データマネジメント（いわゆるデータインテグリティ：DI）の PIC/S ガイドライン最終版が 2021 年 7 月 1 日に発行されました。適切な訳はその後出されるかと思います。早く知る意味で、自動翻訳をかけ、意味の分かりにくい箇所は意訳してわかりやすくしました。この和訳でおおよその理解はできるかと思います。不明な箇所は原文をご参照ください。

このガイドラインは実際にデータを扱う現場だけの問題だけでなく、上級経営者がデータガバナンスの視点から理解することや実践すべきことまで言及されています。英文が 60 数頁と多いですが、一度目を通すことで DI/データガバナンスのことを正しく理解する一助になります。末端で GMP 不備が起きるか起きないかは、上級経営者の考え方＆実践に大きく左右されます。日本電産創業者　永守重信氏の言葉に「会社がおかしくなるのは経営者の考え方が間違っているからである」があります。このガイドラインは GMP＆GDP のデータを扱う現場だけでなく、上級経営者にも役立つものです。

改正 GMP 省令は 2021 年 8 月 1 日から施行されます。いくつかの新しい要求事項があります。その一つに DI 対応が盛り込まれています。日本では欧米のような DI のガイドライン発行は今のところ予定されていません。PIC/S GMP 加盟国の日本も PIC/S GMP ガイドライン実践する上においても、このガイドラインを参考に少しでも早くシステム構築と実践を行うことがよりよい結果を生み出します。具体的な項目については、FDA の DI に関する指摘事項を“過去問”として位置付けて、未対応で容易にできることは早めに対応していくことがよりよい DI 対応構築につながると思います。それが昨今起きている GMP 不正防止の一助にもなります。また、このガイドラインを読み合わせすることにより、DI についての理解も促進されると思います。この和訳がそれらに少しでも貢献できると嬉しく思います。不明な点は原文を併記していますので、ご確認お願いします。

（イギリス英語の単語は一部米国語の単語に変えて自動翻訳をかけました。また筆者の知らない言葉についてはその意味を付記しています）

PIC/S GUIDANCE　1 July 2021

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

https://picscheme.org/docview/4234

PIC/S ガイダンス

規制された GMP/GDP 環境における規制された GMP/GDP 環境でのデータ管理と整合性

TABLE OF CONTENTS

本文の目次

1 DOCUMENT HISTORY

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

1 文書の歴史

委員会による PI 041-1 の採択 2021 年 6 月 1 日
PI 041-1 の発効 2021 年 7 月 1 日

2 INTRODUCTION

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

2 序論

2.1 PIC/S 参加機関は、医薬品製造工程管理（GMP）及び医薬品流通工程管理（GDP）の原則を遵守しているかどうかを判断するために、原薬及び医薬品の製造業者及び流通業者に対して定期的に査察を行う。これらの検査は通常、現場で行われるが、証拠書類の遠隔評価やオフサイトで行われることもあり、その場合にはデータの遠隔レビュー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.

2.2 これらの検査プロセスの有効性は、検査官に提供される証拠の信頼性、そして最終的には基礎となるデータの完全性によって決定される。検査員が提示された証拠や記録の正確性と完全性を判断し、十分に信頼できることが、検査プロセスにとって重要である。

2.3 Data management refers to all those activities performed during the handling of data including but not limited to data policy, documentation, quality and security. Good data management practices influence the quality of all data generated and recorded by a manufacturer. These practices should ensure that data is attributable, legible, contemporaneous, original, accurate, complete, consistent, enduring, and available. While the main focus of this document is in relation to GMP/GDP expectations, the principles herein should also be considered in the wider context of good data management such as data included in the registration dossier based on which API and drug product control strategies and specifications are set.

2.3 データマネジメントとは、データポリシー、文書化、品質およびセキュリティを含むがこれに限定されない、データを取り扱う際に行われるすべての活動をいう。優れたデータマネジメントの実践は、製造者が生成・記録するすべてのデータの品質に影響を与える。これらの実践により、データの帰属性、可読性、同時期性、原本性、正確性、完全性、一貫性、永続性、利用可能性が確保されなければならない。この文書の主な焦点は、GMP/GDP の期待に関連するものであるが、ここに記載されている原則は、より広い範囲で考慮されるべきである。ここに記載されている原則は、原薬および製剤の管理戦略および仕様が設定された登録書類に含まれるデータなど、優れたデータ管理のより広い文脈において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.

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

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

2.5 データの完全性とは、「データが完全であり、一貫性があり、正確であり、信頼性があり、データのこれらの特性がデータのライフサイクルを通じて維持される度合い」と定義される。これは、医薬品が要求された品質であることを確実にする、効果的な医薬品品質システムの基本要件である。データの整合性に欠ける行為や脆弱性は、記録や証拠の質を低下させ、最終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.

2.6 データ管理および完全性に関する優れた実践の責任は、検査を受ける製造業者または販売業者にある。データ管理システムに潜在的な脆弱性がないかどうかを評価し、データの完全性を確実に維持するために優れたデータガバナンスを設計・実施するための手段を講じる全責任と義務がある。

3 PURPOSE

3.1 This document was written with the aim of:

3 目的

3.1 本文書は、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.

3.1.1 優れたデータ管理と査察の実施に関連する GMP/GDP 要求事項の解釈について、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, complete and reliable as described in PIC/S Guides for GMP2 and GDP3 to be implemented in the context of modern industry practices and globalized supply chains.

3.1.2 PIC/S Guide for GMP2 及び GDP3 に記載されている、データの有効性、完全性、信頼性に関する既存の要求事項を、現代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施できるようにする、リスクベースの管理戦略に関する統合的で例示的なガイダン

スを提供する。

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

3.1.3 GMP/GDP 査察の日常的な計画と実施に優れたデータ管理要素を効果的に導入することを促進し、GMP/GDP 査察を調和させるためのツールを提供し、データの完全性に関する期待に関して査察の質を確保する。

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

3.2 この指針は、補佐資料などの検査機関のリソースと合わせて、検査員が検査時間を最適に活用し、検査中にデータインテグリティ要素を最適に評価できるようにするものである。

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

3.3 ここに記載されているガイダンスは、優れたデータ管理方法に関連するリスクベースの検査を計画する際に、検査官の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.

3.4 優れた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いる。したがって、本ガイドは、規制対象となる企業に新たな規制上の負担を課すことを意図したものではなく、むしろ、現在の業界のデータ管理慣行に関連する既存の GMP/GDP 要求事項の解釈に関するガイダンスを提供することを意図したものである。

3.5 The principles of data management and integrity apply equally to paper-based, computerized and hybrid systems and should not place any restraint upon the development

or adoption of new concepts or technologies. In accordance with ICH Q10 principles, this guide should facilitate the adoption of innovative technologies through continual improvement.

3.5 データ管理と完全性の原則は、紙ベースのシステム、コンピュータ化されたシステム、およびハイブリッドシステムに等しく適用され、新しい概念や技術の開発や採用を制限するものであってはならない。ICH Q10 の原則に従い、本ガイドは継続的な改善を通じて革新的な技術の採用を促進すべきである。

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.

3.6 「医薬品品質システム」という用語は、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示すために、この文書で主に使用される。医薬品品質システム」という用語は、主に GMP 規制対象企業で使用されているが、本ガイダンスの目的上、GDP 規制対象企業で使用されている「品質システム」という用語と互換性があるとみなされるべきである。

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

3.7 本ガイドは、法律に基づく義務や強制力はない。本ガイドは、医薬品及び活性物質（原薬）の製造業者及び販売業者のデータインテグリティ要件に関する国内法を制限したり、置き換えたりすることを意図していない。データインテグリティの不備は、国内法または PIC/S GMP もしくは GDP ガイダンスの関連パラグラフを参照する必要がある。

4 SCOPE
4 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.

4.1 本指針は、製造（GMP）及び流通（GDP）活動を行っているサイトの現場検査に適用するために作成された。本ガイドの原則は、製品のライフサイクルのすべての段階に適用される。本ガイドは、査察の際に考慮すべき分野を網羅していないリストと考えるべきである。

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

4.2 本指針は、製造（GMP）及び流通（GDP）活動を行っているサイトの遠隔（デスクトップ） 検査にも適用されるが、これはデータガバナンスシステムの評価に限定されるものである。現場での評価は、通常、データの検証及び業務上の手順遵守の証明のために必要である。

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

4.3 本書は上記の範囲で作成されているが、本書に記載されている優れたデータマネジメントの実践に関する多くの原則は、規制されている医薬品およびヘルスケア産業の他の分野にも適用できる。

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.

4.4 本ガイドは、法廷の専門知識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の「理由のある」検査について、特定のガイダンスを提供することを意図していない。

5 DATA GOVERNANCE SYSTEM

5.1 What is data governance?

5 データガバナンスシステム

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, prioritize 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.

5.1.1 データガバナンスとは、データの完全性を保証するための取り決めの全体である。これらの取り決めは、データが生成され、記録され、処理され、保持され、検索され、使用されるプロセス、フォーマット、または技術にかかわらず、データのライフサイクルを通じて、帰属する、読みやすい、同時期の、オリジナルの、正確な、完全な、一貫した、永続的な、利用可能な記録を保証するものである。データガバナンスシステムを導入するための法律上の要求はないかもしれないが、このシステムを構築することにより、製造業者はデータインテグリティリスクマネジメント活動を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場合は、データインテグリティシステムが調整されていないことを意味し、管理手段にギャップが生じる可能性がある。

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

5.1.2 データ・ライフサイクルとは、データがどのように生成され、処理され、報告され、確認され、意思決定に使用され、保存され、最終的に保存期間の終了時に廃棄されるかを 意味する。製品またはプロセスに関連するデータは、ライフサイクルの中で様々な境界を越えることがある。これには、紙ベースのシステムとコンピュータ化されたシステムとの間でのデータ転送や、異なる組織の境界、内部（製造、QC、QA 間など）と外部（サービスプロ

バイダー間など）の両方が含まれる。サービスプロバイダーや契約書の発行者と受諾者の間など)。

5.2 Data governance systems

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

5.2 データガバナンスシステム

5.2.1 データガバナンスシステムは、PIC/S GMP/GDP に記載されている医薬品品質システムに不可欠である。データガバナンスシステムは、ライフサイクルを通じたデータ所有権に対応し、情報の意図的・非意図的な変更及び削除の管理を含むデータインテグリティの原則に準拠するためのプロセス及びシステムの設計、運用及び監視を考慮する必要がある。

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

5.2.2 データガバナンスシステムは、適切に設計されたシステムの組み込み、技術およびデータセキュリティ対策の使用、ならびにデータの管理および完全性が効果的に制御されることを確実にするための特定の 専門知識に依存する。規制対象企業は、データガバナンスシステムの設計、開発、運用および監視において、システ ムの複雑さ、運用、およびデータの重要性とリスクに見合った適切なリソースが利用可能であり、 適用されることを確実にするための手段を講じるべきである。

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

・ Organizational

o procedures, e.g. instructions for completion of records and retention of completed records;

o training of staff and documented authorization for data generation and approval;

o data governance system design, considering how data is generated, recorded, processed,

retained and used, and risks or vulnerabilities are controlled effectively;
o routine (e.g. daily, batch- or activity-related) data verification;
o periodic surveillance, e.g. self-inspection processes seek to verify the effectiveness of the data governance system; or
o the use of personnel with expertise in data management and integrity, including expertise in data security measures.
・ Technical
o computerized system validation, qualification and control;
o automation; or
o the use of technologies that provide greater controls for data management and integrity.

5.2.3 データガバナンスシステムは、品質リスクマネジメントの原則に見合った、データライフサイクルに関する統制を確保するものとする。これらの統制は以下の通りである。
- 組織的なもの
o 手順（例：記録の記入方法や記入済み記録の保管方法）。
o スタッフのトレーニング、及びデータの生成と承認に関する文書化された権限。
o データがどのように生成、記録、処理、保持および使用され、リスクまたは脆弱性が効果的に管理されているかを考慮した、データガバナンスシステムの設計。
o ルーチン（例：毎日、バッチまたはアクティビティ関連）のデータ検証。
o 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などの定期的な監視。
o データセキュリティ対策の専門知識を含む、データ管理および完全性に関する専門知識を有する人材の活用。
- テクニカル
o コンピュータ化されたシステムの妥当性確認、適格性確認、および管理。
o 自動化、または
o データ管理および完全性のためのより高度な管理を提供する技術の使用。

5.2.4 An effective data governance system will demonstrate Senior management's understanding and commitment to effective data governance practices including the necessity for a combination of appropriate organizational 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 organization in a manner which ensures empowerment to report failures and opportunities for improvement. This reduces the incentive to falsify, alter or delete data.

5.2.4 効果的なデータガバナンスシステムは、適切な組織文化及び行動（セクション 6）の組み合わせ、並びにデータの重要性、データリスク及びデータライフサイクルの理解の必要性を含む、効果的なデータガバナンスの実践に対する上級管理者の理解及びコミットメントを示す。また、失敗を報告する権限を確実に与える方法で、組織内のすべてのレベルの担当者に期待事項を伝えている証拠がなければならない。また、組織内のすべてのレベルの担当者に期待事項が伝達されている証拠があるべきである。これにより、データを改ざん、変更、または削除する動機が減少する。

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

5.2.5 データガバナンスに関する組織の取り決めは、医薬品品質システムの中で文書化され、定期的に見直されるものとする。

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

5.3 データガバナンスに対するリスクマネジメントアプローチ
5.3.1 上級管理者は、ICH Q9 の原則を用いて、データの完全性に対する潜在的リスクを最小化するためのシステム及び手順の実施、並びに残存リスクの特定に責任を負う。契約締結者は、ベンダー保証プログラムの一環として、契約締結者のデータ管理方針及び管理戦略のレビューを行うべきである。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、受入契約者が提供するサービスの重要性に基づいて決定されるべきである。

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.

5.3.2 データガバナンスに割り当てられる労力及び資源は、製品品質に対するリスクに見合うものでなければならず、また、他の品質資源の需要とのバランスをとるべきである。GMP/GDP の原則に従って規制されているすべての事業者（製造業者、分析機関、輸入業者、卸売り 販売業者を含む）は、データ品質のリスクに基づいて許容可能な管理状態を提供し、裏付けとなる 根拠を文書化したシステムを設計し、運用するべきである。

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 prioritization are required, residual data integrity risk should be communicated to senior management, and kept under review. Reverting from automated and computerized systems to paper-based systems will not remove the need for data governance. Such retrograde approaches are likely to increase administrative burden and data risk, and prevent the continuous improvement initiatives referred to in paragraph 3.5.

5.3.3 望ましい管理状態を達成するために長期的な対策が特定された場合、リスクを軽減するために暫定的な対策を実施し、その有効性を監視するものとする。暫定措置またはリスクの優先順位付けが必要な場合は、残存するデータインテグリティリスクを上級管理者に伝え、常に見直しを行うものとする。自動化、コンピュータ化されたシステムを紙ベースのシステムに戻しても、データガバナンスの必要性がなくなるわけではない。このような逆行するアプローチは、管理負担とデータリスクを増大させ、3.5 項で言及されている継続的な改善イニシアチブを妨げる可能性が高い。

5.3.4 Not all data or processing steps have the same importance to product quality and patient safety. Risk management should be utilized 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.

