を備えるソフトウェアを実装しているシステムを購入するか、古いシステムをアップデートする【訳注】よう努めるべきである。 【訳注：原文では、”purchase and upgrade”と and が使われており、「古いシステムを購入

	be implemented, e.g. administrative procedures, secondary checks and controls. Additional guidance may be found under section 9.10 regarding hybrid systems. Audit trail functionality should be verified during validation of the system to ensure that all changes and deletions of critical data associated with each manual activity are recorded and meet ALCOA+ principles. 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: • 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 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. 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	してアップデートする」となっている。これは or の誤りと考え、そのように訳した。】 非常に単純なシステムの中には適切な監査証跡がないものがあることは了解されているが、データの正しさを検証するために代替手段 (例：業務管理手順、二次的なチェックやコントロール) を実装する必要がある。ハイブリッドシステムに関するガイダンスは、第 9.10 章を参照のこと。 監査証跡機能は、システムをバリデーションする時に検証し、手作業に関連する重要なデータへのすべての変更・削除が記録され、ALCOA+の原則を満足することを確実にすべきである。 規制対象ユーザーは、各システムの監査証跡の性質と機能を理解し、適格性評価の際に、それぞれの監査証跡をアセスメントし、監査証跡ごとに GMP/GDP に関連する程度を判断し、重要かつ GMP/GDP に関連するデータに対する監査証跡が正しく管理され、構成設定されることを確実にすべきである。この作業は、どの〔監査〕証跡の、どのエントリが重要で、定められた頻度でレビューする必要があるか決定する上で大事である。例えば、このアセスメントの後で、監査証跡のレビューでは以下に焦点を当てることができる。 • データの変更や修正に関連するエントリ/データを特定し、レビューする。 • 例外によるレビューー 異常な活動や許可のない活動に焦点を当てる。 • 〔機能に〕制限があり、パラメータ/データを変更できてしまう、又は活動〔結果〕を変更できてしまうシステム。 • 注：適切に設計されたシステムが、パラメータ/データの変更を防止する権限設定や、構成設定の変更を防止するアクセス制限を備えていれば、関連する監査証跡を詳細に調べなくてもよいかもしれない。 監査証跡機能は常に有効であり、ロックされている必要があり、機能の無効化・削除・修

	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. Non-critical audit trails reviews can be conducted during system reviews at a pre-defined frequency. This review should be performed by the originating department, and where necessary verified by the quality unit (e.g. during batch release, self-inspection or investigative activities).	正は不可能とすべきである。システム管理者権限を持つユーザーが監査証跡機能を無効化・削除・修正できてしまう場合には、それが発生した旨のエントリが監査証跡に自動的に記録されるべきである。 会社は、監査証跡に必要なデータを決定するための方針とプロセス、及びリスクマネジメントの原則に従った監査証跡のレビューを概説した手順を実行すべきである。 各業務に関連する重要な監査証跡は、その業務に関連する他のすべての記録と一緒に、〔他の監査証跡とは〕独立して、レビューすべきであり、その業務の完了をレビューする前 (例：バッチリリース前) に行うべきである。これは重要なデータ及びその変更に問題がないことを〔前もって〕確認しておくためである。このレビューは、データの発生元となる部門が行うべきであり、必要な場合には品質部門が (例えば、自己点検時又は調査活動時に) 検証する。 重要でない監査証跡のレビューは、事前に定められた頻度で、システムレビュー中に実施してもよい。このレビューは、データの発生元となる部門が実施し、必要な場合には品質部門が (例えば、バッチリリース時、自己点検時又は調査活動時に) 検証することが望ましい。
	Potential risk of not meeting expectations/items to be checked • 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)	**期待事項を満たさない場合の潜在的なリスク/チェックすべき項目** • バリデーション文書は、監査証跡が機能していること、及びシステム内のすべての活動、変更、及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示すべきである。 • 監査証跡が (品質リスクマネジメントの原則に従って) 定期的にレビューされ、不一致があれば調査されていることを検証する。 • 電子的な監査証跡システムが存在しない場合は、完全な監査証跡システム (統合

	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.	されたシステム、又はバリデートされたインター フェイスを使用した独立した監査ソフトウェア) が利用可能になるまで、データへの変更を紙ベースの記録で示してもよい。このようなハイブリッドシステムは、PIC/S GMP Guide の Annex 11 に記載されている統合された監査証跡【訳注】と同等のものを実現する場合のみ許される。 【訳注：Annex 11 で記載されているのは「監査証跡」であり、「統合された監査証跡」ではない。】 • 監査証跡を適切にレビューしないと、不正操作されたデータや誤ったデータが、品質部門及び (又は) Authorised Person によって誤って受け入れられてしまう可能性がある。 • どのデータが重要なのか、どのような変更や削除を記録 (監査証跡) すべきかの詳細を明確に文書化すべきである。
2.	**Expectation** Where available, audit trail functionalities for electronic-based systems should be assessed and configured properly to capture any critical activities relating to the acquisition, deletion, overwriting of and changes to data for audit purposes. Audit trails should be configured to record all manually initiated processes related to critical data. The system should provide a secure, computer generated, time stamped audit trail to independently record the date and time of entries and actions that create, modify, or delete electronic records. The audit trail should include the following parameters: • 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	**期待事項** 電子ベースシステムの監査証跡機能が利用可能な場合は、アセスメントするとともに、監査時に利用できるよう、データ取得・削除・上書き・変更に関連するすべての重要な活動を捕捉するように適切に構成設定すべきである。 監査証跡は、重要なデータに関連するすべての手動で開始したプロセスを記録するように構成設定すべきである。 システムは、安全で、コンピュータが生成するタイムスタンプ付きの監査証跡を提供すべきである。監査証跡には、〔操作者とは〕独立して、各エントリの日付・時刻、及び電子記録を作成・変更・削除するアクションが記録される。 監査証跡には、以下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ーの詳細。

	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. The audit trail should allow for reconstruction of the course of events relating to the creation, modification, or deletion of an electronic record. The system 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. 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). 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.	• どのようなアクションが発生したか。何が変更されたのか、新旧の値を含む。 • いつアクションが実行されたか、日付と時間を含む。 • なぜアクションが実行されたか (理由) 。 • データの変更や修正の場合は、変更を許可した者の名前。 監査証跡は、電子記録の作成・修正・削除に関連するイベントの経過を再現できるようにする必要がある。 システムは、監査証跡を印刷することができ、また電子コピーを提供することができるべきである。〔監査証跡を〕オンラインで、システム上で閲覧する場合でも、ハードコピーで閲覧する場合でも、監査証跡は意味のあるフォーマットで提供すべきである。 可能であれば、監査証跡は、コンピュータ化システム内であれば利用できる動的な機能 (例：検索機能やスプレッドシート等へのデータのエクスポート機能) を保持すべきである。 注：監査証跡は、変更コントロールシステムと混同すべきではない。変更コントロールシステ ムでは、変更は PQS〔医薬品品質システム〕 に基づいて適切にコントロールし、承認する必要がある。
	Potential risk of not meeting expectations/items to be checked • 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	**期待事項を満たさない場合の潜在的なリスク /チェックすべき項目** • 監査証跡のフォーマットを検証し、重要かつ関連する情報がすべて取得されていることを確認する。 • 監査証跡は、過去のすべての値を含むべきであり、記録を変更したときは、以前の記録情報を上書きしたり、隠したりしないこと。 • 監査証跡のエントリは、真の時間で記録し、活動の実際の時間を反映すべきである。特に個々の対話型操作や作業順序