5.3.4 すべてのデータまたは処理ステップが、製品の品質および患者の安全性に対して同じ

重要性を持つわけではない。各データ／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管理アプローチでは、以下を考慮する。
- データの重要性（意思決定及び製品品質への影響）及び
- データのリスク（データの変更及び削除の機会、メーカーの定期的なレビュープロセスによる変更の検出及び可視性の可能性）。
これらの情報から、リスクに応じた管理策を実施することができる。本ガイダンスの後続の章では、リスクマネジメント手法に言及しているが、「リスク」とは、 データリスクとデータ・クリティカルの概念を組み合わせたものである。

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

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

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

5.4 データの重要性
5.4.1 データが影響を与える意思決定は、重要性が異なる場合があり、意思決定に対するデータの影響度も異なる場合がある。データの重要性について考慮すべき点は以下の通りである。

- そのデータはどの意思決定に影響を与えるか？
例えば、バッチリリースの決定を行う場合、重要な品質属性への準拠を決定するデータは、通常、倉庫の清掃記録よりも重要である。

- 製品の品質や安全性に対するデータの影響は何か？
例：経口錠剤の場合、原薬のアッセイデータは、一般的に錠剤の摩損度データよりも製品の品質や安全性に大きな影響を与える。

5.5 Data risk

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

5.5 データリスク
5.5.1 データの完全性の要件はすべての GMP/GDP データに関連するが、データの重要性の評価は、組織がデータガバナンスの取り組みに優先順位をつけるのに役立つ。この優先順位付けの根拠は、品質リスク管理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 unauthorized activity, and increase visibility / detectability can be used as risk mitigating actions.

5.5.2 データ・リスク評価は、不本意な変更、削除、喪失（偶発的またはセキュリティ障害による）または再作成もしくは意図的な改竄に対するデータの脆弱性、およびそのような行為の発見の可能性を考慮するものとする。また、災害時に完全かつタイムリーにデータを復旧させることも考慮しなければならない。不正行為を防止し 未承認の活動を防止し、可視性／検出性を高める管理策は、リスクを軽減するための措置として使用することができる。

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

5.5.3 データ障害のリスクを増大させる要因の例としては、複雑なプロセス、一貫性のないプロセス、自由な主観的な結果を伴うプロセスなどが挙げられる。一貫性があり、明確に定義され、客観的なタスクを持つ単純なプロセスは、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);
・ 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.

5.5.4 リスクアセスメントは、単に情報技術（IT）システムの機能性や複雑性を考慮するのではなく、ビジネスプロセス（製造、QC など）に焦点を当て、データフローやデータの生成・処理方法を評価するものとする。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：多段階プロセス、プロセスまたはシステム間のデータ転送、複雑なデータ処理)。
- データの生成、処理、保存、アーカイブの方法、およびデータの品質と整合性を保証する能力。
- 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、低分子化学に比べてより高度な変動性を示す可能性がある)。
- 自動化の程度／人間の介入
- 結果の主観性（すなわち、プロセスが自由であるか、明確に定義されているか)。
- 電子システムのデータと手動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の取得時間の間に明らかな不一致がある場合)、および
- システムまたはソフトウェアに組み込まれた固有のデータインテグリティコントロール。

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

5.5.5 コンピュータ化されたシステムでは、IT システムとの手動によるインターフェース

をリスクアセス メントプロセスにおいて考慮するものとする。コンピュータ化されたシステムのバリデーションを単独で実施した場合、特に、ユーザがバリデーションされたシステムからのデータの報告に影響を与えることができる場合や、システムのバリデーションが本文書の第 9 章に概説されている基本的な要求事項に対応していない場合には、データインテグリティのリスクが低下しない可能性がある。完全に自動化され検証されたプロセスと、人の介入を許さない、または人の介入を最小限に抑える構成は、データインテグリティリスクを低下させる設計であるため望ましい。技術的な理由で統合された制御が不可能な場合は、適切な手続き的制御を導入し、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 organizational understanding and acceptance of residual risk, which prioritises actions. An organization which believes that there is 'no risk' of data integrity failure is unlikely to have made an adequate assessment of inherent risks in the data lifecycle. The approach to assessment of data lifecycle, criticality and risk should therefore be examined in detail. This may indicate potential failure modes which can be investigated during an inspection.

5.5.6 査察員は、統制及びレビューの手順が望ましい結果を効果的に達成しているかどうかを判断するために、批判的思考スキルを使用するものとする。データガバナンスの成熟度を示す指標は、残留リスクに対する組織の理解と受容であり、これによって行動の優先順位が決まる。データの完全性が損なわれる「リスクはない」と信じている組織は、データのライフサイクルに内在するリスクを適切に評価していない可能性が高い。したがって、データのライフサイクル、重要性及びリスクの評価に対するアプローチを詳細に検討する必要がある。これにより、査察期間中に調査可能な潜在的な故障モードが示される可能性がある。

5.6 Data governance system review

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

5.6 データガバナンスシステムのレビュー

5.6.1 データインテグリティコントロール手段の有効性は、自己点検（内部監査）またはその他の定期的なレビュープロセスの一環として定期的に評価されるものとする。これにより、データのライフサイクルに関する統制が意図したとおりに機能していることを確認すべきである。

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 focused 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 computerized system logs / audit trails to ensure that information of relevance to GMP/GDP activity is reported accurately. This is relevant to situations where routine computerized system data is reviewed manually or by a validated 'exception report'4.
・ A review of quality system metrics (i.e. trending) that may also be indicators of data governance effectiveness.

5.6.2 日常的なデータ検証チェック（例：毎日、バッチまたは活動に関連したもの）に加えて、自己点検活動は以下のような管理手段のより広範な見直しに拡大するものとする。
- 患者を保護するという観点から、優れたデータマネジメントの実践を従業員が継続的に理解しているかどうか、また、品質と問題のオープンな報告に重点を置いた作業環境の維持を確保しているかどうかの確認（例えば、優れたデータマネジメントの原則と期待に関する継続的なトレーニングの見直しなど）。
- 報告されたデータ/結果が生データと一致しているかどうかを確認すること。これは、ルーチンのデータ検証チェックに含まれていないデータ（リスクに基づいて正当化される場合）や、ルーチンプロセスの継続的な有効性を確保するために以前に検証されたデータのサンプルをレビューすることができる。
- GMP/GDP 活動に関連する情報が正確に報告されていることを確認するために、コンピュータシステムのログ/監査証跡のリスクベースのサンプル。これは、ルーチンのコンピュータ化されたシステムのデータが手動でレビューされている場合や、検証された「例外報告書」によってレビューされている場合に関連する。
- データガバナンスの有効性の指標となる可能性のある品質システムメトリクスのレビュー（すなわち、傾向）。

5.6.3 An effective review of the data governance system will demonstrate understanding regarding importance of interaction of company behaviours with organizational 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.

5.6.3 データガバナンスシステムの効果的なレビューは、企業の行動と組織的及び技術的な管理との相互作用の重要性に関する理解を示すものである。レビューの結果は、上級管理者に伝えられ、残存するデータインテグリティリスクの評価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ーマネジメントを成功させるための組織的影響

6.1 General

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

6.1 一般事項

6.1.1 組織の行動に関連する査察の欠陥を報告することは適切でないか、または可能でないかもしれない。行動が(i)データの修正、削除、または改ざんを行う動機や、(ii)データの完全性を確保するために設計された手続き上の管理の有効性にどのような影響を与えるかを理解することで、査察員はさらに調査可能なリスクの 有用な指標を得ることができる。

6.1.2 Inspectors should be sensitive to the influence of culture on organizational behaviour, and apply the principles described in this section of the guidance in an appropriate way. An effective ‘quality culture’ and data governance may be different in its implementation from one location to another. However, where it is apparent that cultural approaches have led to data integrity concerns; these concerns should be effectively and objectively reported by the inspector to the organization for rectification.

6.1.2 査察官は、文化が組織の行動に与える影響に敏感でなければならず、本指針の本項に記載されている原則を適切に適用しなければならない。効果的な「品質文化」とデータガバナンスは、場所によってその実施方法が異なるかもしれない。しかし、文化的なアプローチがデータインテグリティの懸念につながっていることが明らかな場合、 これらの懸念は、

次のように効果的かつ客観的に組織に報告されるべきである。
このような懸念は、是正のために査察員から組織に効果的かつ客観的に報告されるべきである。

6.1.3 Depending on culture, an organization's control measures may be:
・ 'open' (where hierarchy can be challenged by subordinates, and full reporting of a systemic or individual failure is a business expectation)
・ 'closed' (where reporting failure or challenging a hierarchy is culturally more difficult)

6.1.3 組織の文化に応じて、組織の統制手段は以下のようになるでしょう。
- オープン（階層に対して部下が異議を唱えることができ、組織的または個人的な失敗の完全な報告が ビジネス上の期待事項である場合)。
- 閉鎖的（失敗の報告や階層への異議申し立てが文化的に困難な場合)。

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

6.1.4 「オープン」な文化における優れたデータガバナンスは、医薬品品質システムを通じて問題を特定し報告するという従業員の権限によって促進される場合がある。「閉鎖的」な文化では、望ましくない情報を伝えることの社会的障壁のために、同等の管理レベ ルを達成するためには、監視及び二次レビューをより重視する必要があるかもしれない。このような状況では、上級管理者への秘密のエスカレーションプロセスを利用できることも重要であり、これらの取り決めは、報告が上級管理者によって積極的にサポートされ、奨励され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 organization'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 computerized (both hybrid and electronic) workflows.

6.1.5 データインテグリティに関する経営陣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。経営者は、データインテグリティの失効が発生するのを防ぎ、万一発生した場合にはそれを検知するという、法的および道徳的な義務（すなわち義務と権限）を知っていなければならない。経営陣は、紙とコンピュータ（ハイブリッドと電子の両方）のワークフローのデータインテグリティリスクについて、十分な可視性と理解を持つべきである。 および電子化された）ワークフローのデータインテグリティリスクを十分に可視化し、理解する必要がある。

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

6.1.6 データの完全性の欠落は、不正行為や改ざんに限らず、意図しないものであってもリスクとなり得る。データの信頼性が損なわれる可能性は、適切な管理を行うために特定し理解すべきリスクである（5.3〜5.5 項を参照）。直接的な管理は通常、文書化された方針及び手順の形で行われるが、従業員の行動に対する間接的な影響（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、データの危険化の機会、従業員による否定的な行動の合理化など）についても理解し、対処する必要がある。

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

6.1.7 データインテグリティの侵害は、いつでも、どの従業員によっても発生する可能性があるため、管理者は、問題の検出に注意を払い、問題が見つかった場合にはその理由を理解して、問題の調査と是正措置および予防措置の実施を可能にする必要がある。

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

6.1.8 データインテグリティの欠落は、患者の安全性に直接影響を与え、組織とその製品に対する信頼性を損なうなど、様々な利害関係者（患者、規制当局、顧客）に影響を与える結果となる。このような結果を従業員が認識し、理解することは、品質を優先する環境を醸成するのに役立つ。

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

6.1.9 経営陣は、データインテグリティの侵害を防止、検出、評価及び是正するための統制を確立するとともに、それらの統制がデータインテグリティを保証するために意図されたとおりに機能していることを検証するものとする。セクション 6.2 から 6.7 では、データインテグリティを成功させるために経営陣が取り組むべき主要項目の概要を示している。

6.1.10 Senior Management should have an appropriate level of understanding and commitment to effective data governance practices including the necessity for a combination of appropriate organizational 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 organization in a manner which ensures empowerment to report failures and opportunities for improvement. This reduces the incentive to falsify, alter or delete data.

6.1.10 上級管理者は、適切な組織文化及び行動（セクション 6）と、データの重要性、データリスク及びデータライフサイクルの理解との組み合わせの必要性を含め、効果的なデータガバナンスの実践に対する適切なレベルの理解とコミットメントを持つものとする。また、失敗や改善の機会を報告する権限を保証する方法で、組織内のすべてのレベルの担当者に期待事項を伝えている証拠が必要になる。これにより、データを改ざん、変更、または削除する動機が減少する。

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

6.2.1 Appropriate expectations for staff conduct, commitment to quality, organizational values and ethics should clearly communicated throughout the organization 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.

6.2 組織的価値、品質、スタッフの行動及び倫理に関する方針
6.2.1 スタッフの行動、品質へのコミットメント、組織の価値および倫理に対する適切な期待は、組織全体で明確に伝達されるものとし、適切な品質文化の実施および維持を支援するための方針が利用できるものとする。方針は、品質に関する経営陣の哲学を反映すべきであり、すべての個人が患者の安全と製品の品質を確保することに責任と説明責任を持つ、信頼の環境を構築する意図で書かれるべきである。

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.

6.2.2 経営陣は、データ品質確保における自分の役割の重要性、及び製品 品質の保証と患者の安全性の保護に対する自分の活動の影響を従業員に認識 させるものとする。

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.

6.2.3 方針は、正直さなどの倫理的行動の期待値を明確に定義するものとする。これは、すべての従業員に伝えられ、よく理解されるべきである。この伝達は、要件を知ることだけに限定されるべきではなく、なぜその要件が設定されたのか、要件を満たせなかった場合の結果も知るべきである。

6.2.4 Unwanted behaviours, such as deliberate data falsification, unauthorized 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.

6.2.4 意図的なデータの改ざん、不正な変更、データの破壊など、データの品質を損なう望ましくない行動には、速やかに対処するものとする。望ましくない行儀及び態度の例は、会社の方針に文書化されるべきである。望ましくない行動に対応するために事例を文書化するべきである。ただし、（懲戒処分などの）措置が、特定されたデータの完全性の問題に関するその後の調査を妨げないように注意する必要がある。例えば、厳しい報復により、他のスタッフが調査に価値のある情報を開示するのを妨げる可能性がある。

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

6.2.5 データ管理および完全性に関する優れた実践に適合する行動を示すことは、積極的に奨励され、適切に認識されるものとする。

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.

6.2.6 会社のポリシー及び手順に裏付けられた秘密のエスカレーション・ プログラムが存在し、情報提供者／従業員に影響を与えることなく、ポリシー違反の可能性がある事例を上級管理者に知らせることを従業員に奨励するものとする。上級管理者によるポリシー違反の可能性は認識されるべきであり、そのような場合のための適切な報告メカニズムが利用可能であるべきである。

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

6.2.7 可能であれば、経営陣は企業ポリシーの意図と要件を維持する標準（デフォルト）なコントロール機能を備えたシステムを導入するものとする。

6.3 Quality culture

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

between personnel at all levels.

6.3 品質文化
6.3.1 経営陣は、透明でオープンな職場環境（すなわち品質文化）の構築を目指すものとする。これは、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ことを従業員が奨励し、是正措置および予防措置を講じることができる環境である。組織の報告構造は、すべてのレベルの担当者間の情報の流れを可能にするものでなければならない。

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

6.3.2 データの品質と完全性を保証するための品質文化の構築に貢献する、経営陣、チームリーダー、品質担当者、及び全ての担当者が一貫して示す価値観、信念、考え方、及び行動の集合体である。

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 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 organization.