	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.	が重要な場合 (例：混合容器への 4 つの原材料の投入を電子的に記録する場合) 、多くの連続した対話型操作を〔まとめて〕同じ時間で記録したり、又はすべての対話型操作完了後にたった 1 つのエントリとして監査証跡に記録したりするシステムは、データインテグリティの期待に適合していない可能性がある。投入の順番が重要なプロセスパラメータ〔Critical Process Parameter〕(CPP) である場合、それぞれの投入はタイムスタンプ付きで個別に記録されるべきである。投入の順番が CPP でないのであれば、4 つの原材料の投入を 1 つのタイムスタンプ付きのアクティビティとして記録してもよい。

9.7 Data capture/entry for computerised systems

9.7 コンピュータ化システムへのデータ収集/入力

Item:	**Data capture/entry**	**データ収集/入力**
1.	**Expectation** Systems should be designed for the correct capture of data whether acquired through manual or automated means. For manual entry: • The entry of critical data should only be made by authorised individuals and the system should record details of the entry, the individual making the entry and when the entry was made. • Data should be entered in a specified format that is controlled by the software, validation activities should verify that invalid data formats are not accepted by the system. • All manual data entries of critical data should be verified, either by a second operator, or by a validated computerised means. • Changes to entries should be captured in the audit trail and reviewed by an appropriately authorised and independent person. For automated data capture: (refer also to table	**期待事項** システムは、手動・自動のいずれかの方法であれ、データを正しく取得するように設計すべきである。 マニュアル入力の場合： • 重要なデータの入力は、許可された個人によってのみ行われるべきであり、システムは、入力の詳細、入力を行った個人、及びいつ入力が行われたか、を記録すべきである。 • データは、ソフトウェアによってコントロールされる指定フォーマットで入力すべきである。バリデーション活動ではシステムが無効なデータフォーマットを受け付けないことを検証する。 • 重要なデータを手作業で入力する場合は、二人目のオペレーター又はバリデートされたコンピュータを用いた手段により検証すべきである。 • 入力内容の変更は、監査証跡に記録し、

	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.	適切に許可された、独立した者が確認すべきである。 自動データ収集の場合： (表 9.3 も参照) • 〔データ〕発生元システムとデータを収集・記録するシステムの間のインターフェイスをバリデートし、データの正確性を確実にすべきである。 • システムに取り込まれたデータは、不正操作・消失・変更に対して脆弱でないフォーマットでメモリ【訳注】に保存すべきである。 【訳注：永続的な電磁的記録媒体の意図と思われる。】 • システムソフトウェアにバリデートされたチェック機能を組み込み、データ及びデータに関連するすべてのメタデータが完全に収集されるようにすべきである。
	Potential risk of not meeting expectations/items to be checked • 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.	**期待事項を満たさない場合の潜在的なリスク/チェックすべき項目** • 手動で重要なデータをコンピュータ化システムへ入力している場合は、適切な二次チェックが行われていることを確認する。 • 自動データ収集を利用しているシステムについては、バリデーション記録をレビューすべきである。これにより、データ検証及びデータインテグリティの方策が実施され、効果的であることを確認する。例えば、自動保存機能がバリデートされているか、またユーザーはこの機能を無効にすることができず、報告されていないデータを作り出せないことを検証する。
2.	**Expectation** Any necessary changes to data should be authorised and controlled in accordance with approved procedures. For example, manual integrations and reprocessing of laboratory results should be	**期待事項** 必要なすべてのデータ変更は、承認された手順に従って許可し、コントロールすべきである。 例えば、ラボの結果を手作業で統合したり再

	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. 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.	処理する場合は、承認されコントロールされた方法で行われるべきである。会社の品質部門は、データの変更が、必要な場合にのみ、指名された個人により行われるようにするための方策を確立すべきである。 (変更されていない) 原本データは、当初のコンテキストで保管すべきである。 生データに対するあらゆる変更及び修正は、完全に文書化し、一人以上の適切な訓練を受けた適格な個人によりレビュー及び承認される必要がある。
	Potential risk of not meeting expectations/items to be checked • 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.	**期待事項を満たさない場合の潜在的なリスク /チェックすべき項目** • データの修正や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検証する。提案された変更の正式な承認、コントロールされた/制限された/定義された変更、及び変更後の正式なレビューの適切なプロセスがあることを証拠により示すべきである。

9.8 Review of data within computerised systems

9.8 コンピュータ化システム内のデータのレビュー

Item:	**Review of electronic data**	**電子データのレビュー**
1.	**Expectation** 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. 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,	**期待事項** 規制対象ユーザーは、リスクアセスメントを実施し、コンピュータ化システムで生成される GMP/GDP に関連するすべての電子データ、及びデータ重要度を明らかにすべきである。規制対象ユーザーは、監査により、明らかになった重要なデータを検証し、業務が正しく行われたか、電子記録の原本の情報が変更 (修正・削除・上書き) されたか、報告されていない関連データが作成されたかを判断すべきである。すべての変更は正式な許可のもとで行うべきである。 SOP には、データを第二のオペレーターによってチェックするプロセスを記述すべきである。SOP は、レビュー対象となる重要な生データ、データサマリのレビュー、関連するロ

	and explain how the review is performed, recorded and authorised. The review of audit trails should be part of the routine data review within the approval process. The frequency, roles and responsibilities of audit trail review should be based on a risk assessment according to the GMP/GDP relevant value of the data recorded in the computerised system. For example, for changes of electronic data that can have a direct impact on the quality of the medicinal products, it would be expected to review audit trails prior to the point that the data is relied upon to make a critical decision, e.g. batch release. The regulated user should establish an SOP that describes in detail how to review audit trails, what to look for and how to perform searches etc. The procedure should determine in detail the process that the person in charge of the audit trail review should follow. The audit trail review activity should be documented and recorded. Any significant variation from the expected outcome found during the audit trail review should be fully investigated and recorded. A procedure should describe the actions to be taken if a review of audit trails identifies serious issues that can impact the quality of the medicinal products or the integrity of data.	グブック及びハードコピー記録のレビューについて概説するとともに、レビューをどのように実施し、記録し、承認するかを説明すべきである。 監査証跡のレビューは、承認プロセスにおける日常的なデータレビューの一部とすべきである。 監査証跡のレビューの頻度、役割及び責任は、コンピュータ化システムに記録されたデータの GMP/GDP 上の価値に応じたリスクアセスメントに基づくべきである。例えば、医薬品の品質に直接影響を及ぼす可能性のある電子データが変更された場合、重要な意思決定 (例：バッチリリース) にそのデータを使う前に、監査証跡をレビューすることが期待されている。 規制対象ユーザーは、どのように監査証跡をレビューするか、何を見るか、どのように検索するか等を詳細に説明する SOP を設けるべきであり、そこで監査証跡のレビュー者が従うべきプロセスを詳細に定めるべきである。監査証跡のレビュー活動は、文書化し、記録すべきである。 監査証跡のレビューで、期待される結果からの重大な乖離が見つかった場合、徹底的に調査し、記録すべきである。監査証跡のレビューにより医薬品の品質やデータ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を見つけたときに取るべきアクションを、手順書に記載すべきである。
	Potential risk of not meeting expectations/items to be checked • 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	**期待事項を満たさない場合の潜在的なリスク/チェックすべき項目** • ローカル手順をチェックし、電子データがその重要度 (製品品質及び/又は意思決定への影響) に基づいてレビューされていることを確認する。レビューの証拠を記録し、査察官に提供できるようにすること。 • 内部又は外部への報告のためにデータサマリを使用する場合は、そのサマリが生データと一致することの検証が済んでい

	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.	ることを示す証拠を用意しておく必要がある。 • 規制対象者が、二次レビューや監査証跡レビューの実行手順や、レビューで問題が発見された場合に辿るべき実行手順を説明する詳細な SOP を持っていることをチェックする。 • グローバルシステムが使用されている場合、日時の記録には、記録の同時記録性を証明するためにタイムゾーンの記録が必要となる場合がある。 • 実施されたことがわかっているデータの変更・修正・削除について、それらが実際に監査証跡機能により記録されていることをチェックする。
2.	The company's quality unit should establish a program and schedule to conduct ongoing reviews of audit trails based upon their criticality and the system's complexity in order to verify the effective implementation of current controls and to detect potential non-compliance issues. These reviews should be incorporated into the company's self-inspection programme. 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.	会社の品質部門は、監査証跡の重要度とシステムの複雑さに基づいて、継続的なレビューを行うプログラムとスケジュールを確立することで、現在のコントロールが効果的に実施されていることを検証し、不適合を引き起こす可能性のある問題を検出できるようにすべきである。このレビューは、会社の自己点検プログラムに組み込むべきである。 監査証跡の乖離に対応し、調査するための手順を設けるべきである。手順には、上級管理職、及び必要に応じて当局に連絡するためのエスカレーションプロセスを含める。
	Potential risk of not meeting expectations/items to be checked • 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).	**期待事項を満たさない場合の潜在的なリスク/チェックすべき項目** • 監査証跡のチェックが、既存のコントロールの有効性及びデータレビューの内部手順への適合性を検証する意図で、自己点検プログラムに組み込まれていることを検証する。 • 監査証跡のレビューは、random (偶然に基づいて選択) と targeted (重要性やリスクに基づいて選択) の両方を行う必要がある。

9.9 Storage, archival and disposal of electronic data

9.9 電子データの保存、アーカイブ、処分

Item:	**Storage, archival and disposal of electronica data**	**電子データの保存・アーカイブ・処分**
1.	**Expectation** Storage of data should include the entire original data and all relevant metadata, including audit trails, using a secure and validated process. If the data is backed up, or copies of it are made, then the backup and copies 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.	**期待事項** データを保存するときは、安全でバリデートされたプロセスを用いて、原本データ全体と関連するすべてのメタデータ (監査証跡を含む) を保存すべきである。 データがバックアップされている、又はコピーが作成されている場合は、データへの許可のないアクセス・変更・削除、又はそれら〔コントロール〕への変更を禁止するために、バックアップ及びコピーに対しても、〔元のデータと〕同様な、適切なレベルのコントロールが必要である。例えば、データを携帯可能なハードディスクにバックアップする場合は、ハードディスクからデータを削除することを禁止すべきである。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以下の通りである： • 動的な電子記録の真正コピーを作成できる。その際、原本の記録のコンテンツ全体 (すなわち、すべてのデータと関連するすべてのメタデータが含まれる) 及び意味が保存されることが期待されている。 • 保存されたデータは、完全な見読性のあるフォーマットでアクセスできる必要がある。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又はコピーにアクセスするために、会社は、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かもしれない。 • 日常的なバックアップコピーは、災害に備えて、遠隔地 (物理的に離れた場所) に保存すべきである。 • バックアップデータは、定められた規制上の保存期間のすべての期間において見読性を持つ必要がある。これはソフトウェアが新しいバージョンに更新された

		り、より性能の良いものに置き換えられたりした場合も同様である。 • システムは、すべてのデータ (メタデータや監査証跡を含む) のバックアップと復元を可能にすべきである。
	Potential risk of not meeting expectations/items to be checked • 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.	**期待事項を満たさない場合の潜在的なリスク/チェックすべき項目** • データの保存・バックアップ・アーカイブを行うシステムが、すべてのデータと関連メタデータを取り込むように設計されていることをチェックする。これらのシステムがバリデートされ、検証されたことを示す、文書化された証拠があるべきである。 • 収集す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いて決定すべきであり、ユーザーは、活動やプロセスの再現に不可欠なメタデータがすべて収集されることを確実にすべきである。 • 新しいシステムで置き替えられた〔旧い〕システムやアップグレード前の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チェックする。
2.	**Expectation** 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.	**期待事項** 記録保管手順には、メタデータを保管するための規定を含めるべきである。これにより、将来の問い合わせや調査において、バッチに関連して発生した活動を再現できるようになる。
3.	**Expectation** 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. The data should be accessible and readable and its integrity maintained for all the period of	**期待事項** データは、書面による手順に従って、定期的にバックアップし、アーカイブすべきである。アーカイブのコピーは、バックアップや原本データが保存されている場所とは別の離れた場所で、物理的な (又は必要に応じて仮想的な) 安全を確保すべきである。 データは、アーカイブの全期間にわたって、