6.3.3 経営陣は以下の方法により品質文化を育成することができる。
- 期待されることの認識と理解を確実にする（価値観・倫理規範、行動規範など）。
- 模範を示して導く。経営者は、期待される行動を示すべきである。
- 行動と決定（特に委任された活動）に責任を持つこと。
- 事業の運営に継続的かつ積極的に関与すること。
- 従業員にプレッシャーを与える制限を考慮し、現実的な期待値を設定すること。
- 業務上の要求と期待に応えるために、適切な技術的および人的資源を割り当てる。

- データの完全性を確保するための良好な文化的態度を促進するような、公平で公正な結果と報酬を実施すること。
- 規制の動向を把握し、「学んだ教訓」を組織に適用する。

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

6.4 医薬品品質システムの近代化
6.4.1 現行の医薬品品質システムに近代的な品質リスクマネジメントの原則及び優れたデータマネジメントの実践を適用することにより、複雑なデータの生成に伴う課題に対応するためにシステムを近代化する。

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),
・ Computerized system validation,
・ IT infrastructure, services and security (physical and virtual),
・ Vendor/contractor management,
・ Training program to include company's approach to data governance and data governance SOPs,
・ Storage, processing, transfer and retrieval of completed records, including decentralized/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.

6.4.2 会社の医薬品品質システムは、データの完全性の失効につながる可能性のあるシステ

ムまたはプロセスの弱点を防止、検出、修正できるものとする。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かつ完全で信頼できるものとなるように、適切な管理及び手順を統合するべきである。具体的には、このような統制と手続きの変更は、以下の分野になる可能性がある。
- 品質リスク管理。
- 調査プログラム。
- データレビューの実施（セクション 9）。
- コンピュータ化されたシステムのバリデーション。
- IT インフラ、サービス、セキュリティ（物理的および仮想的）。
- ベンダー／請負業者の管理
- データガバナンスに対する会社のアプローチおよびデータガバナンス SOP を含むトレーニングプログラム。
- 分散型／クラウド型のデータ保管、処理、転送、および転送活動を含む、完了した記録の保管、処理、転送、および検索。
- ユーザー要求仕様書（URS）など、データの完全性に関する期待に応えるように設計された要件を組み込んだ GMP/GDP 重要機器および IT インフラストラクチャの購入に関する適切な監督（9.2 項参照）
- データの品質および整合性を含む自己点検プログラム、および
- パフォーマンス指標（品質メトリクス）と上級管理者への報告。

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

6.5 パフォーマンス指標（品質指標を含む）の定期的なマネジメントレビュー
6.5.1 データの完全性に関連するものを含め、パフォーマンス指標の定期的なマネジメントレビューを行うものとし、重要な問題を特定し、タイムリーに積極的に対処する。重要なパフォーマンス指標（KPI）を選択する際には、データの完全性の優先度が低い文化を不用意に生まないように注意する必要がある。

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

6.5.2 品質ユニットの責任者は、上級管理者が問題に対処するためのリソースを認識し割り当てることができるよう、リスクを直接伝えるために上級管理者への直接アクセス権を有するものとする。

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

6.5.3 経営陣は、独立した専門家に、自社のシステムおよび統制の有効性を定期的に検証させることができる。

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

6.6 資源配分
6.6.1 経営陣は、優れたデータインテグリティマネジメントをサポートし維持するために、適切なリソースを割り当て、データ生成および記録保持の担当者の作業量やプレッシャーが、エラー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やさないようにするものとする。

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 organization.

6.6.2 品質および管理の監督、IT サポート、調査の実施、研修プログラムの管理のために、組織の業務に見合った十分な数の人員を配置するべきである。

6.6.3 There should be provisions to purchase equipment, software and hardware that are appropriate for their needs, based on the criticality of the data in question. Companies should implement technical solutions that improve compliance with ALCOA+5 principles and thus mitigate weaknesses in relation to data quality and integrity.

6.6.3 問題となっているデータの重要性に基づき、そのニーズに適した機器、ソフトウェア、及び ハードウェアを購入するための規定があるべきである。企業は、ALCOA+5 の原則へ

の準拠を向上させ、その結果、データの品質と完全性に関する弱点を緩和する技術的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.

6.6.4 人員は、適切な職務分離を行い、適正な文書化の実施（GdocP）注の重要性を含め、特定の職務に対する資格と訓練を受けるものとする。また、電子データレビューなどの重要な手順に関するトレーニングの効果を示す証拠があるべきである。良好なデータマネジメントの実践という概念は、IT やエンジニアリングなどの分野を含め、GMP/GDP において役割を果たすすべての機能部門に適用される。
注）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、文書がデータ管理と整合性の原則を満たしていることを集合的かつ個別に確認するための文書管理（例：ALCOA+）

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

6.6.5 データの品質と完全性は誰もが知っているはずだが、様々なレベルのデータ品質専門家（SME、監督者、チームリーダー）が、調査の実施／支援、システムギャップの特定、改善の実施の推進のために協力するよう求められることがある。

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

6.6.6 データ管理者など、優れたデータマネジメントに関連する組織内の新しい役割の導入が検討されるかもしれない。

6.7 Dealing with data integrity issues found internally
6.7.1 In the event that data integrity lapses are found, they should be handled as any deviation

would be according to the Pharmaceutical Quality System. It is important to determine the extent of the problem as well as its root cause, then correcting the issue to its full extent and implement preventive measures. This may include the use of a third party for additional expertise or perspective, which may involve a gap assessment to identify weaknesses in the system.

6.7 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 データインテグリティの欠落が発見された場合は、医薬品品質システムに従った逸脱と同様に対処するものとする。問題の程度およびその根本原因を判断し、問題を完全に修正し、予防措置を実施することが重要である。これには、追加の専門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こともある。

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

6.7.2 患者の安全性及び製品品質への影響を考慮する場合、導き出された結論は健全な科学的証拠によって裏付けられるものとする。

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.

6.7.3 是正措置には製品リコール、顧客への通知、規制当局への報告が含まれる。是正処置、是正処置計画およびその実施は記録し、監視するものとする。

6.7.4 Further guidance may be found in section 12 of this guide.
6.7.4 本ガイドのセクション 12 には、さらなるガイダンスが記載されている。

7 GENERAL DATA INTEGRITY PRINCIPLES AND ENABLERS

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.

7 一般的なデータインテグリティの原則と実現手段

7.1 医薬品品質システムは、原薬及び医薬品のライフサイクルの様々な段階を通じて実施さ

れるべきであり、科学及びリスクベースのアプローチの使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).

7.2 十分な情報に基づいた意思決定を行い、情報の信頼性を確認するためには、その意思決定について情報を提供した事象又は行為を十分に文書化する必要がある。このように、適正な文書化の実施は、データの完全性を確保するための鍵であり、適切に設計された医薬品品質システム（セクション 6 で説明）の基本的な部分である。

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.

7.3 GdocPs の適用は、データの記録に使用される媒体（物理的記録と電子的記録など）によって異なる場合があるが、原則はどちらにも適用できる。このセクションでは、これらの重要な原則を紹介し、次のセクション（8 と 9）では、紙ベースと電子ベースの両方の記録管理における文書化に関連して、これらの原則を探る。

7.4 Some key concepts of GdocPs are summarized by the acronym ALCOA:
Attributable, Legible, Contemporaneous, Original, And Accurate. The following attributes can be added to the list: Complete, Consistent, Enduring and Available (ALCOA+6). Together, these expectations ensure that events are properly documented and the data can be used to support informed decisions.

7.4 GdocPs のいくつかの重要なコンセプトは、ALCOA という頭字語でまとめられている。Attributable, Legible, Contemporaneous, Original, and Accurate. 次のような属性を加えることもできる。Complete, Consistent, Enduring and Available (ALCOA+6)。これらにより、イベントが適切に文書化され、そのデータが十分な情報に基づいた意思決定に使用されることが保証される。

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

7.5 ペーパーシステムと電子システムの両方に適用される基本的なデータインテグリティの原則（例：ALCOA +）。

Data Integrity Attribute	Requirement
データインテグリティ属性	要件

Attributable
It should be possible to identify the individual or computerized 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.

帰属性
記録されたタスクを実行した個人またはコンピュータ化されたシステムを、そのタスクがいつ実行されたのかを特定できるようにすること。これは、誰がいつ、何のために変更を行ったのかを知ることが重要な、修正、削除、変更など、記録に加えられた変更にも適用される。

Legible
All records should be legible – the information should be readable and unambiguous in order for it to be understandable and of use. This applies to all information that would be required to be considered Complete, including all Original records or entries. Where the 'dynamic' nature of electronic data (the ability to search, query, 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.

読みやすさ
すべての記録は判読可能でなければならない。つまり、情報を理解し、利用するためには、情報が読みやすく、明確でなければならない。これは、オリジナルの記録やエントリーを含め、完全であるとみなされるために必要なすべての情報に適用される。電子データの「動的」な性質（検索、照会、傾向分析などの機能）が記録の内容と意味にとって重要である場合、適切なアプリケーションを使用してデータと対話できることが記録の「可用性」にとって重要である。

Contemporaneous
The evidence of actions, events or decisions should be recorded as they take place. This

documentation should serve as an accurate attestation of what was done, or what was decided and why, i.e. what influenced the decision at that time.

Contemporaneous
行動、出来事、決定の証拠は、それらが行われたときに記録されるべきである。この文書は、何が行われたか、何が決定されたか、そしてその理由、すなわちその時の決定に何が影響したかを正確に証明するものでなければならない。

Original
The original record can be described as the first-capture of information, whether recorded on paper (static) or electronically (usually dynamic, depending on the complexity of the system). Information that is originally captured in a dynamic state should remain available in that state.

オリジナル
オリジナルの記録とは、紙に記録されているか（静的)、電子的に記録されているか（システムの複雑さにもよるが、通常は動的）を問わず、情報の最初の取得と表現することができる。動的な状態で最初に取得された情報は、その状態で利用可能なままでなければならない。

Accurate
Records need to be a truthful representation of facts to be accurate. Ensuring records are accurate is achieved through many elements of a robust Pharmaceutical Quality System. This can be comprised of:
・ equipment related factors such as qualification, calibration, maintenance and computer validation.
・ policies and procedures to control actions and behaviours, including data review procedures to verify adherence to procedural requirements
・ deviation management including root cause analysis, impact assessments and CAPA
・ trained and qualified personnel who understand the importance of following established procedures and documenting their actions and decisions. Together, these elements aim to ensure the accuracy of information, including scientific data that is used to make critical decisions about the quality of products.

正確さ
記録が正確であるためには、事実を忠実に表現している必要がある。記録が正確であることは、強固な医薬品品質システムの多くの要素によって達成される。これには次のようなものがある。

- 資格認定、校正、メンテナンス、コンピュータバリデーションなどの機器関連要素
- 手続き上の要求事項の遵守を確認するためのデータレビュー手順を含む、行動と行為を管理するための方針と手順
- 根本原因分析、影響評価、CAPA を含む逸脱管理
- 訓練を受けた有資格者で、確立された手順に従い、自らの行動と決定を文書化することの重要性を理解している者。これらの要素を組み合わせることで、製品の品質に関する重要な意思決定に使用される科学的データを含む情報の正確性を確保することを目的としている。

Complete

All information that would be critical to recreating an event is important when trying to understand the event. It is important that information is not lost or deleted. The level of detail required for an information set to be considered complete would depend on the criticality of the information (see section 5.4 Data criticality). A complete record of data generated electronically includes relevant metadata (see section 9).

完成

イベントを理解しようとする際に、イベントを再現するのに重要となる情報はすべて重要になる。情報が失われたり削除されたりしないことが重要である。情報セットが完全であると判断されるために必要な詳細レベルは、情報の重要性に依存する（5.4 データの重要性参照）。

電子的に生成されたデータの完全な記録には、関連するメタデータが含まれる（セクション 9 参照）。

Consistent

Information should be created, processed, and stored in a logical manner that has a defined consistency. This includes policies or procedures that help control or standardize data (e.g. chronological sequencing, date formats, units of measurement, approaches to rounding, significant digits, etc.).

一貫性

情報は、定義された一貫性を持つ論理的な方法で作成、処理、保存されなければならない。これには、データの管理や標準化に役立つポリシーや手順が含まれる（例：時系列の順序、日付のフォーマット、測定単位、丸め方のアプローチ、有効数字など）。

Enduring

Records should be kept in a manner such that they exist for the entire period during which

they might be needed. This means they need to remain intact and accessible as an indelible/durable record throughout the record retention period.

永続性
記録は、それが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な方法で保管されるべきである。これは、記録保持期間中、消えない/耐久性のある記録として、そのままの状態でアクセス可能である必要があることを意味する。

Available
Records should be available for review at any time during the required retention period, accessible in a readable format to all applicable personnel who are responsible for their review whether for routine release decisions, investigations, trending, annual reports, audits or inspections.

利用可能
記録は、必要とされる保存期間中、いつでも閲覧できるようにしておく必要がある。また、日常的なリリースの決定、調査、傾向、年次報告書、監査、検査など、記録の閲覧に責任を持つすべての該当する担当者が、読みやすい形式でアクセスできるようにしておく必要がある。

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

7.6 これらの要素が、医薬品品質システムの他の支援要素とともに、GMP 及び GDP 関連活動のすべての適用領域に適切に適用されるならば、医薬品に関する重要な決定を行うために使用される情報の信頼性は十分に保証されるはずである。

7.7 True copies
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).

7.7 真のコピー

7.7.1 オリジナルの紙記録（例：分析サマリーレポート、バリデーションレポートなど）のコピーは、一般的に、例えば異なる場所で活動する企業間のコミュニケーション目的で非常に有用である。これらの記録は、別のサイト（姉妹会社、請負業者など）から受け取ったデータが、必要に応じて「真正なコピー」として維持されるか、または「真正なコピー」の要件を満たさない場合（複雑な分析データの要約など）に「要約レポート」として使用されるように、そのライフサイクルにおいて管理されるべきである。

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.

7.7.2 静的な記録が元のデータの完全性を維持することが正当化される場合、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 形式で保持することが考えられる。しかしながら、データ保持プロセスは、医薬品の品質のあらゆる側面に直接または間接的に影響を与え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、及び特定の生データセットの再構築に必要なすべてのデータ処理実行（方法及び監査証跡を含む）が含まれる）。また、印刷された記録が正確に表現されていることを検証するための文書化された手段も必要となる。このアプローチは、GMP/GDP に準拠した記録を可能にするための管理において、負担が大きいと思われる。

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

7.7.3 多くの電子記録は、データとのインタラクションを可能にするため、動的形式で保持することが重要である。データの完全性や後の検証に不可欠な場合は、データを動的な形式で保持すべきである。データを動的形式で保存すべきかどうか、またどのくらいの期間保存すべきかを裏付け、 正当化するために、リスク管理の原則を利用すべきである。

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.