	archiving. There should be in place a procedure for restoring archived data in case an investigation is needed. The procedure in place for restoring archived data should be regularly tested. If a facility is needed for the archiving process then specific environmental controls and only authorised personnel access should be implemented in order to ensure the protection of records from deliberate or inadvertent alteration or loss. When a system in the facility has to be retired because problems with long term access to data are envisaged, procedures should assure the continued readability of the data archived. For example, it could be established to transfer the data to another system.	アクセス可能で、見読性があり、インテグリティが維持される必要がある。 調査が必要な場合に備えて、アーカイブデータを復元するための手順を設けるべきである。アーカイブデータを復元するための手順は、定期的にテストすべきである。 アーカイブプロセスのために施設〔の利用〕が必要な場合は、意図的又は不注意による改ざんや消失から記録を確実に保護するために、〔その施設の〕環境のコントロール及び許可された社員のみによるアクセスを実現する必要がある。長期的なデータアクセスに問題が想定され、施設内のシステムをリタイアしなければならない場合、アーカイブデータの継続的な見読性を保証する手順を設ける必要がある。例えば、データを別のシステムに転送することで対応できるであろう。
	Potential risk of not meeting expectations/items to be checked • 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.	**期待事項を満たさない場合の潜在的なリスク/チェックすべき項目** • アーカイブデータには、ソフトウェアアプリケーションの更新や機器の交換によって、データへのアクセスや見読性が失われるリスクがある。アーカイブデータにアクセスできること、及びアーカイブデータのレビューに必要なソフトウェアへのアクセスが維持されていることを検証する。 • データのアーカイブのために外部又は第三者の施設を利用する場合、これらのサービスプロバイダーはアセスメントの対象となる。また、すべての責任は品質技術合意書に記録すべきである。合意書及びアセスメント記録をチェックし、アーカイブされた記録のインテグリティを確実にするために十分な検討が行われたことを検証する。
4.	**Expectation** It should be possible to print out a legible and meaningful record of all the data generated by a computerised system (including metadata). If a change is performed to records, it should be	**期待事項** コンピュータ化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) について、判読性があり、意味のある記録を印刷で

	possible to also print out the change of the record, indicating when and how the original data was changed.	きるべきである。 記録が変更された場合、原本データがいつ、どのように変更されたかを示す記録の変更内容も印刷できるようにする。
	Potential risk of not meeting expectations/items to be checked • 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.	**期待事項を満たさない場合の潜在的なリスク/チェックすべき項目** • システムのバリデーション文書をチェックし、システムが判読性・完全性のある記録を生成できることを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を検証してもよい。
5.	**Expectation** 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.	**期待事項** 電子的に保存されたデータを処分するプロセスを記載した手順を設ける必要がある。その手順は、データのアセスメント、保存期間の配分についてのガイダンスとともに、不要になったデータの処分について説明すべきである。
	Potential risk of not meeting expectations/items to be checked • 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.	**期待事項を満たさない場合の潜在的なリスク/チェックすべき項目** • データの処分条件が手順に明確に規定されていることをチェックする。また、必要なデータがライフサイクル途中でうっかり処分されないように配慮されていることを確認する。

9.10 Management of Hybrid Systems

9.10 ハイブリッドシステムの管理

Item:	**Management of Hybrid Systems**	**ハイブリッドシステムの管理**
1.	Hybrid systems require specific and additional controls in reflection of their complexity and potential increased vulnerability to manipulation of data. For this reason, the use of hybrid systems is discouraged and such systems should be replaced whenever possible. Each element of the hybrid system should be	ハイブリッドシステムは、その複雑さとデータ不正操作に対する潜在的な脆弱性のため、特別な追加コントロールが必要となる。そのため、ハイブリッドシステムを使用することは推奨しない。そのようなシステムは可能な限り置き換えるべきである。

	qualified and controlled in accordance with the guidance relating to manual and computerised systems as specified above. Appropriate quality risk management principles should be followed when assessing, defining, and demonstrating the effectiveness of control measures applied to the system. A detailed system description of the entire system should be available that outlines all major components of the system, the function of each component, controls for data management and integrity, and the manner in which system components interact. Procedures and records should be available to manage and appropriately control the interface between manual and automated systems, particularly steps associated with: • manual input of manually generated data into computerised systems; • transcription (including manual) of data generated by automated systems onto paper records; and • automated detection and transcription of printed data into computerised systems.	ハイブリッドシステムの各要素は、上記の手作業システム及びコンピュータ化システムに関するガイダンスに従って、適格性評価を実施し、コントロールする必要がある。 適切な品質リスクマネジメントの原則に従って、システムに適用されるコントロール方策をアセスメントし、定義し、有効性を示すべきである。 システム全体の詳細なシステム記述書を用意すべきである。そこには、システムのすべての主要なコンポーネント、各コンポーネントの機能、データマネジメントとデータインテグリティのためのコントロール、システムコンポーネント間の相互作用が概説される。 手作業システムと自動システムの間のインターフェイスを管理し、適切にコントロールするための手順と記録を用意すべきである。特に以下に関連する実行手順： • 手作業で作成したデータをコンピュータ化システムへマニュアル入力する。 • 自動化されたシステムで生成されたデータを紙の記録に転記 (手作業を含む) する。 • 印刷されたデータを自動的に検出し、コンピュータ化システムへ転記する。
	Potential risk of not meeting expectations/items to be checked • 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	**期待事項を満たさない場合の潜在的なリスク/チェックすべき項目** • ハイブリッドシステムが明確に定義され、特定され、システムの各関連する有効な要素がバリデートされていることをチェックする。 • 手作業システムとコンピュータ化システムの間のインターフェイスに注意すべきである。査察官は、システム間で手作業による転記が行われる場合、適切なコントロールと二次チェックが行われていることを検証すべきである。 • 原本データは、転記や加工した後も保管しておく必要がある。

	systems. Particular attention should be paid to verifying: - The extent of qualification and/or validation of the computerised system; and, - The robustness of controls applied to the management of the manual element of the hybrid system due to the difficulties in consistent application of a manual process.	• ハイブリッドシステムは、一般的にコンピュータ化システムと手作業システムの組み合わせで構成される。特に以下を検証する際には注意が必要である： - コンピュータ化システムの適格性評価及び (又は) バリデーションの程度 - ハイブリッドシステムの手作業部分の管理に適用されるコントロールの堅牢性。〔コントロールを〕手作業プロセスに、一貫性をもって適用することが困難なため。
2.	Procedures should be in place to manage the review of data generated by hybrid systems which clearly outline the process for the evaluation and approval of electronic and paper-based data. Procedures should outline: • 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	ハイブリッドシステムで生成されたデータのレビューを管理するための手順を設ける必要がある。そこには電子データと紙ベースのデータをレビューし、承認するプロセスが明確に概説される。手順には、以下を記載する： • 完全な記録を作成するために、電子データと紙ベースのデータをどのように組み合わせるか、という指示。 • 〔電子、手作業〕それぞれのシステムのデータ出力の承認に関する期待事項。 • ハイブリッドシステムについて特定されたリスク。コントロールが有効に適用されていることの検証に焦点を当てる。
	Potential risk of not meeting expectations/items to be checked • Verify that instructions for the review of hybrid system data is in place.	**期待事項を満たさない場合の潜在的なリスク/チェックすべき項目** • ハイブリッドシステムのデータをレビューするための指示が存在することを検証する。

10. DATA INTEGRITY CONSIDERATIONS FOR OUTSOURCED ACTIVITIES

10. アウトソース活動におけるデータインテグリティの考慮事項

10.1 General supply chain considerations

10.1 サプライチェーンに関する一般的な考慮事項

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、医薬品の安全かつ継続的な供給確保のために協業する複数のパートナー会社により構成されることが多い。典型的なサプライチェーンでは API 生産業者、剤形製造業者、分析研究所、卸売業者・流通業者が関与しており、その組織や場所も様々である。また、これらのサプライチェーンは、アウトソースサービス、IT サービス及びインフラストラクチャ、専門技術、コンサルティングサービスといった付加的な組織によって支えられていることが多い。
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実にする上で重要な役割を果たす。サプライチェーンのパートナーから、信頼性の低い又は改ざんされたデータや原料が提供されるような場合、契約委託者のデータガバナンス方策は著しく弱められるであろう。このことは、原材料の供給者、製造受託会社、分析サービス、卸売業者、契約サービスプロバイダー、コンサルタント等、すべてのアウトソースされる活動に当てはまる。
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.	サプライチェーンのパートナー及びアウトソースした活動を、最初及び定期的に、適格性評価する際に、データインテグリティリスクと適切なコントロール方策を考慮すべきである。
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.	各組織では、サプライチェーンから入手する情報 (例：サマリ記録、コピー/プリントアウト) のデータインテグリティの限界と、遠隔監視の課題を認識しておくことが重要である。これらの限界は、本ガイダンスの 第 8.11 章で述べられているものと同様である。これを認識しておくことにより、品質リスクマネジメントアプローチを用いて、〔サプライチェーンから入手する情報の〕データイン

		テグリティの検証と監督に資源を集中させることができる。

10.2 Routine document verification

10.2 日常的な文書の検証

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.	サプライチェーンでは、ある組織から別の組織へ渡される文書やデータに依存することになる。多くの場合、契約委託者が、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現実的ではない。品質リスクマネジメントの原則を用いて、外部委託している供給者や契約者に対する強固な適格性評価プロセスに重点を置くべきである

10.3 Strategies for assessing data integrity in the supply chain

10.3 サプライチェーンにおけるデータインテグリティをアセスメントするための戦略

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:	会社は、サプライチェーン及びアウトソースされた活動について定期的にリスクレビューすべきである。リスクレビューでは、どの程度データインテグリティコントロールが必要なのか評価する。リスクレビューの頻度は、リスクマネジメントの原則を用いて、契約受託者が提供するサービスの重要度に応じたものとすべきである。リスクレビューで考慮すべき情報には以下が含まれる： • 訪問監査の結果。データガバナンス方策に着目する。 • データインテグリティやセキュリティに関する国際的な基準やガイドラインへの適合を説明できるようにする。 • 定例報告書で提出されたデータのレビュー。例を下表に示す【訳注】： 【訳注：下表は原文では表形式になっているが、訳文では表を列ごとに並べている。】

Area for review	**レビュー対象領域**
Comparison of analytical data reported by the contractor or supplier vs in-house data from analysis of the same material	契約者又は供給者から報告された分析データと、同じ原料を分析した社内データとの比較。
Rationale	**根拠**
To look for discrepant data which may be an indicator of falsification	改ざんが行われたことの指標となる矛盾したデータを探すため。

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.	製造業者と、原料の供給者・サービスプロバイダー・製造受託会社 (CMO) ・ (流通の場合) 医薬品の供給者との間には、品質合意書 (又はそれに相当するもの) が締結されるべきである。そこには、サプライチェーン全体でデータインテグリティを確実にするための具体的な規定が含まれる。これは、データガバナンスに関する期待事項を提示するとともに、契約受託者から契約委託者へのエラー・逸脱の透明性のある報告を行うことで実現できるであろう。また、契約受託者の拠点で発見されたすべてのデータインテグリティの障害を、契約委託者に通知するという要件も必要である。
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 (又は製造業者に代わって第三者) が行う、原薬の供給者/製造業者・重要な中間供給者・一次包装材料/印刷された包装材料の供給者・ 製造委託先・サービス提供者への監査では、契約組織におけるデータインテグリティ方策を検証すべきである。契約受託者は、監査中に、契約委託者のために生成したデータに対する合理的なアクセスを〔監査者に〕提供し、データインテグリティ及びデータマネジメントの原則に適合していることのアセスメント及び実証ができるようにすることが期待されている。

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:	契約委託者の品質部門は、監査及び日常的な監視により、品質リスクマネジメントアプローチを用いて、元となっている電子データ及びメタデータを適切に検証すべきである。これは以下のような手段で達成できる：

Site audit 訪問監査	Review the contract acceptors organisational behaviour, and understanding of data governance, data lifecycle, risk and criticality.	契約受託者の組織的行動、及びデータガバナンス、データライフサイクル、リスク、重要度に関する理解をレビューする。
Material testing vs CoA 原料試験と分析証明書の比較	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.	分析試験の結果とサプライヤーが報告した分析証明書〔Certificates of Analysis〕(CoA)を比較する。精度、精密度、純度の結果の不一致を調べる。この作業は、原料や供給者のリスクに応じて、日常的に、定期的に、又は抜き打ちで行う。必要に応じて、サンプルを定期的に検定試験することを検討する。
Remote data review リモートデータレビュー	The contract giver may consider offering the Contracted Facility/Supplier use of their own hardware and software system (deployed over a Wide Area Network) to use in batch manufacture and testing. The contract giver may monitor the quality and integrity of the data generated by the Contracted Facility personnel in real time. In this situation, there should be segregation of duties to ensure that contract giver monitoring of data does not give provision for amendment of data generated by the contract acceptor.	契約委託者は、バッチ製造及び試験のために、契約施設・供給者に自身のハードウェア及びソフトウェアシステム (Wide Area Network 上に配置) を使わせることを検討してもよい。契約委託者は、契約施設の社員が生成したデータ品質及びインテグリティをリアルタイムで監視することができる。 このような状況では、データを監視する契約委託者が、契約受託者の生成したデータを修正することのないように職務を分離する必要がある。
Quality monitoring 品質監視	Quality and performance monitoring may indicate incentive for data falsification (e.g. raw materials which marginally comply with specification on a frequent basis.	品質と性能を監視することで、データ改ざんの動機が存在することが分かる可能性がある。 (例えば、仕様にぎりぎり適合している原材料が頻繁に使用されている。)

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.	契約委託者は、契約受託者と協力して、顧客のすべての機密情報がコード化され、顧客が匿名化されるようにすべきである。これにより、契約委託者の拠点において、他の顧客に対する守秘義務を破ることなく、元となっている電子データ及びメタデータのレビューができるようになる。より多くのデータセットをレビューすることで、契約受託者のデータガバナンス方策をよりしっかりとアセスメントすることができる。また、これにより、データインテグリティの障害を示す指標 (例えば、同じデータセットが繰り返し現れる、データが予想される変化を示さない等) を見つけることができるようになる。
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及び正確性を確実にするために注意を払うべきである (第 8.11 章参照) 。契約者及びサプライチェーンの適格性評価〔結果〕を判断する際には、データインテグリティリスク及びトレーサビリティリスクの観点から「真正コピー」と「サマリ報告書」の差異を考慮する必要がある。