7.7.4 受入サイトでは、これらの記録（真のコピー）は、紙または電子フォーマット（例：PDF）のいずれかで管理され、承認された QA 手順に従って管理されるものとする。

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.

7.7.5 文書の真正性を容易に検証できる方法、例えば、手書き又は電子署名の使用、又は真正な コピーを作成するための有効なプロセスに従って生成された文書が、「真正なコピー」として適切に 認証されるよう、注意を払うものとする。

Item　How should the “true copy” be issued and controlled?
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 recipient.

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

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.

1. 紙の文書の「真正なコピー」を作成すること。
真正なコピーを発行する会社で
- 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、原本をコピーする。
- コピーされた文書の真正性を確認し、「True Copy」として新しいハードコピーに署名および日付を記入する。

この「True Copy」を目的の受信者に送信することができる。

電子文書の「True Copy」の作成。
電子記録の「真正なコピー」は、必要なメタデータをすべて含めて、電子的手段（電子ファイルコピー）で作成する必要がある。メタデータが失われる可能性がある場合、電子データの pdf 版を作成することは禁止されるべきである。

True Copy」を意図した受信者に送信することができる。

発行された全ての "True Copy"(ソフト/ハード)の配布リストを維持すべきである。

記録を確認する際にチェックすべき特定の要素
- 真正コピーの作成手順を確認し、作成方法が適切に管理されていることを確認する。
- 発行された真正なコピーがオリジナルの記録と同一（完全かつ正確）であることを確認する。コピーされた記録は、オリジナルの文書記録と照合し、スキャン画像の改ざんがないことを確認する。
- データの整合性を確保するために、スキャンまたは保存された記録が保護されていることを確認する。
- 紙の記録をスキャンし、「真のコピー」の作成を確認した後
 -真正なコピーが顧客への送付などの配布目的で作成された場合、スキャン画像の元となったオリジナル文書は、記録所有者がそれぞれの保存期間中に保持する必要がある。
-文書の保管を支援するために真正なコピーが生成される場合、スキャン画像が作成された元の記録文書の代わりにコピーを保管することが可能な場合がある。

2. At the company who receives the true copy:
- The paper version, scanned copy or electronic file should be reviewed and filed according to good document management practices.
The document should clearly indicate that it is a true copy and not an original record.

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.

2. 真正なコピーを受け取った会社で。
- 紙版、スキャンされたコピー、または電子ファイルは、優れた文書管理の慣行に従って検討され、ファイルされるべきである。
文書には、それが原本の記録ではなく真正なコピーであることを明確に示す必要がある。

記録を確認する際にチェックすべき具体的な要素
- 受け取った記録がチェックされ、適切に保管されていることを確認する。
- "真正なコピー "の真正性を検証するシステムを導入すること。
例：正しい署名者を確認すること。

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.

7.7.6 「真正なコピー」の生成及び転送、並びにデータインテグリティの管理に関する責任を取り扱うために、品質協定を設けるものとする。「真正なコピー」の発行及び管理のためのシステムは、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保証するために、契約の授受者によって監査されるべきである。

7.8 Limitations of remote review of summary reports
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.

7.8 サマリーレポートのリモートレビューの限界
7.8.1 サマリーレポート内のデータのリモートレビューは一般的に必要とされるものであるが、データの完全性を適切に管理するために、リモートデータレビューの限界を十分に理解する必要がある。

7.8.2 Summary reports of data are often supplied between physically remote manufacturing sites, Market Authorization 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.

7.8.2 データのサマリーレポートは、物理的に離れた場所にある製造施設、市場認可権者及びその他の関係者の間で提供されることが多い。しかし、重要な裏付けデータやメタデータが含まれていないことが多く、そのため元のデータをレビューすることができないという点で、サマリーレポートは本質的に限定された性質のものであることを認識する必要がある。

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.

7.8.3 したがって、サマリー・レポートはデータ転送プロセスの一つの要素であると考え、

利害関係者及び 検査機関がサマリー・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 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.

7.8.4 サマリーデータを受領する前に、サプライヤーの品質システムの評価及びデータインテグリティ原則への準拠を確立するものとする。データインテグリティの原則への準拠を机上または同様の評価で決定することは、通常、受け入れられず、また不可能である。

7.8.4.1 For external entities, this should be determined through on-site audit when considered important in the context of quality risk management. The audit should assure the veracity of data generated by the company, and include a review of the mechanisms used to generate and distribute summary data and reports.

7.8.4.1 外部機関については、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、現地での監査により決定されるものとする。監査では、会社が作成したデータの真実性を保証するものとし、サマリーデータや報告書を作成・配布するために使用されるメカニズムの見直しを含むものとする。

7.8.4.2 Where summary data is distributed between different sites of the same organization, 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.).

7.8.4.2 サマリーデータが同一組織の異なるサイト間で配布されている場合、供給元サイトのコンプライ アンスの評価は、別の手段（企業の手順に準拠していることの証拠、内部監査報告書など）を用いて 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 authorized staff at the original site. Summaries should be accompanied with a declaration signed by the Authorized 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.

7.8.5 サマリーデータは、合意された手順に従って作成され、オリジナルサイトの権限を有するスタッ フによってレビュー及び承認されるものとする。サマリーには、サマリーの真正性及び正確性を記載した権限を有する者が署名した宣言書を添 付するものとする。サマリーレポートの生成、転送及び検証のための取り決めは、品質／技術協定の中で取り扱われるべきである。

8 SPECIFIC DATA INTEGRITY CONSIDERATIONS FOR PAPERBASED SYSTEMS

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

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 医薬品品質システムの構造とブランクフォーム／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.

8.1.1 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。従って、文書システムは GMP/GDP の要求事項を満たすように設計され、文書と記録がその完全性を維持するために効果的に管理されることを確実にする必要がある。

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

8.1.2 紙の記録は管理されるべきであり、データのライフサイクルを通じて、帰属性、可読性、同時期性、原本性と正確性、完全性、一貫性のある永続性（indelible/durable)、および利用可能性（ALCOA+）を維持しなければならない。

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 disposal of records.

8.1.3 適正な文書化の実施及び文書管理の取り決めを概説する手順書が医薬品品質システム内に用意されるものとする。これらの手順は、以下を含む、データのライフサイクルを通してデータの整合性を維持する方法を明記するものとする。
- マスター文書及び手順の作成、レビュー及び承認
- データ（マスター、ログなど）を記録するために使用されるテンプレートの生成、配布および管理。
- 記録に関する検索および災害復旧プロセス
- SOP（標準操作手順書）やブランクフォームなどの文書のコピーを確実に発行し、管理された追跡可能な方法で使用できるように調整することに特に重点を置いた、日常使用する文書の作業コピーの作成。
- 個々の個人の識別方法、データ入力フォーマット、記録の修正、および正確性、真正性、完全性のための定期的なレビューを明記した、紙ベースの文書の完成。
- 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
8.2.1 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.

8.2 記録を管理することの重要性
8.2.1 記録は GMP/GDP 運営に不可欠であり、以下の管理が必要である。

確保する。
- 実施された活動の証拠。
- GMP/GDP 要求事項及び会社の方針、手順、作業指示に準拠していることの証拠。
- 医薬品品質システムの有効性。
- トレーサビリティー
- プロセスの信頼性と一貫性
- 製造された医薬品の良質な属性の証拠
- 苦情やリコールが発生した場合、記録は調査目的で使用される可能性がある。
- 逸脱やテストの失敗があった場合、記録は効果的な調査を完了するために重要である。

8.3 Generation, distribution and control of template records
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).

8.3 テンプレート記録の生成、配布および管理
8.3.1 マスター文書の管理および制御は、「通常の手段」（すなわち、専門的な不正技術を必要としない）で誰かが記録を不適切に使用および／または改竄するリスクを、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。以下の期待事項は、記録されたデータのリスクと重要性を考慮し、品質リスク管理アプローチを用いて実施されるべきである（5.4、5.5 項参照）。

8.4 Expectations for the generation, distribution and control of records
Item　　Generation
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.

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 traceablility. In addition, uncontrolled

records may not be designed to correctly record critical data.
・ It might be easier to falsify uncontrolled records.
・ Use of temporary recording practices may lead to data omission, and these temporary original records are not specified for retention.
・ If records can be created and accessed without control, it is possible that the records may not have been recorded at the time the event occurred.
・ There is a risk of using superseded forms if there is no version control or controls for issuance.

8.4 記録の生成、配布、管理に期待すること
項目の生成
1. 期待されること
すべての文書は、ユニーク（特有）な識別性（バージョン番号を含む）を持ち、チェック、承認、署名、日付が入っているべきである。

管理されていない文書の使用は、ローカルな手順によって禁止されるべきである。紙切れなどの一時的な記録方法の使用は禁止されるべきである。

期待を満たさないことによる潜在的リスク／チェックすべき項目
- 管理されていない文書は、追跡可能性がないまま廃棄または破棄される可能性があるため、重要なデータの漏れや損失の可能性が高まる。また、管理されていない記録は、重要なデータを正しく記録するように設計されていない可能性がある。
- 管理されていない記録は改ざんが容易である可能性がある。
- 一時的な記録方法を使用すると、データの漏れが発生する可能性があり、このような一時的なオリジナル記録は保存のために指定されていない。
- 管理されていない記録が作成され、アクセスできる場合、事象が発生した時点で記録されていなかった可能性がある。
- バージョン管理や発行のコントロールが行われていない場合、古くなったフォームを使用するリスクがある。

2. Expectation
The document design should provide sufficient space for manual data entries.
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.

2. 期待すること

ドキュメントのデザインは、手動でデータを入力するための十分なスペースを提供すべきである。

期待値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

- データ入力のためのスペースが十分に確保されていない場合、手書きデータは明確で読みやすいものにならない可能性がある。
- ドキュメントは、コメントのための十分なスペースを提供するように設計されるべきである。例えば、転写エラーの場合、オペレーターがエラーを消し、イニシャルと日付を記入し、必要な説明を記録するための十分なスペースが必要である。
- 完全な文書化のために文書のページを追加する場合は、追加したページの数と参照先を主記録ページに明確に記録し、署名すること。
- すべての必要なデータを追加するために、文書フォーマットに十分なスペースを設けるべきであり、データを文書に無造作に記録してはならない。例えば、この目的のためではない印刷されたページの裏に記録することを避けるために意図していない印刷物の裏に記録されないようにするなど、無造作にデータを記録しないこと。

3. Expectation

The document design should make it clear what data is to be provided in entries.

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.

3. 期待すること
ドキュメントデザインでは、エントリーにどのようなデータが提供されるべきかを明確にする必要がある。
期待値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
- 曖昧な指示は、データの一貫性のない/間違った記録につながる可能性がある。
- 優れたデザインは、すべての重要なデータが確実に記録され、記入内容が明確に、同時に、永続的に（消えないように/耐久性のあるように）記入されることを保証する。
- また、重要なデータを不用意に省略するリスクを最小限にするために、運用プロセスおよび関連する SOP と同じ順序で情報を記録するように文書を構成すること。

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 unauthorized changes.

Potential risk of not meeting expectations/items to be checked
・ Inappropriate storage conditions can allow unauthorized 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.

4. 期待すること
文書は、適切なバージョン管理を確実にする方法で保管されるべきである。
マスター文書には、不用意な使用を防ぐために色紙やインクを使用するなど、マスターとコピーを区別するための特徴的なマーキングを施すべきである。

マスター・ドキュメント（電子形式）は、無許可または不注意による変更を防止すべきであ

る。
例えば、以下のように。電子的に保存されたテンプレート記録については、以下の予防措置を講じるべきである。
- マスターテンプレートへのアクセスは管理されるべきである。
- バージョンの作成と更新のためのプロセス管理が明確で、実際に適用/検証されていること。
- マスタードキュメントは、不正な変更を防止する方法で保存されるべきである。

期待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
- 不適切な保管条件は、無許可の変更、期限切れ及び／又はドラフト文書の使用を可能にし、又はマスター文書の紛失を引き起こす可能性がある。
- 文書と同様に重要なのは、実施のプロセスと、必要に応じて実施前に適切なトレーニングを行うことによる効果的なコミュニケーションである。

Item　Distribution and Control
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.
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.

アイテムの配布と管理
1. 期待されること
更新されたバージョンは、タイムリーに配布されるべきである。
旧式のマスタードキュメントやファイルはアーカイブ化し、アクセスを制限すべきである。
発行された未使用の物理的文書はすべて回収し、照合するものとする。
品質管理者が許可した場合、文書の復元コピーを破棄することができる。ただし、承認された文書のマスターコピーは保存されるべきである。
期待を満たさない潜在的リスク／チェックすべき項目
- 古いバージョンが使用可能な場合、誤って使用してしまうリスクがあるかもしれない。

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 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.

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.

2. 期待すること
文書の発行は、以下の管理を含む書面による手順で管理されるべきである。
- 誰がコピーを発行したか、いつ発行されたかの詳細。
- 承認された文書のコピーを区別する明確な手段（例：安全なスタンプ、作業場所にない紙

のカラーコード、またはその他の適切なシステムを使用すること)。
- 最新の承認済みバージョンのみが使用可能であることを保証すること。
- 発行された各ブランク文書に一意の識別子を割り当て、各文書の発行を登録簿に記録すること。
- 配布されたすべてのコピーに番号を付け（例：コピー2／2)、製本された書籍の発行ページに連番を付ける。
- 白紙のテンプレートを追加で発行する必要がある場合は、再発行に関する管理されたプロセスに従って、配布されたすべてのコピーを維持し、追加コピーの必要性の正当性と承認を記録する必要があります（例：「オリジナルのテンプレートの記録が破損した」)。"例：「オリジナルのテンプレートの記録が破損した」。
- 重要な GMP/GDP 空白書式（例：ワークシート、実験ノート、バッチ記録、管理記録）は、記録の正確性と完全性を保証するために、使用後に照合されるべきである；および
- 記録以外の文書（手順書など）のコピーが参照用にのみ印刷される場合、文書の作成時にタイムスタンプが押され、文書にその短期的な有効性が記されていれば、照合は必要ないかもしれない。

期待を満たさない潜在的なリスク／チェックすべき項目
- セキュリティ対策を行わない場合、テンプレートレコードをコピーまたはスキャンした後に、データの書き換えや改ざんが行われるリスクがある（ユーザーは別のテンプレートコピーを使用することになる)。
- 旧式のバージョンは、意図的にまたは誤って使用される可能性がある。
- 変則的なデータ入力が行われた記入済みの記録は、新たに書き直されたテンプレートで置き換えることができる。
- すべての未使用のフォームは、説明を受け、汚して破棄するか、安全なファイリングのために返却する必要がある。
- 文書の参照用コピー（使用する場合）には、作成日、有効期間、および参照用であって正式なコピーではないことの明確な表示（例：「印刷時に管理されていない」と表示されている）が明示されていることを確認する。

8.4.1 An index of all authorized 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.).

8.4.1 承認された全てのマスター文書（SOP、フォーム、テンプレート及び記録）の索引を

医薬品品質システム内に維持するものとする。
この索引には、テンプレート記録の種類ごとに、少なくとも次の情報が記載されていなければならない：タイトル、バージョン番号を含む識別性、場所（例：文書データベース、発効日、次回レビュー日など）。

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

8.5 ポイントオブユース（使用場所）にある記録の使用と管理
8.5.1 記録は使用時に作業者が利用できるものとし、これらの記録を管理するために適切な管理が行われるものとする。これらの管理は、記録の損傷または紛失のリスクを最小化し、データの完全性を確保するために実施されるべきである。必要に応じて、記録が汚されないように保護する手段を講じるべきである（例：水に濡れる、物質で汚れるなど）。

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

8.5.2 記録は、これらの領域で指定された人またはプロセスにより、書面による手順に従って適切に管理されるものとする。

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

8.6 記録の記入
8.6.1 記録が適切に記入されていることを保証するために、以下の表に示す項目を管理するものとする。

Item　Completion of records
1. Expectations
Handwritten entries should be made by the person who executed the task.