11. REGULATORY ACTIONS IN RESPONSE TO DATA INTEGRITY FINDINGS

11. データインテグリティに関する指摘事項に応じた規制措置

11.1 Deficiency references

11.1 欠陥があったときの参照先

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 GMP の基本であり、グッドデータマネジメントの要件は、現行の PIC/S Guides to GMP/GDP for Medicinal Products に組み込まれている。以下の表は、〔指摘事項の〕参照先となる既存の要件を示す。

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 帰属性	[4.20, c & f], [4.21, c & i], [4.29 point 5]	[5.43], [6.14], [6.18], [6.52]	[2], [12.1], [12.4], [15]	[4.2.4], [4.2.5]
Legible 判読性	[4.1], [4.2], [4.7], [4.8], [4.9], [4.10]	[6.11], [6.14], [6.15], [6.50]	[4.8], [7.1], [7.2] [8.1], [9], [10], [17]	[4.2.3], [4.2.9]
Contemporaneous 同時記録性	[4.8]	[6.14]	[12.4], [14]	[4.1], [4.2.9]
Original 原本性	[4.9], [4.27], [Paragraph "Record"]	[6.14], [6.15], [6.16]	[8.2], [9]	[4.2.5]
Accurate 正確性	[4.1], [6.17]	[5.40], [5.42], [5.45], [5.46], [5.47], [6.6]	[Paragraph "Principles"] [4.8], [5], [6], [7.2], [10], [11]	[4.2.3]
Complete 完全性	[4.8]	[6.16], [6.50], [6.60], [6.61]	[4.8], [7.1], [7.2], [9]	[4.2.3], [4.2.5]
Consistent 一貫性	[4.2]	[6.15], [6.50]	[4.8], [5]	[4.2.3]
Enduring 永続性	[4.1], [4.10]	[6.11], [6.12], [6.14]	[7.1], [17]	[4.2.6]

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:**
Available 可用性	[Paragraph "Principle"], [4.1]	[6.12], [6.15], [6.16]	[3.4], [7.1], [16], [17]	[4.2.1]

11.2 Classification of deficiencies

11.2 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を報告し、分類するときに一貫性を持たせるためのものであり、各査察当局機関が、その内部方針又は国の規制フレームワークに従って行動することを妨げるものではない。**
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、製品の品質に様々な影響を与える可能性がある。また、障害の広がり方は、一人の従業員の行動〔に限られるもの〕から、査察対象組織全体に蔓延するものまで様々である。
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".	PIC/S ガイダンス[12]は欠陥の分類に関して次のように記載している： 「重大な欠陥とは、ヒトや動物の患者に有害な製品、又は食品を産み出す動物に有害な残留物になりえる製品の製造に使われた慣行・プロセス、又はそういった製品を製造する重大なリスクを引き起こしかねない慣行・プロセスのことである。製造業者が製品やデータの不正行為・不当表示・改ざんに関与していることが確認された場合にも重大な欠陥となる。」

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

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.	不正行為・不当表示・改ざんに関する欠陥を「重大」と分類しているが、データインテグリティの欠陥は以下にも関連すると考えられる： • バッドプラクティスに起因するデータインテグリティの障害。 • 求められているデータコントロール方策がないため、(実際の欠陥の証拠はないが)〔データインテグリティ〕障害を引き起こす機会がある。
11.2.4	In these cases, it may be appropriate to assign classification of deficiencies by taking into account the following (indicative list only):	このような場合には、以下の点を考慮して欠陥の分類を行うことが適切であると考えられる (あくまでも参考例) ：
	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.	**患者の健康への実際又は潜在的なリスクのある製品に影響がある：Critical な欠陥：** • 製品が、リリース時又は保存期間中に、製造販売承認された仕様に適合していない。 • QC テスト〔結果〕・重要な製品・プロセスパラメータを報告する際に、実際の規格外の結果ではなく「望ましい」結果を報告している。 • 広範囲にわたってデータが不当表示・改ざんされている。上級管理職が知っていたかどうか、又は関与していたかどうかにかかわらず、これにより医薬品品質システムの信頼性が決定的に損なわれ、当該拠点で製造されている、又は取り扱われている医薬品の品質及び安全性に対する信頼性が完全に失われる。
	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	**患者の健康へのリスクがない製品に影響する：Major な欠陥** • 誤ったデータが報告されている。例えば、元の結果は「仕様通り」だが、より好ましい傾向を示すように変更した。 • QC テスト〔結果〕・重要な製品・プロセスパラメータに関連しないデータを報告する際に、実際の規格外の結果ではな

	parameters. • Failures arising from poorly designed data capture systems (e.g. using scraps of paper to record info for later transcription).	く「望ましい」結果を報告している。 • データ収集システムの設計不良による失敗 (例：後で転写するために情報を記録するために紙の切れ端を使っている。)
	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.	**製品に影響がないものの、中程度の障害の証拠がある：Major な欠陥：** • バッドプラクティスや不適切に設計されたシステムにより、限られた機能領域 (QA、製造、QC 等) においてデータインテグリティの問題やトレーサビリティの喪失が発生する可能性がある。それぞれ単独では、製品の品質に直接的な影響はない。
	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.	**製品に影響はなく、障害の証拠は限定的である：その他の欠陥：** • バッドプラクティスや不適切な設計されたシステムにより、データインテグリティ問題が生じたり、単独の領域でトレーサビリティが失われたりする可能性がある。 • 他の点では問題のないシステムにおける限定的な欠陥。例えば、重要でないデータが個人によって不正操作される等。
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.	全社的な障害なのか、範囲や影響が限定的な障害なのかをしっかりとアセスメントするためには、重要な要素 (データガバナンスプロセス、適合したデータ記録を行うようにするためのシステム設計、監査証跡の利用と検証、IT ユーザーアクセス等) の適切さについて全体像を把握することが重要である。
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・緩和する因子) が最終的な分類又は規制措置の〔決定〕に影響することもある。欠陥の分類及び不適合の当局内報告に関するガイダンスは、PIC/S Guidance on the classification of deficiencies PI 040 を参照のこと。