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.
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.

項目 記録の記入
1. 期待されること
手書きの記入は、その作業を実行した人が行うべきである。

文書内の未使用の空欄は無効にし（例：消しゴムをかける)、日付を記入し、署名する。
手書きでの記入は、明確で読みやすい文字で行うこと。
日付欄の記入は、現場で定義された曖昧さのないフォーマットで行うこと。例：dd/mm/yyyy または mm/dd/yyyy。
期待値を満たさない場合の潜在的リスク／チェックすべき項目
- 同一人物が記入した場合、筆跡が一貫していることを確認する。
- 記入内容が読みやすく明確であること（曖昧さがなく、不明な記号や略語（例：ditto (") マークの使用）が含まれていないこと)。
- 記録されたデータが完全であるかどうかを確認する。
- 記録の正しいページネーション注）を確認し、すべてのページが存在するかどうか。

注）その記録の元がどこにあるかを明記したもの

2. Expectation
Records relating to operations should be completed contemporaneously.

Potential risk of not meeting expectations/items to be checked
・ Verify that records are available within the immediate areas in which they are used, i.e. Inspectors should expect that sequential recording can be performed at the site of operations. If the form is not available at the point of use, this will not allow operators to fill in records at the time of occurrence.

2. 期待すること
操作に関連する記録は同時期に完了すべきである。

期待値を満たさない場合の潜在的リスク／チェックすべき項目
- 記録が使用される直近のエリア内で利用可能であることを検証する。すなわち、検査官は、操作の現場で逐次記録を行うことができることを期待するべきである。使用する場所でフォームが利用できない場合、これでは作業者が発生時に記録を記入することができない。

3. Expectation
Records should be enduring (indelible).
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.

3. 期待すること
記録は永続的なものでなければならない（消せない）。
期待値を満たさない場合の潜在的リスク／チェックすべき項目
- 記録はインクで書かれているが、インクは消せないし、（保存期間中に）汚れたり消えたりしないことを確認する。
- 記録は、ペンを使う前に鉛筆で記入されていないか（上書き）。
- なお、システムから出力された紙の中には、感熱紙のように時間の経過とともに色あせてしまうものもある。これらの記録は、署名と日付の入った不可解なコピーを作成し、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.
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 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.

4. 期待すること
記録は、作成者に帰属する一意の識別性を用いて署名し、日付を記入すべきである。
期待値を満たさない場合の潜在的リスク／チェックすべき項目
- 管理された最新の署名とイニシャルのログがあり、標準化された印刷された文字だけでなく、独自の例を使用していることを実証していることを確認する。
- すべての重要な入力項目に署名と日付が入っていることを確認する。特に、時間をかけてステップが行われる場合は、ページやプロセスの最後に署名するだけではないこと。
- 個人的な印鑑の使用は一般的に推奨されていないが、使用する場合には、アクセスのために印鑑を管理する必要がある。個人と他の人の印鑑の間のトレーサビリティー（識別）を明確に示すログがあるべきである。個人の印鑑の使用には（所有者による）日付が記録されることで本人と認められる。

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

8.7 記録の修正
記録の修正は、完全なトレーサビリティーが維持されるような方法で行われなければならない。

Item　How should records be corrected?

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.
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.

項目 記録はどのように修正されるべきか？

1 期待すること
変更すべき箇所を一本の線で消す。
必要に応じて、訂正の理由を明確に記録し、重要な場合は検証する。
変更した箇所にイニシャルと日付を入れる。
記録を確認する際にチェックすべき特定の要素
- 元のデータが読めて、不明瞭でないことを確認する（例：液体の紙を使って不明瞭になっていないか、上書きは許されない)。
- 重要な記録データの記入に変更が加えられた場合は、変更の正当な理由が記録されているか、また、変更の裏付けとなる証拠があるかを確認する。
- 記録に説明のつかない記号や記入がないか確認する。

2. Expectation
Corrections should be made in indelible ink.
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).

2. 期待すること
訂正は消えることのないインクで行ってください。
記録を確認する際にチェックすべき具体的な要素。
- 記入された内容は、消せないインクで書かれているか、汚れたり消えたりしないかを確認する（保存期間中)。
- 記録は、ペンを使う前に鉛筆で記入されていないか（上書き）を確認する。

8.8 Verification of records (secondary checks)
Item　When and who should verify the records?
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. Authorized 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.
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.
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.

8.8 記録の検証（二次チェック）
項目 いつ、誰が記録を検証すべきか？
1. 期待されること
重要なプロセスステップの記録（例：バッチ記録内の重要なステップ）は、以下の通りであるべきである。
- 重要なプロセスステップの記録のレビュー＆確認は，個別に事前に承認された人が、その記録が品質ユニットに送付する前に、生産部門内で確認する。
- 製造されたバッチのリリースまたは出荷前に、品質ユニット（例：認定者／資格者）がレビューし、承認すること。
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担当者がレビューする。
試験段階の実験室記録もまた、試験の完了後に指定された要員（例：第二分析者）によって

レビューされるべきである。レビュー担当者は、データ統合性の原則に従って、すべての記入事項、重要な計算を確認し、 試験結果の信頼性について適切な評価を行うことが期待される。
重要な試験の解釈を一人の人間が行う場合（例：寒天プレート上の微生物コロニーの記録）は、追加の管理を考慮すべきである。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となる場合がある。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かもしれない。重要なデータを検証するための適切な電子的手段は、データの写真画像を保存するなど、容認可能な代替手段となる場合がある。
この検証は、生産に関連する作業および活動を行った後に実施し、適切な人が署名または署名し、日付を記入すること。
書面による文書のレビューのプロセスを記述したその製造所のローカル SOP を設置することが望ましい。
記録をレビューする際にチェックすべき具体的な要素。
- 記録が関連する活動を行う際に、正しい担当者がすぐに利用できるように、加工エリア内での生産記録の取り扱いプロセスを検証すること。
- 処理中に行われる二次的なチェックが、適切な資格を持った独立した要員（製造監督者や QA など）によって行われたことを確認する。
- 作業活動の完了後、製造担当者、品質保証担当者の順で文書がレビューされたことを確認する。

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

2. 期待すること
現在の（承認された）テンプレートを使用してすべてのフィールドが正しく記入されていること、およびデータが受入れ基準と厳格に規格に適合しているか比較し確認する。
8.6 項の項目 1、2、3、4、および 8.7 項の項目 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な要素。
- 査察員は、手動データのレビューに関する会社の手順を確認し、プロセスの妥当性を判断する。
- 二次チェックの必要性と程度は、生成されるデータの重要性に基づいて、品質リスク管理の原則に基づくべきである。
- データの二次レビューには、使用された計算の検証が含まれていることを確認する。
- 元のデータ（可能な場合）を見て、正しいデータが計算のために転記されたことを確認する。

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

8.9 電子システムからの直接プリントアウト
8.9.1 いくつかの非常に単純な電子システム、例えば天秤、pH メータ、またはデータを保存しない単純な処理機器は、直接印刷された紙の記録を生成する。このようなタイプのシステムおよび記録では、（再）処理や電子的な日付／時間スタンプの変更によってデータの表示に影響を与える機会が限られている。このような状況では、記録の原本には記録を作成した人の署名と日付を入れ、サンプル ID、バッチ番号などのトレーサビリティを確保するための情報を記録するべきである。これらの原本の記録は、バッチ処理または試験の記録に添付されるべきである。

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

8.9.2 これらの記録が永続的であることを考慮するものとする（8.6.1 項参照）。

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

8.10 文書保持（記録保持要件の特定および記録のアーカイブ化）

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.

8.10.1 各種類の記録の保存期間は（少なくとも）GMP/GDP 要求事項で指定された期間を満たすものとする。より長い保存期間を規定している可能性のある他の地域または国の法律を考慮するものとする。

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.

8.10.2 記録は、社内で保持することもできるし、品質協定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。この場合、データセンターの所在地を特定する必要がある。保管システム／設備／サービスが適切であること、および残存リスクが理解されていることを示すために、リスクアセスメントが利用可能でなければならない。

Item　Where and how should records be archived?
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

項目 記録はどこで、どのように保管されるべきか？
1. 期待すること
記録を保管するためのさまざまな手順（保管ボックスの識別、ボックスごとの記録のリスト、保存期間、保管場所など）を記述したシステムがあること。
記録の保管、アクセス、回収の管理についての指示があること。
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、確実に保管されるべきである

Specific elements that should be checked when 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 authorized 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.

記録を確認する際に確認すべき具体的な要素。

- 保管された記録を検索するために実施されたシステムが効果的であり、追跡可能であることを確認する。

- 記録が整然と保管されているか、容易に識別できるかを確認する。

- 記録が定められた場所にあり、適切に保護されているかを確認する。- 保存された記録の完全性を確保するために、保管された文書へのアクセスが許可された担当者に制限されていることを確認する。

- 記録へのアクセスと返却の記録があるかどうかを確認する。

- 使用される保管方法は、必要なときに文書を効率的に取り出せるものでなければならない。

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.

2. 期待されること

すべてのハードコピー品質記録は、以下の場所に保管されるべきである。

- 損傷や紛失を防ぐために安全な場所に保管する。
- 簡単に追跡でき、検索できるような方法で。
- 記録の保存期間中の耐久性を確保する方法。

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.
・ Verify whether the storage methods used permit efficient retrieval of documents when required.

記録を確認する際にチェックすべき具体的な要素。
- 委託された保管業務について、品質協定が締結されているか、保管場所が監査されているかを確認する。
- 文書が保管期間中も読みやすく、利用可能であることを保証するための評価があるかどうかを確認する。
- 永久的ではないプリントアウト（熱転写紙など）の場合は、検証された（「真実の」）コピーを保持すること。
- 使用されている保管方法が、必要なときに文書を効率的に取り出せるかどうかを検証する。

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.

3. 期待すること
すべての記録は、以下の原因による損傷や破壊から保護されなければなりません。
- 火。
- 液体（例：水、溶剤、緩衝液）。
- ネズミ。
- 湿度など。
- 記録を修正、破壊、交換しようとする無権限者のアクセス。

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.

記録を確認する際にチェックすべき特定の要素
- 記録を保護するシステムがあるかどうかを確認する（害虫駆除やスプリンクラーなど)。
- 注：スプリンクラーシステムは、地域の安全要件に従って導入されるべきであるが、文書が水から保護されるなど、文書へのダメージを防ぐように設計されている必要がある。
- 記録に対する適切なアクセスコントロールを確認する。

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

8.11 記録原本または真正コピーの廃棄
8.11.1 記録の廃棄のための文書化されたプロセスは、定義された保存期間後に正しい原本記録または真正のコピーが廃棄されることを確実にするために設置されるものとする。このシステムは、現行の記録が誤って破壊されないようにし、歴史的な記録が誤って現行の記録の流れに戻ってこないようにする必要がある（例：歴史的な記録が現行の記録と混同／混合される)。

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

8.11.2 記録/登録は、ローカルポリシーに従い、適切かつタイムリーに退職記録の保管または廃棄を行うことを証明するために利用できるものとする。

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.

8.11.3 誤った文書を消し去るリスクを低減するための対策を講じるものとする。記録の廃棄を許可するアクセス権は管理され、少数の人に限定されるべきである。

9 SPECIFIC DATA INTEGRITY CONSIDERATIONS FOR COMPUTERISED SYSTEMS

9 コンピュータ化された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 computerized systems
9.1.1 A large variety of computerized 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 computerized systems and manage them in accordance with GMP10 and GDP11 requirements.

9.1 医薬品品質システムの構造及びコンピュータ化システムの管理
9.1.1 企業は、多くの業務活動を支援するために、多種多様なコンピュータ化システムを使用している。これらは、単純な独立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っており、その多くが製造される製品の品質に影響を与えている。すべてのコンピュータ化システムを十分に評価・管理し、GMP10 および GDP11 の要求事項に従って管理することは、各規制対象企業の責任である。

9.1.2 Organizations should be fully aware of the nature and extent of computerized systems utilized, 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 computerized systems and any associated data, in respect of product quality.

9.1.2 組織は利用しているコンピュータ化システムの性質及び範囲を十分に認識し、各システム、その意図された使用及び機能、並びに操作される可能性のあるデータインテグリティリスク又は脆弱性を説明する評価を実施するものとする。特に、製品の品質に関わるコンピュータ・システムおよび関連データの重要性を判断することに重点を置くべきである。

9.1.3 All computerized 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.

9.1.3 製品の品質に影響を与える可能性のある全てのコンピュータシステムは、偶発的又は意図的な操作、変更、又はデータの品質と完全性に影響を与える可能性のあるその他の活動

からシステムが確実に保護されるように設計された医薬品品質システムの下で効果的に管理されるものとする。

9.1.4 The processes for the design, evaluation, and selection of computerized 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.

9.1.4 コンピュータ化システムの設計、評価及び選択のプロセスは、システムのデータ管理及び完全性の側面の適切な検討を含むものとする。規制対象となるユーザーは、システムのベンダーが GMP/GDP 及びデータインテグリティの要求事項を適切に理解していること、及び新しいシステムが効果的なデータ管理を確実にするための適切なコントロールを含んでいることを確認すべきである。従来のシステムも同様の基本的要件を満たすことが期待されるが、完全に準拠するためには、管理手順のサポートや補助的なセキュリティハードウェア／ソフトウェアなど、追加的なコントロールの使用が必要となる場合がある。

9.1.5 Regulated users should fully understand the extent and nature of data generated by computerized 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:

9.1.5 規制対象ユーザーは、コンピュータ化されたシステムによって生成されるデータの範囲及び性質を十分に理解すべきであり、データ（メタデータを含む）のデータリスク及び重要性、並びに生成されたデー タを管理するために必要なその後の管理を決定するために、リスクベースのアプローチが取られるものとする。例えば

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

9.1.5.1 生データを扱う場合、製造イベント又は分析を再構築するためには、通常、生データの完全な捕捉及び保存が必要となる。

9.1.5.2 In dealing with metadata, some metadata is critical in reconstruction of events, (e.g.

user identification, times, critical process parameters, units of measure), and would be considered as 'relevant metadata' that should be fully captured and managed. However, non-critical meta-data such as system error logs or non-critical system checks may not require full capture and management where justified using risk management.