12. REMEDIATION OF DATA INTEGRITY FAILURES

12. データインテグリティ障害の修復

12.1 Responding to Significant Data Integrity issues

12.1 データインテグリティに関する重大な問題への対応

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:	第一に考慮すべきことは、特定された当面のデータインテグリティ問題を解決するとともに、その問題に関連するリスクをアセスメントすることである。問題を起こした会社は〔当局への〕回答において、修復計画において、実施するアクションの概要を記載すべきである。回答には以下を含むべきある：
12.1.1.1	A comprehensive investigation into the extent of the inaccuracies in data records and reporting, to include: • A detailed investigation protocol and methodology; a summary of all laboratories, manufacturing operations, 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	データ記録・報告の不正確さの程度に関する包括的な調査。以下を含む： • 詳細な調査プロトコルと調査方法。アセスメント対象となるすべてのラボ、製造業務、製品及びシステムの概要。規制対象ユーザーが、業務の一部を〔調査〕対象から除外することを提案する場合、その合理的な理由[13]。 • 現従業員、及び可能かつ適切な場合は元従業員へのインタビュー。これはデータの不正確さの性質・範囲・根本原因を特定するために行う。インタビューは、適格な第三者が行ってもよい。 • 施設におけるデータインテグリティの欠陥の程度についてのアセスメント。漏れ、変更、削除、記録の破壊、記録の同時記録性のない完成、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、特定のバッチ) 及びインシデントの期間 (時間の区切り方は合理的であること) の決定。 • データインテグリティ違反が発生した

[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.
[13] 調査の範囲には、影響を受ける可能性のあるすべての施設・拠点・部門を含む全社レベルでのデータインテグリティの程度についてのアセスメントを含める必要がある。

	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.	業務のすべての部分についての説明。多国籍会社や複数の拠点で操業する会社の場合は、グローバルな是正措置をさらに検討すべきである。 • 調査プロトコルに従った、データインテグリティの欠陥の性質についての包括的な回顧的評価、及び是正・予防措置のもととなる根本原因又は根本原因となる可能性の最も高いものの特定。違反の可能性が指摘された分野において専門技術を有する適格な第三者コンサルタントのサービスが必要となるかもしれない。 • 観察された障害が、関係する物質・医薬品・製品の品質に及ぼす潜在的な影響についてのリスクアセスメント。このアセスメントには、次の分析が含まれるべきである：データインテグリティ違反のあった製品がリリース/流通することにより引き起こされる患者への潜在的なリスク、操業を続けていることにより引き起こされるリスク、(製品の登録申請書類に関連するデータ等の)規制当局に提出されたデータのインテグリティへの影響。
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	データインテグリティの脆弱性に対処するための是正・予防措置、及びそのための実施期間。以下を含む： • 患者を保護し、医薬品の品質を確実にするためのアクションを記述した暫定措置。例えば、顧客への通知、製品の回収、追加試験の実施、安定性を確保するための安定性プログラムへのロットの追加、医薬品申請に係るアクション、苦情モニタリングの強化等。暫定措置の有効性を監視するとともに、残存リスクを上級管理職に伝え、常にレビューすべきである。 • データインテグリティを確実に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、管理監督、人的資源 (トレーニング、人員配置の改善等) に対する改善努力及び強化を

	integrity. Where long term measures are identified interim measures should be implemented to mitigate risks.	記述した長期的措置。長期的措置が特定された場合、リスクを軽減するために暫定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.	実施したアクションにより問題がなくなったことを監視するために実施する 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.	査察官は可能な限り当該会社の上級代表者と会い、特定された欠陥の性質を伝え、包括的な調査、問題の完全な開示、及び迅速な解決の約束を、書面で確認すべきである。管理戦略が規制当局に提出されるべきであり、そこにはグローバルな是正・予防措置計画の詳細が含まれる。この戦略には以下が含まれる： • データインテグリティ違反の根本原因の包括的な説明。説明には、現在のアクション計画の範囲と深さが、調査結果とリスクアセスメント結果に応じたものであるという証拠を含む。また、データインテグリティ違反に関与した個人が、GMP/GDP 関連又は医薬品申請データへの影響力を持ち続けるかどうかを示す必要がある。 • 規制対象ユーザーが、生成されるすべてのデータ (分析データ、製造記録、管轄当局に提出・提示されるすべてのデータを含む) について、どのように「ALCOA+」【訳注】属性 (第 7.4 章参照) 〔への適合〕を確実にするつもりなのかを説明する詳細な是正措置計画。 【訳注：原文は「ALOCA+」であるが「ALCOA+」の誤りと思われる。】
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、査察で特定された重大なデータインテグリティ問題を管理するための方針を実行し、データインテグリティ違反に関連するリスクを管理し、封じ込むようにすべきである。

12.2 Indicators of improvement

12.2 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問題に対処するために講じられた措置の有効性を検証するために、オンサイト査察が推奨される。〔それができない場合、〕リスクマネジメントの原則に基づいて、効果的な修復策が講じられていることが検証できる代替アプローチを検討してもよい。改善の指標の例を以下に示す：
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;	特定された問題を徹底的かつオープンに評価し、タイムリーに効果的な是正・予防措置を実施した証拠。組織レベルでの適切な是正・予防措置の実施を含む。
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;	顧客及び他の規制当局との間での問題についてのオープンなコミュニケーションの証拠。調査及び修復の段階を通して、透明性のあるコミュニケーションが維持されるべきである。規制当局側は、詳細な調査を行ったことにより、さらなるデータインテグリティ障害が報告される可能性があることを認識すべきである。これらの連絡があったときの追加的な対応は、継続的な報告を促すためにも、公衆衛生上のリスクに見合ったものとすべきである。
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;	データインテグリティに関する期待事項を組織全体に伝え、〔社員が〕潜在的な問題や改善の機会をオープンに報告するプロセスを取り入れ、奨励している証拠。
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;	規制対象ユーザーは、データの不正操作に対する電子システムの脆弱性を適切に評価し、フォローアップアクションによりすべての違反が完全に解決されたことを確実にすべきである。この評価には、関連する専門技術を有する適格な第三者コンサルタントのサービスが必要となるかもしれない。
12.2.1.5	Implementation of data integrity policies in line with the principles of this guide;	本書の原則に沿ったデータインテグリティポリシーの実施。

12.2.1.6	Implementation of routine data verification practices.	日常的なデータ検証作業の実施。

13. Glossary

13. 用語集

Archiving Long term, permanent retention of completed data and relevant metadata in its final form for the purposes of reconstruction of the process or activity.	**アーカイビング** プロセス又は活動の再現を目的とした、完成したデータ及び関連メタデータの最終的な形での長期的かつ恒久的な保管。
Audit Trail 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.	**監査証跡** GMP/GDP 監査証跡とは、GMP/GDP に不可欠な情報 (例えば、GMP/GDP 関連データの作成、変更、削除等) を記録したメタデータであり、GMP/GDP 活動の再現を可能にするものである。
Back-up A copy of current (editable) data, metadata and system configuration settings (e.g. variable settings which relate to an analytical run) maintained for the purpose of disaster recovery.	**バックアップ** 災害復旧の目的で維持される、現在の (編集可能な) データ、メタデータ、システム構成設定 (例：分析の実行に関連する変数設定) のコピー。
Computerised system A system including the input of data, electronic processing and the output of information to be used either for reporting or automatic control.	**コンピュータ化システム** データの入力、電子的な処理、報告又は自動制御のために使用される情報の出力を含むシステム。
Data Facts, figures and statistics collected together for reference or analysis.	**データ** 参照や分析のために集められた事実、数字、統計。
Data Flow Map A graphical representation of the "flow" of data through an information system	**データフローマップ** 情報システムにおけるデータの「流れ」を図式化したもの
Data Governance The sum total of arrangements to ensure that data,	**データガバナンス** データの生成されるフォーマットにかかわら