9.1.5.2 メタデータの取り扱いにおいて、メタデータの中にはイベントの再現に不可欠なもの（例：ユーザ識別、時間、重要なプロセスパラメータ、測定単位）があり、完全に捕捉し管理すべき「関連するメタデータ」とみなされる。しかし、システム・エラー・ログや重要でないシステム・チェックなどの重要でないメタデータは、リスク管理を用いて正当化される場合には、完全な捕捉と管理を必要としないかもしれない。

9.1.6 When determining data vulnerability and risk, it is important that the computerized system is considered in the context of its use within the business process. For example, the integrity of results generated by an analytical method utilizing 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 computerized systems, particularly interfaced systems.

9.1.6 データの脆弱性及びリスクを判断する際には、コンピュータ化されたシステムをビジネスプロセスの中で使用されている状況の中で考慮することが重要である。例えば、統合されたコンピュータ・インターフェースを利用する分析方法によって生成された結果の完全性は、試料の準備、システムへの試料重量の入力、データを生成するためのシステムの使用、およびそのデータを使用した最終結果の処理／記録によって影響を受ける。データ・フロー・マップの作成と評価は、コンピュータ化されたシステム、特にインターフェイス化されたシステムのリスクと脆弱性を理解するのに役立つかもしれない。

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.

9.1.7 システム及び/又はソフトウェアに組み込まれている固有のデータインテグリティコ

ントロール、特に現代のデータ管理要件を満たすように設計されたより近代的なシステムよりも悪用されやすい可能性があるものについて考慮するものとする。脆弱性を持つ可能性のあるシステムの例としては、手動記録システム、旧式のセキュリティ対策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、ファイアウォール（外部からの不正なアクセス）や侵入検知・防止システムなどを使用して追加のネットワークセキュリティ保護を必要とするシステムなどがある。

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

9.1.8 コンピュータ化されたシステムの検査においては、査察員は評価の際に会社の専門知識を活用することが推奨される。会社の代表者に、アクセスとナビゲーションを容易にするよう依頼し、指示することは、システムの検査に役立つ。
9.1.9 本ガイダンスは、コンピュータ化された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を提供することを意図している。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 Computerized 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 computerized 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.

9.1.10 本原則は、コンピュータ化されたシステムの提供を外部に委託する場合にも同様に適用される。このような場合、規制対象企業は、外部委託されたサービスが GMP/GDP の要求事項に従って管理・評価されていること、また、適切なデータ管理・整合性管理が双方で理解され、効果的に実施されていることを保証する責任を有する。

9.2 Qualification and validation of computerized systems
9.2.1 The qualification and validation of computerized 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 computerized systems.

9.2 コンピュータ化システムの適格性確認及びバリデーション
9.2.1 コンピュータ化システムの適格性確認及びバリデーションは、関連する GMP/GDP ガイドラインに 従って実施するものとする。

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.

9.2.2 バリデーションだけでは、生成された記録が必ずしも適切に保護されていることを保証するものではなく、バリデーションされたシステムは偶発的または悪意のある手段による損失や改ざんに対して脆弱である可能性がある。したがって、バリデーションは、適切な管理および物理的管理、ならびにユーザーのトレーニングによって補完されるべきである。

9.3 Validation and Maintenance
Item:　System Validation & Maintenance
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.

9.3 バリデーションとメンテナンス
項目: システムのバリデーションとメンテナンス

1. 期待されること

規制対象企業は、システム調達の初期段階、およびシステムとデータのライフサイクル全体を通じて、データ管理と整合性の要件が考慮されていることを保証するために、適切な管理を文書化し、実施しなければならない。規制対象となるユーザに対しては、機能仕様書（FS）及び／又はユーザ要求仕様書（URS）において、データ管理及び完全性の要件を適切に取り扱うべきである。

GMP/GDP に不可欠な機器を購入する際には、購入前にデータインテグリティの管理についてシステムが適切に評価されていることを確認するため、特に注意を払う必要がある。

レガシーシステム（既存の使用中のシステム）は、既存のシステム構成や機能が、適切なデータ管理と完全性の実践に従ったデータの適切な管理を可能にするかどうかを判断するために評価されるべきである。これらのシステムの機能または設計が適切なレベルの管理を提供しない場合、追加の管理を検討し、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, which may allow the manipulation of data with a low probability of detection.

・ Assessments of existing systems should be available and provide an overview of any vulnerabilities and list any additional controls implemented to assure data integrity. Additional controls should be appropriately validated and may include:

o Using operating system functionality (e.g. Windows Active Directory groups) to assign users and their access privileges where system software does not include administrative controls to control user privileges;

o Configuring operating system file/folder permissions to prevent modification/deletion of files when the modification/deletion of data files cannot be controlled by system software; or

o Implementation of hybrid or manual systems to provide control of data generated.

期待値を満たさない場合の潜在的リスク／チェックすべき項目

- DI 要件の検討が不十分なため、データ管理・完全性に関する期待を満たすために必要な基本機能を含まないソフトウェアシステムを購入してしまう可能性がある。

- 査察官は、新しいシステムの導入が、DI の原則を十分に考慮したプロセスに従っているかどうかを確認する必要がある。

- レガシーシステムの中には、データ管理のための適切なコントロールが含まれていないものがあり、これにより、発見される可能性の低いデータ操作が可能になっている場合がある。
- 既存システムの評価を入手し、脆弱性の概要を示し、データの完全性を保証するために実施された追加的な管理策を列挙すべきである。追加の管理策は適切に検証されるべきであり、以下のようなものが考えられます。
o システムソフトウェアがユーザ権限を制御するための管理制御を含んでいない場合に、オペレーティング・システムの機能（例えば、Windows Active Directory グループ）を使用して、ユーザとそのアクセス権限を割り当てる。
o データファイルの変更／削除をシステムソフトウェアで制御できない場合に、ファイルの変更／削除を防止するためにオペレーティングシステムのファイル／フォルダの権限を設定すること。
o 生成されたデータの制御を行うためのハイブリッドシステムまたは手動システムの導入。

2. Expectation
Regulated users should have an inventory of all computerized systems in use. The list should include reference to:
- The name, location and primary function of each computerized system;
- Assessments of the function and criticality of the system and associated data; (e.g. direct GMP/GDP impact, indirect impact, none)
- The current validation status of each system and reference to existing validation documents.
Risk assessments should be in place for each system, specifically assessing the necessary controls to ensure data integrity. The level and extent of validation of controls for data integrity should be determined based on the criticality of the system and process and potential risk to product quality, e.g. processes or systems that generate or control batch release data would generally require greater control than 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 unauthorized changes to critical configuration settings or manipulation of data. All controls should be documented and their effectiveness verified.

Potential risk of not meeting expectations/items to be checked
・ Companies that do not have adequate visibility of all computerized systems in place may overlook the criticality of systems and may thus create vulnerabilities within the data lifecycle.
・ An inventory list serves to clearly communicate all systems in place and their criticality,

ensuring that any changes or modifications to these systems are controlled.
・ Verify that risk assessments are in place for critical processing equipment and data acquisition systems. A lack of thorough assessment of system impact may lead to a lack of appropriate validation and system control. Examples of critical systems to review include:
o systems used to control the purchasing and status of products and materials;
o systems for the control and data acquisition for critical manufacturing processes;
o systems that generate, store or process data that is used to determine batch quality;
o systems that generate data that is included in the batch processing or packaging records; and
o systems used in the decision process for the release of products.

2. 期待されること
規制対象ユーザーは、使用中のすべてのコンピュータシステムの一覧表を持つべきである。このリストには、以下の事項への言及が含まれるべきである。
- 各コンピュータシステムの名称、設置場所、および主な機能。
- システム及び関連データの機能及び重要性の評価（例：GMP/GDP への直接的な影響、間接的な影響、なし
- 各システムの現在のバリデーション状況及び既存のバリデーション文書の参照。
リスクアセスメントは各システムに対して実施されるべきであり、特にデータの完全性を確保するために必要なコントロールを評価する。データの完全性を確保するためのコントロールのレベル及びバリデーションの程度は、システム及びプロセスの重要性並びに製品品質に対する潜在的なリスクに基づいて決定されるべきである。例えば、 バッチリリースデータを生成又は管理するプロセス又はシステムは、一般的に重要性の低いデータ又は 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を必要とするであろう。
また、災害、誤動作、またはシステムが機能しなくなる状況が発生す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。
評価では、重要な構成設定に対する不注意または不正な変更、あるいはデータの操作に対するシステムの脆弱性についても検討する必要がある。すべてのコントロールは文書化され、その有効性が検証されるべきである。

期待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
- 設置されているすべてのコンピュータシステムを十分に把握していない企業は、システムの重要性を見落とし、その結果、データのライフサイクルの中に脆弱性を生み出す可能性がある。
- インベントリー（在庫）リストは、設置されているすべてのシステムとその重要性を明確に伝える役割を果たし、これらのシステムへの変更や修正が確実に管理される。

- 重要な処理装置およ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確認する。システムへの影響が十分に評価されていないと、適切なバリデーションやシステムコントロールが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としては、以下のようなものがある。
o 製品や材料の購入や状態を管理するためのシステム。
o 重要な製造プロセスの制御とデータ取得のためのシステム。
o バッチの品質を決定するために使用されるデータを生成、保存、または処理するシステム。
o バッチ処理または包装の記録に含まれるデータを生成するシステム。
o 製品リリースの決定プロセスに使用されるシステム。

3. Expectation
For new systems, a Validation Summary Report for each computerized system (written and approved in accordance with Annex 15 requirements) should be in place and state (or provide reference to) at least the following items:
- Critical system configuration details and controls for restricting access to configuration and any changes (change management).
- A list of all currently approved normal and administrative users specifying the username and the role of the user.
- Frequency of review of audit trails and system logs.
- Procedures for:
o creating new system user;
o modifying or changing privileges for an existing user;
o defining the combination or format of passwords for each system
o reviewing and deleting users;
o back-up processes and frequency;
o disaster recovery;
o data archiving (processes and responsibilities), including procedures for accessing and reading archived data;
o approving locations for data storage.
- The report should explain how the original data are retained with relevant metadata in a form that permits the reconstruction of the manufacturing process or the analytical activity.
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.

3. 期待すること
新規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概要報告書（附属書15 の要求事項に従って作成され、承認されたもの）が整備されており、少なくとも以下の項目が記載されている（または参照されている）必要がある。
- 重要なシステム構成の詳細と、構成および変更点へのアクセスを制限するための管理（変更管理）。
- 現在承認されているすべての通常ユーザおよび管理ユーザのリスト（ユーザ名およびユーザの役割を明記したもの
- 監査証跡およびシステムログのレビューの頻度。
- 以下の手順
o 新しいシステムユーザーの作成。
o 既存のユーザーの特権を修正または変更する。
各システムのパスワードの組み合わせまたはフォーマットの定義
o ユーザーのレビューおよび削除
バックアップのプロセスおよび頻度
o ディザスタリカバリ
保管されたデータへのアクセスと読み取りの手順を含む、データの保管（プロセスと責任）。
o データ保管場所の承認。
- 報告書では、製造プロセスや分析活動の再構築を可能にする形で、オリジナルデータが関連するメタデータとともにどのように保持されているかを説明する必要がある。
既存のシステムについては、上記の要求事項を明記した文書が入手可能であるべきであるが、バリデーション概要報告書盛り込む必要はない。
これらの概要報告書の文書は、規制対象となるユーザーが必要に応じて維持・更新すべきである。

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. authorization to generate data should be separate to authorization 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 authorized persons and is not used for routine operations.
・ Check the procedures for granting, modifying and removing access to computerized

systems to ensure these activities are controlled.

Check the currency of user access logs and privilege levels, there should be no unauthorized users to the system and access accounts should be kept up to date.
・ There should also be restrictions to prevent users from amending audit trail functions and from changing any pre-defined directory paths where data files are to be stored.

期待を満たさない場合の潜在的リスク／チェックすべき項目
- バリデーションシステム及び報告書が、GMP/GDP の要求事項に従い、また ALCOA の原則を考慮して、データインテグリティの要求事項を具体的に扱っていることを確認する。
- システム構成及び職務の分離（例：データを生成する権限とデータを検証する権限は別であるべきである）は、バリデーションに先立って定義され、テストの際に有効であることが確認されるべきである。
- システムへの修正または変更が制限され、変更管理の対象となっていることを確認するために、システムへのアクセスに関する手順を確認すること。
- システム管理者のアクセスが権限のある者に限定され、日常業務に使用されていないことを確認すること。
- コンピュータ化されたシステムへのアクセスを許可、変更、削除するための手順を確認し、これらの活動が管理されていることを確認する。

ユーザーのアクセスログや権限レベルの最新性を確認する。システムに未承認のユーザーがいないこと、アクセスアカウントが最新の状態に保たれていることが望ましい。
- また、ユーザーが監査証跡機能を修正したり、データファイルを保存するために事前に定義されたディレクトリパスを変更したりすることを防ぐための制限を設ける必要がある。

4. Expectation
Companies should have a Validation Master Plan in place that includes specific policies and validation requirements for computerized systems and the integrity of such systems and associated data.
The extent of validation for computerized systems should be determined based on risk. Further guidance regarding assessing validation requirements for computerized 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 computerized systems is conducted. Appropriate validation data should be available for systems already in-use.

Computerized 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 computerized 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 computerized system. For critical and/or more complex systems, detailed verification testing is required during IQ, OQ & PQ stages.

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.

4. 期待すること
企業は、コンピュータ化されたシステムとそのシステムと関連するデータの完全性に関する具体的なポリシーとバリデーション要件を含むバリデーションマスタープランを実施する必要がある。
コンピュータ化されたシステムのバリデーションの範囲は、リスクに基づいて決定されるべきである。コンピュータ化されたシステムのバリデーション要件の評価に関する詳細なガイダンスは、 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、受入基準への適合性を確認するためのテストを行うべきである。
コンピュータ化されたシステムのプロスペクティブ（予測）バリデーション（PV）を実施

することが期待される。既に使用されているシステムについては、適切なバリデーションデータを入手できること。
コンピュータ化されたシステムのバリデーションは、必要に応じてURS、DQ、FAT（工場受入れ試験）、SAT（現地受入試験）、IQ、 OQ及びPQ試験を実施し、GMP Annex 15に基づいて設計されるべきである。
適格性確認試験の方法は、バリデーション対象の特定のシステムに合わせて調整されるべきであり、規制対象となるユーザーによって正当化されるべきである。適性評価には、設計適格性評価（DQ）、設置適格性評価（IQ）、運用適格性評価（OQ）、及び性能適格性評価（PQ）が含まれる。特に、データの品質や整合性が問題となる以下の分野に挑戦するために、特定のテストを設計する必要がある。
特に、データの品質や完全性が危険にさらされている分野に挑戦するために、特定のテストを設計する必要がある。
会社は、コンピュータ化されたシステムがその意図された用途に適合していることを確認しなければならない。したがって、企業は、ベンダーの適格性評価パッケージのみに依存してはならない。検証作業には、通常の使用および意図された使用を反映した操作中にデータの完全性が維持されることを確認するための特定のテストを含めるべきである。
テストの数はリスクアセスメントによって決定されるべきであるが、重要な機能性は少なくとも特定され、テストされるべきである。例えば、基本的なアルゴリズムやロジックセットに基づく特定のPLCやシステムでは、機能テストによってコンピュータシステムの信頼性が十分に保証される可能性がある。重要なシステムや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になる。

期待値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規定が含まれていることを確認する。バリデーション報告書は、データインテグリティの原則を具体的に取り上げ、適切なコントロールが行われていることを設計とテストによって実証する必要がある。
- バリデーションが行われていないシステムは、ユーザーのアクセスやシステム構成によってデータの修正が可能となるため、データの完全性に関して重大な脆弱性をもたらす可能性がある。
- エンドユーザテストには、ソフトウェアがベンダーの要求事項を満たしているだけでなく、意図した用途に適合していることを実証するために設計されたテストスクリプトが含まれていることを確認する。

5. Expectation
Periodic System Evaluation
Computerized 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 computerized systems considering the cumulative effect of changes to the system since last review. The assessment performed should be documented.