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.	ず、データのライフサイクルを通して記録の完全性、一貫性、正確性を確実にするために、データを記録・処理・保管・使用するための準備事項の総体。
Data Integrity 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** データが完全であり、一貫性があり、正確であり、信用でき、信頼でき、かつデータのこれらの特性がデータのライフサイクルを通して維持される程度。 データは安全な方法で、帰属性を持ち、判読でき、同時に記録され、原本 (又は真正コピー) であり、正確となるように、収集・維持されるべきである。データインテグリティを確保するためには、健全な科学的原則と GdocPs に適合した、適切な品質管理システム及びリスクマネジメントシステムが必要である。データは ALCOA+の原則に適合する必要がある。
Data Lifecycle All phases in the life of the data (including raw data) from initial generation and recording through processing (including transformation or migration), use, data retention, archive / retrieval and destruction.	**データライフサイクル** 最初の生成及び記録から、処理 (変換又は移行を含む) 、利用、データ保管、アーカイブ/検索、破棄に至るまでの、データ (生データを含む) の一生におけるすべての段階。
Data Quality The assurance that data produced is exactly what was intended to be produced and fit for its intended purpose. This incorporates ALCOA + principles.[14]	**データ品質** 生成されたデータが正しく意図された通りのものであり、意図された目的に合っていることの保証。これには ALCOA +の原則が組み込まれる[14]。
Data Ownership 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.	**データオーナーシップ** データのコントロールに関する責任を特定のプロセスのオーナーに割り当てること。会社は、システム及び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導入すべきである。

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

Dynamic Record Records, such as electronic records, that allow an interactive relationship between the user and the record content.[13]	**動的な記録** 電子記録等の記録で、ユーザーと記録内容との間で対話型に操作できるもの [13]。
Exception Report A validated search tool that identifies and documents predetermined 'abnormal' data or actions, which require further attention or investigation by the data reviewer.	**例外報告書** バリデートされた検索ツール。事前に設定された「異常」データやアクションを特定し、記録することで、データレビュー者に注意・調査を促す。
Good Documentation Practices (GdocP) Those measures that collectively and individually ensure documentation, whether paper or electronic, meet data management and integrity principles, e.g. ALCOA+.	**グッドドキュメンテーションプラクティス (GdocP)** 紙か電子かを問わず、文書がデータマネジメント及びデータインテグリティの原則を満たしていることを集合的かつ個別に確実にするための方策 (例：ALCOA+) 。
Hybrid Systems 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.	**ハイブリッドシステム** データを管理し、コントロールするためのシステムであり、一般的に、電子データを生成する電子システムと、それを補足する定義された手作業システム (一般的に紙ベースの記録を生成する) により構成される。したがって、ハイブリッドシステムから得られる完全なデータセットは、電子データと紙ベースのデータの両方で構成される。ハイブリッドシステムが正しく機能するためには、両方のサブシステムを効果的に管理する必要がある。
Master Document An original approved document from which controlled copies for distribution or use can be made.	**マスタードキュメント** 承認された文書の原本で、それをもとに配布・使用のための管理コピーを作成できる。
Metadata 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).	**メタデータ** 他のデータの属性を説明し、文脈や意味を提供するファイル内のデータ。 一般的には、データの構造、データ要素、相互関係、及びその他のデータ特性を記述するデータである (例えば監査証跡)。メタデータは、データを個人 (又は自動生成された場合はもともと

Metadata form an integral part of the original record. Without the context provided by metadata the data has no meaning.	のデータソース) に帰属させることもできる。メタデータは原本記録の一部である。メタデータの提供する文脈無しではデータは意味を持たない。
Quality Unit The department within the regulated entity responsible for oversight of quality including in particular the design, effective implementation, monitoring and maintenance of the Pharmaceutical Quality System.	**品質部門** 規制対象会社の中で、品質の監督に責任を持つ部門であり、特に医薬品品質システムの設計、効果的な実施、監視、維持等を行う。
Raw Data 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** 生データとは、紙に記録されているか電子的に記録されているかを問わず、情報を最初に取得した記録 (データ) と定義される。動的な状態で最初に取得された情報は、その状態を保ったまま利用可能とする必要がある [14]。
Static Record 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]	**静的な記録** 紙や電子記録等の記録形式で、固定され、ユーザーと記録内容との対話型操作が、ほとんど又は全くできないもの。[14]
Supply Chain 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.	**サプライチェーン** 〔医薬品が〕製造されてから販売又は使用されるまでの流通過程において、医薬品の品質が確保されることを確実にするための、製造の各拠点及び卸売・流通の各拠点の間の取り決めの総体。
System Administrator A person who manages the operation of a computerised system or particular electronic communication service.	**システム管理者** コンピュータ化システムや特定の電子通信サービスの運用を管理する者。

14. REVISION HISTORY

14. 改訂履歴

Date	Version Number	Reasons for revision

Footnote 8

脚注 8

The use of scribes (second person) to record activity on behalf of another operator should be considered 'exceptional', and only take place where: • The act of recording places the product or activity at risk e.g. documenting line interventions by sterile operators. • To accommodate cultural or staff literacy / language limitations, for instance where an activity is performed by an operator, but witnessed and recorded by a scribe. In these cases, bilingual or controlled translations of documents into local languages and dialect are advised. In both situations, the scribe recording 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.	他のオペレーターに代わって活動を記録する記録者 (第二者) の使用は、「例外的」と見なされ、以下の場合に限定すべきである： • 記録することにより、製品や活動が危険にさらされる。例えば、無菌オペレーターによるライン介入の記録。 • 文化的またはスタッフのリテラシー/言語の制限に対応するために、例えば、ある活動がオペレーターによって実行され、記録者が立ち会い、記録する場合等。このような場合には、文書を二か国語併記にするか、ローカル言語・方言へコントロールされた翻訳を行うことが推奨される。 いずれの状況においても、記録者による記録は、実施されているタスクと同時に行われるべきであり、観察されたタスクを実施する者及び記録を完成する者の両方を特定すべきである。観察されるタスクを実施する者は、可能な限り記録に連署すべきであるが、この連署 のステップは後で行ってもよい。記録者が文書を完成させるためのプロセスを、承認された手順書に記述すべきであり、そこには、プロセスが適用される活動及び関連するリスクのアセスメント〔結果〕を記載する。