5. 期待すること
定期的なシステム評価
コンピュータ化されたシステムは、データインテグリティコントロールに関する継続的なコンプライアンスを確保するために、定期的に評価されるべきである。評価には、逸脱、変更（変更の累積的影響を含む)、アップグレードの履歴、パフォーマンス及びメンテナンスを含み、これらの変更がデータ管理及び完全性の管理に有害な影響を与えていないかどうかを評価する必要がある。
再評価の頻度は、前回のレビュー以降にシステムに加えられた変更の累積的な影響を考慮し、コンピュータ化されたシステムの重要性に応じたリスクアセスメントに基づくべきである。実施された評価は文書化されるべきである。

Potential risk of not meeting expectations/items to be checked
・ Check that re-validation reviews for computerized 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.

期待を満たさない潜在的なリスク／チェックすべき項目
- コンピュータ化されたシステムの再検証レビューがバリデーションスケジュールの中に概説されていることを確認する。
- システムが定期的なレビューを受けていること、特にデータの完全性に関する潜在的な脆弱性に関して検証すること。
- 現行のソフトウェア/ハードウェアの限界など、特定された問題は、適時に対処され、是正措置、予防措置、暫定的な管理が利用可能であり、特定されたリスクを管理するために実施されるべきである。

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 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.

6. 期待すること

オペレーティングシステムおよ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適時に更新されるべきであり、古いプラットフォームから新しいプラットフォームへのアプリケーションの移行は、システムで生成されたデータの管理および整合性に影響を与える可能性のあるサポートされない状態にプラットフォームが到達する前に、事前に計画して実施されるべきである。

システムで生成されたデータの管理と完全性に影響を与える可能性がある。

データのセキュリティを維持するために、オペレーティングシステム及びネットワークコンポーネントのセキュリティパッチは、ベンダーの推奨に従い、管理された方法でタイムリーに適用されるべきである。セキュリティパッチの適用は、変更管理の原則に基づいて行う必要がある。

変更管理の原則に基づいて行う必要がある。

サポートされていないオペレーティングシステムが維持されている場合、すなわち、ベンダーのサポートが終了した後も古いオペレーティングシステムが使用されていたり、サポートされているバージョンにセキュリティパッチが適用されていない場合は、そのシステム（サーバ）をネットワークの他の部分から可能な限り隔離する必要がある。残りのインター

フェイスや他の機器とのデータ転送は、サポートされていないオペレーティングシステムに起因する脆弱性が悪用されないように、慎重に設計、設定、および認定されるべきである。サポートされていないシステムへのリモートアクセスは、固有の脆弱性リスクがあるため、慎重に評価する必要がある。

Potential risk of not meeting expectations/items to be checked

・ 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

- システムの更新が管理された方法でタイムリーに行われていることを確認する。古いシステムは、適切なデータインテグリティコントロールが統合されているかどうか、あるいは（統合されたコントロールが不可能な場合）適切な管理コントロールが実装されていて有効であるかどうかを判断するために、批判的にレビューされるべきである。

9.4 Data Transfer

Item: Data transfer and migration

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 minimize data integrity risks. Verification methods may include the use of: o Secure transfer

o Encryption

o Checksums

Where applicable, interfaces between systems should be designed and qualified to include an automated transfer of GMP/GDP data. Potential risk of not meeting expectations/items to be checked

・ Interfaces between computerized 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 computerized 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.

9.4 データ転送
項目　　データの転送と移行
1. 期待されること
正しく完全なデータの転送を保証するために、バリデーションの際にインターフェースを評価し、対処すべきである。
インターフェースには、データ整合性のリスクを最小化するために、データの正確かつ安全な入力及び処理のための適切な組み込みチェックを含めるべきである。検証方法には以下の方法が含まれる：
o 安全な転送
o 暗号化
o チェックサム（検査合計：誤り検出符号）
該当する場合、システム間のインターフェースは、GMP/GDP データの自動転送を含むように設計され、適格でなければならない。期待値を満たさない場合の潜在的リスク／チェックすべき項目
- コンピュータシステム間のインターフェースは、転送プロセス中にデータが不注意で失われたり、修正されたり、誤って転記されたりするリスクがある。
- データが安全な場所／データベースに直接転送され、（改ざんされる可能性のある）ローカルドライブから単にコピーされないことを確認する。
- 最終的な保管場所またはデータ処理場所に移動する前に、ローカルのコンピュータ化されたシステム（機器のコンピュータなど）に一時的にデータを保管すると、データが削除または操作される可能性がある。これは「スタンドアロン」（非ネットワーク型）システムの場合に特に危険である。データを最初に保存する環境に、適切な DI コントロールがあることを確認する。
- 適切に設計された適格な自動データ転送は、人間が行う手動の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 available as a backup media in order to have the opportunity to read the archived data in case of an investigation.

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.

2. 期待すること

システムソフトウェア（オペレーティングシステムを含む）をインストールまたは更新する場合、ユーザーは、既存のデータおよびアーカイブされたデータが新しいソフトウェアで読み取れることを確認する必要があります。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かもしれません。

新しいソフトウェアの新しいデータ形式への変換が不可能な場合は、古いソフトウェアを維持する必要がある。例えば、1 台のコンピュータまたはその他の技術的ソリューションにインストールし、調査の際にアーカイブされたデータを読む機会を持てるように、バックアップメディアとしても利用できるようにしておく。

期待を満たさない場合の潜在的リスク／チェックすべき項目

- データのライフサイクルを通じて、データが元の形で読めることが重要であり、したがってユーザはデータの可読性を維持する必要があり、そのためには後継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の移行は、文書化されたプロトコルに従って、管理された方法で実行されるべきであり、データの完全な移行の適切な検証を含むべきである。

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 unauthorized changes to critical configuration settings or manipulation of data. All controls to mitigate risk should be documented and their effectiveness verified. It is recognized that the need to maintain accessibility may require migration to a file format that loses some attributes and/or dynamic data functionality.

3. 期待すること
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、データアクセスの目的でソフトウェアを維持することを考慮しなければならない（特定の保存要件に応じて可能な限り長く）。
これは、仮想環境でソフトウェアを維持することで実現できる。
レガシーデータの年代が上がるにつれて、データの「真のコピー」属性を可能な限り保持する代替ファイル形式への移行が必要になる場合がある。
元のデータの機能を完全に維持したまま移行することが技術的に不可能な場合は、リスクと時間経過に伴うデータの重要性に基づいてオプションを評価する必要がある。移行ファイル形式は、長期的なアクセス性と動的なデータ機能（データ照会、トレン ド、再処理など）の低下の可能性との間のリスクバランスを考慮して選択されるべきである。 また、リスクアセスメントでは、重要な構成設定に対する不注意または不正な変更やデータ操作に対する システムの脆弱性を検討する必要がある。リスクを軽減するためのすべての管理策を文書化し、その有効性を検証しなければならない。アクセシビリティを維持する必要性から、一部の属性や動的なデータ機能を失ったファイル形式への移行が必要になる場合があることを認識している。
ファイルフォーマットへの移行が必要になる場合がある。

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 authorized persons, etc.) are in place. All controls should be documented and their effectiveness verified.

期待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
- ソフトウェアが仮想環境で管理されている場合、ソフトウェアを管理するための適切な手

段（バリデーションの状態、権限のある者によるアクセスコントロールなど）が実施されていることを確認する。すべてのコントロールを文書化し、その有効性を検証すること。

9.5 System security for computerized systems
Item:　System security
1. Expectation
User access controls shall be configured and enforced to prohibit unauthorized access to, changes to and deletion of data. The extent of security controls is dependent on the criticality of the computerized system.

9.5 コンピュータ化システムのシステムセキュリティ
項目：システムセキュリティ
1. 期待されること
データへの不正なアクセス、変更、および削除を禁止するために、ユーザのアクセス制御が設定され、実施されること。セキュリティ管理の程度は、コンピュータ化されたシステムの重要性に依存する。

For example:
- Individual Login IDs and passwords should be set up and assigned for all staff needing to access and utilize 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.
- Input of data and changes to computerized records should be made only by authorized personnel. Companies should maintain a list of authorized 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 computerized 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 computerized 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:
o User identification
o User access role
o Date and time of the attempted login, either in local time or traceable to local time
o Session length, in the case of successful logins
- 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 organizations (e.g. Information Technology administrators) should serve as the system administrators and have enhanced permission levels.
- For smaller organizations, 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 authorized 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.
- Computerized systems giving access to GMP/GDP critical data or operations should have an inactivity logout, which, either at the application or the operating system level, logs out a

user who has been inactive longer than a predefined time. The time should be shorter, rather than longer and should typically be set to prevent unauthorized 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.
Potential risk of not meeting expectations/items to be checked
・ Check that the company has taken all reasonable steps to ensure that the computerized 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 computerized 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 computerized systems support only a single user login or limited numbers of user logins. Where no suitable alternative computerized system is available, equivalent control may be provided by third party software, or a paper based method of providing traceability (with version control). The suitability of alternative systems should be justified and documented.
Increased data review is likely to be required for hybrid systems.
・ Inspectors should verify that a password policy is in place to ensure that systems enforce good password rules and require strong passwords. Consideration should be made to using stronger passwords for systems generating or processing critical data.
・ Systems where a new password cannot be changed by the user, but can only be created by the admin, are incompatible with data integrity, as the confidentiality of passwords cannot be maintained.
・ Check that user access levels are appropriately defined, documented and controlled. The use of a single user access level on a system and assigning all users this role, which per definition will be the admin role, is not acceptable.
・ Verify that the system uses authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computerized system input or output device, alter a record, or perform the operation at hand.

例えば、以下のようなものがある。
- 特定の電子システムへのアクセスおよび利用を必要とするすべてのスタッフに対して、個別のログイン ID およびパスワードを設定し、割り当てるべきである。ログイン認証情報を共有すると、アクティビティを実行した個人への追跡ができない。このため、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、禁止されるべきである。ログインプロファイル、構成及びパスワードの形式が明確に定義され、意図された通りに 機能することを確実にするために、電子システムの検証中にログインパラメータを検証すべき である。
- データの入力およびコンピュータ化された記録の変更は、権限を与えられた者のみが行うべきである。企業は、使用中の各電子システムについて、権限を有する者のリストとそのアクセス権を維持すべきである。
- システムが効果的に保護されていることを保証するために、パスワードの形式と使用に関して適切な管理を行うべきである。- システムへのアクセスが最初に許可された時点で、システムは、通常のパスワード規則に従って、ユーザが新しいパスワードを作成できるようにすべきである。
- システムは、異なるユーザ・アクセス・ロール（レベル）をサポートし、ロールの割り当ては、最小特権ルール、すなわち、あらゆる職務に必要な最小限のアクセス・レベルを割り当てることに従うべきである。
単純なシステムでは、最低限、通常ユーザと管理者ユーザを持つべきであるが、複雑なシステムでは、アクセス制御を効果的にサポートするために、通常、より多くのレベルのユーザ（例えば、階層）が必要となる。
- GMP/GDP にとって重要なアプリケーションを実行するためのコンピュータ化されたシステムおよびインフラに対する管理者アクセス権の付与は、厳密に管理されなければならない。管理者アクセス権は、システム上の通常のユーザーに与えてはならない（すなわち、職務の分離）。
- 通常のユーザは、システムクロック、ファイル削除機能など、コンピュータ化されたシステムの重要な側面にアクセスしてはならない。
- システムは、システムに実際にアクセスできるユーザのリストを、ユーザの識別と役割を含めて生成できるべきである。ユーザ・リストには、特定の個人の識別を可能にする名前または一意の識別子が含まれるべきである。このリストは、定期的なユーザレビューの際に使用されるべきである。
- システムは、以下を含む、成功したログイン試行と失敗したログイン試行のリストを生成することができなければならない。
o ユーザ識別
o ユーザのアクセス・ロール
o ログイン試行の日付と時刻（現地時間または現地時間から追跡可能なもの）。
o 成功したログインの場合、セッションの長さ
- ユーザーのアクセス制御は、厳密な職務分離を保証するものでなければなりません（すなわち、システム上で通常の作業を行っているすべてのユーザーは、通常のアクセス権のみを持つべき）。通常、昇格したアクセス権を持つユーザ（admin など）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から独立しているべきであり、電子システムで生成された、又は利用可能なデータの結果に関与又は関心を持たない。
例えば、QC スーパーバイザー及びマネージャーは、各自のラボの電子システム（HPLC、GC、UV-Vis 等）のシステム管理者として割り当てられるべきではない。一般的には、品質及び生産組織以外の個人（例：情報技術管理者）がシステム管理者を務めるべきである。
技術管理者など）がシステム管理者となり、強化された権限レベルを持つべきである。
- 小規模な組織では、品質部門または生産部門で指名された人がシステム管理者としてアクセス権を持つことが許容される場合がある。しかしこのような場合、管理者アクセスは日常業務の実行に使用すべきではなく、ユーザーは日常業務の実行のために 2 番目の制限されたアクセス権を持つべきである。このような場合、実施されたすべての管理者活動は、品質システムの中で記録され、承認されなければならない。
- 新たなユーザーやユーザーの新たな権限の要求は、適切な担当者（ラインマネージャーやシステム所有者など）によって承認され、標準的な手順に従って追跡可能な方法でシステム管理者に転送されるべきである。
- GMP/GDP の重要なデータや業務へのアクセスを可能にするコンピュータ化されたシステムは、アプリケーションまたはオペレーティングシステムレベルで、事前に定義された時間を超えて活動していないユーザーをログアウトさせる非活動時ログアウト機能を持つべきである。この時間は長くするのではなく短くし、通常はシステムへの不正アクセスを防ぐために設定します。非活動時のログアウトを有効にすると、システムはユーザに通常の認証手続きを要求する。
再度ログインするための通常の認証手順を要求するべきである。
期待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
- 使用中のコンピュータ化されたシステムが安全であり、故意または不注意による変更から保護されていることを保証するために、会社があらゆる合理的な手段を講じていることを確認する。
- 物理的・管理的にセキュリティが確保されていないシステムは、データの整合性に問題が生じる可能性がある。検査機関は、システム・セキュリティを管理する検証済みの手順が存在し、コンピュータ化されたシステムが有効な状態で維持され、操作から保護されていることを確認すべきである。
- 個々のユーザのログイン ID が使用されていることを確認すること。システム構成上、個別のユーザ・ログイン ID の使用が可能な場合は、これを使用すること。
- レガシーのコンピュータ化されたシステムの中には、単一のユーザ・ログインまたは限られた数のユーザ・ログインしかサポートしていないものがあることが認められている。適切なコンピュータ化されたシステムが利用できない場合、同等の管理はサードパーティのソフト ウェアによって提供されるか、トレーサビリティーを提供する紙ベースの方法（バージョン管理を 含む）によって提供される。代替システムの適合性は正当化され、文書化さ

れなければならない。
ハイブリッド・システムでは、データのレビューを強化することが必要である。
- 査察官は、システムが適切なパスワード規則を実施し、強力なパスワードを必要とすることを保証するために、パスワード・ポリシーが実施されていることを確認すべきである。重要なデータを生成または処理するシステムには、より強力なパスワードを使用することを検討すべきである。
- 新しいパスワードをユーザが変更できず、管理者のみが作成できるシステムは、パスワードの機密性を維持できないため、データインテグリティと相容れない。
- 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確認する。システムで単一のユーザ・アクセス・レベルを使用し、すべてのユーザにこのロール（定義上は admin ロール）を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、許可された個人のみがシステムを使用したり、記録に電子的に署名したり、操作やコンピュータ化されたシステムの入力または出力デバイスにアクセスしたり、記録を変更したり、手元の操作を実行したりできるようにしていることを確認する。

2. Expectation
Computerized systems should be protected from accidental changes or deliberate manipulation. Companies should assess systems and their design to prevent unauthorized changes to validated settings that may ultimately affect data integrity. Consideration should be given to:
- The physical security of computerized system hardware:
o Location of and access to servers;
o Restricting access to PLC modules, e.g. by locking access panels.
o Physical access to computers, servers and media should be restricted to authorized individuals. Users on a system should not normally have access to servers and media.
- Vulnerability of networked systems from local and external attack;
- Remote network updates, e.g. automated updating of networked systems by the vendor.
- Security of system settings, configurations and key data. Access to critical data/operating parameters of systems should be appropriately restricted and any changes to settings/configuration controlled through change management processes by authorized personnel.
- The operating system clock should be synchronized with the clock of connected systems and access to all clocks restricted to authorized 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 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.
Potential risk of not meeting expectations/items to be checked
・ Check that access to hardware and software is appropriately secured, and restricted to authorized 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.

2. 期待すること
コンピュータ化されたシステムは、偶発的な変更や意図的な操作から保護されるべきである。企業は、最終的にデータの完全性に影響を与える可能性のある、有効な設定に対する不正な変更を防止するために、システムとその設計を評価しなければならない。
以下の点を考慮すべきである。
- コンピュータ・システム・ハードウェアの物理的セキュリティ
o サーバーの設置場所およびサーバーへのアクセス。
o アクセスパネルをロックするなどして、PLC（機械を自動的に制御する装置。Programmable Logic Controller）モジュールへのアクセスを制限する。
o コンピュータ、サーバ、メディアへの物理的なアクセスは、許可された個人に制限されるべきである。システム上のユーザは、通常、サーバおよびメディアへのアクセス権を持つべきではない。
- ネットワークシステムのローカルおよび外部からの攻撃に対する脆弱性。
- ベンダーによるネットワークシステムの自動更新など、リモートネットワークの更新。
- システム設定、構成および主要データのセキュリティ。システムの重要なデータや動作パラメータへのアクセスを適切に制限し、権限のある担当者による変更管理プロセスを通じ

て設定/構成の変更を制御すること。
- オペレーティングシステムのクロックは、接続されているシステムのクロックと同期させ、すべてのクロックへのアクセスを権限のある担当者に制限すること。
- 侵入防止および検知システムを含む、適切なネットワークセキュリティ対策を適用すること。
- 重要なデータやオペレーションを保護するために、ファイアウォールを設定すること。
ポートオープン（ファイアーウォールのルール）は、最小特権ポリシーに基づき、ファイアーウォールのルールを可能な限り厳しくすることで、許可されたトラフィックのみを許可するようにすべきである。(特定のポート番号のみアクセス可能)
規制対象となるユーザは、ネットワークセキュリティ対策の継続的な適切性と有効性について定期的なレビューを行い(例えば、潜在的なセキュリティ上の弱点を特定するためにITインフラストラクチャのネットワーク脆弱性スキャンを使用するなど)、オペレーティングシステムが最新のセキュリティ対策で維持されていることを確認する必要がある。

期待を満たさない場合の潜在的リスク／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、許可された人員に制限されていることを確認する。
- 適切な認証方法が実施されていることを確認する。これらの方法にはユーザーID とパスワードが含まれるべきであるが、他の方法も可能であり、必要となる場合もある。ただし、ユーザを確実に識別できることが重要である。
- インターネット経由で利用可能な重要データを含むシステムへのリモート認証の場合、パスコー ド・トークンやバイオメトリクスの使用など、追加の認証技術が採用されていることを検証する。
- システムの主要な動作パラメータへのアクセスが適切に制御されていること、及び必要に応じて、 GMP/GDP ステップの重要なシーケンスにおけるイベント及びパラメータの正しい順序がシステムに よって強制されていることを検証すること。
システムがイベントやパラメータの正しい順序を強制することを検証すること。

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 unauthorized 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 computerized systems from attempted attacks and malware.
Potential risk of not meeting expectations/items to be checked
・ Inadequate network security presents risks associated with vulnerability of systems from unauthorized access, misuse or modification.
・ Check that appropriate measures to control network access are in place. Processes should be in place for the authorization, 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.

3. 期待すること
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し、防止するための適切な方法が含まれるべきである。
実施するネットワーク保護のレベルは、データリスクの評価に基づくべきである。
不正なアクセスを防止するためにファイアウォールを使用し、そのルールが必要に応じて制限的に設定され、許可されたトラフィックのみを許可することを保証するために、仕様に照らして定期的なレビューを行うべきである。このレビューは文書化されるべきである。
ファイアウォールは、データやコンピュータシステムを未遂の攻撃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/検出システムで補完されるべきである。

期待値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
- ネットワークセキュリティが不十分な場合、不正なアクセス、誤用、改変などによるシステムの脆弱性に関連するリスクがある。
- ネットワークアクセスを制御するための適切な手段が実施されていることを確認する。アクセスの承認、監視、削除のためのプロセスが整備されていること。
- 脅威を防止し、ネットワークへの侵入の試みを検出するようにシステムを設計し、これらの対策を設置、監視、維持する必要がある。
- ファイアウォールのルールは通常、サーバーのメンテナンスなどにより一時的にポートが開かれるなど、時間の経過とともに変更される。見直しをしないと、ファイアウォール・ルールが時代遅れになり、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生まれ

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.
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.

4. 手書き署名の代わりに使用される電子署名は、その真正性と電子署名を行った特定の人物へのトレーサビリティを確保するための適切な管理を行うべきである。
例えば、署名された記録に後から変更が加えられた場合、その記録には修正内容が表示され、署名されていないと表示されるべきである。
電子署名機能を使用する場合は、署名が適用された日時を自動的に記録する。
高度な形式の電子署名の使用が一般的になってきている（例：バイオメトリクスの使用が企業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。
期待を満たさない場合の潜在的リスク／チェックすべき項目
- 電子署名が適切に検証されていること、スタッフへの発行が管理されていること、電子署名が常に個人に容易に帰属することを確認する。
- 電子署名が付与された後にデータに変更があった場合、データを再度確認して再署名するまで署名は無効となる。

5. Restrictions on use of USB devices
For reasons of system security, computerized systems should be configured to prevent vulnerabilities from the use of USB memory sticks and storage devices on computer clients

and servers hosting GMP/GDP critical data. If necessary, ports should only be opened for approved purposes and all USB devices should be properly scanned before use.
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.
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 authorized users and measures to screen USB devices before use should be in place.

5. USB デバイスの使用制限について
システムセキュリティの観点から、GMP/GDP に関わる重要なデータが保存されているクライアントやサーバーにおいて、USB メモリや記憶装置が使用されても脆弱性が生じないようにコンピュータシステムを設定すること。必要に応じて、許可された目的のためにのみポートを開き、すべての USB デバイスは使用前に適切にスキャンされるべきである。
GMP/GDP のデータを保管する会社のコンピュータのクライアントおよびサーバーでの私的な USB デバイス（フラッシュドライブ、カメラ、スマートフォン、キーボードなど）の使用、または私的なコンピュータでの会社の USB デバイスの使用は、セキュリティ違反を防ぐために管理されるべきである。
期待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
- これは、USB デバイスがキーボードなどの他の外部デバイスのふりをしてコンピュータを騙すことができ、実行可能コードを含んで起動することができるというオペレーティングシステムの脆弱性が知られている場合には特に重要である。
- 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管理を行い、使用前に USB デバイスをスクリーニングするための対策を講じるべきである。

9.6 Audit trails for computerized systems
Item:　Audit Trails
1. Expectation
Consideration should be given to data management and integrity requirements when purchasing and implementing computerized 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 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 unauthorized 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 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).
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) 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 Authorized Person.
・ Clear details of which data are critical, and which changes and deletions should be recorded (audit trail) should be documented.

9.6 コンピュータ化システムの監査証跡
項目　監査証跡
1. 期待すること
コンピュータシステムを購入・導入する際には、データの管理と整合性に関する要件を考慮する必要がある。
企業は、適切な電子監査証跡機能を含むソフトウェアを選択すべきである。
企業は、古いシステムを購入してアップグレードする際には、電子的な監査証跡機能を備えたソフトウェアを導入するよう努めるべきである。
非常に単純なシステムの中には、適切な監査証跡を持たないものがあることは認識しているが、データの真実性を確認するための代替手段を実施すべきである。例えば、管理手順、二次的なチェックとコントロールなどである。ハイブリッド・システムに関しては、9.10 項に追加のガイダンスがある。
監査証跡の機能は、各手動操作に関連する重要なデータのすべての変更及び削除が記録され、 ALCOA+の原則を満たしていることを確認するために、システムの検証時に検証されるべきである。
規制対象ユーザーは、システム内の監査証跡の性質と機能を理解し、各監査証跡の GMP/GDP 関連性を判断し、重要かつ GMP/GDP 関連のデータに対する監査証跡の正しい管理と設定を確実にするために、 適性評価の際に異なる監査証跡の評価を行うべきである。この作業は、どの特定の監査証跡および監査証跡内のどの項目が重要であるかを判断す

る上で重要である。
この作業は、どの特定の証跡および証跡内のどの項目が重要であるかを判断するために重要であり、定められた頻度でレビューを行う。例えば、このような評価に基づく監査証跡のレビューでは、以下の点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記録の入力やデータを特定し、レビューする。
- 例外的なレビュー：異常な活動や不正な活動に焦点を当てる。
- パラメーター／データの変更を可能にする制限があるシステム、または活動が修正可能なままになっているシステム
- 注：パラメータ／データの変更を防止する権限設定や、構成設定の変更を防止するアクセス制限を持つ、よく設計されたシステムでは、関連する監査証跡を詳細に調査する必要がない場合がある。
監査証跡の機能は常に有効であり、ロックされていて、機能の停止、削除、変更ができないようにすべきである。管理者ユーザが監査証跡機能を無効化、削除、または修正することが可能な場合は、監査証跡にその旨の自動入力を行うべきである。
企業は、監査証跡で必要とされるデータを決定するための方針及びプロセス、並びにリスク管理の原則に従った監査証跡のレビューを概説する手順を実施しなければならない。
各操作に関連する重要な監査証跡は、操作に関連する他のすべての記録と一緒に、重要なデータ及びその変更が許容されることを確認するために、操作の完了のレビューの前に（例えば、バッチリリースの前に）独立してレビューされるべきである。このレビューは、起点となる部門が行うべきであり、必要に応じて、自己点検や調査活動などの際に品質ユニットが検証する。
重要でない監査証跡のレビューは、事前に定義された頻度でシステムレビュー中に実施することができる。このレビューは、起点となる部門が実施すべきであり、必要に応じて品質ユニットが検証する（例：バッチリリース時、自主検査又は調査活動時)。
期待値を満たさない場合の潜在的リスク／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、およびシステム内のすべての活動、変更、およびその他のトランザクションが、関連するすべてのメタデータとともに記録されていることを示すべきである。
- 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（統合されたシステムまたは有効な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）システムが利用可能になるまで、データへの変更を証明するための紙ベースの記録が許容される場合がある。このようなハイブリッドシステムは、PIC/S GMP ガイドの附属書 11 に記載されているような統合された監査証跡と同等のものを達成する場合には認められる。
- 監査証跡を適切にレビューしないと、操作された又は誤ったデータが品質ユニット及び／

又 は認定者によって誤って受け入れられる可能性がある。
- どのデータが重要で、どのような変更や削除を記録（監査証跡）すべきか、明確な詳細を文書化すること。

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 time ;
- why the action was taken (reason); and
- in the case of changes or modifications to data, the name of any person authorizing 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 computerized 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.

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 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.

2. 期待すること
利用可能な場合は、電子ベースのシステムの監査証跡機能を評価し、監査目的でデータの取得、削除、上書き、変更に関連する重要な活動を記録するように適切に設定すべきである。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されたプロセスを記録するように設定されるべきである。
システムは、電子記録を作成、変更、または削除するエントリおよびアクションの日時を独立して記録するために、コンピュータで生成された安全なタイムスタンプ付きの監査証跡を提供する必要がある。

監査証跡には、以下のパラメータが含まれること。
- アクションを行ったユーザーの詳細。
- どのようなアクションが発生し、変更され、新旧の値を含む。
- アクションがいつ行われたか（日付と時間を含む）。
- アクションが行われた理由（理由）、および
- データの変更または修正の場合は、変更を承認した人物の名前。

監査証跡は、電子記録の作成、変更、または削除に関連するイベントの経過を再構築できるものでなければならない。
システムは、監査証跡の電子コピーを印刷して提供することができなければならない。また、オンラインでシステムを閲覧する場合でも、ハードコピーで閲覧する場合でも、監査証跡を意味のある形式で利用できるようにしなければならない。
可能であれば、監査証跡は、コンピュータ化されたシステムに見られる動的な機能（例：検索機能、表計算ソフトなどへのデータのエクスポート機能）を保持するべきである。
注：監査証跡を、PQS に基づいて変更を適切に管理・承認する必要のある変更管理システムと混同してはならない。

期待値を満たさないことによる潜在的リスク／チェックすべき項目
- すべての重要かつ関連する情報が確実に取得されるよう、監査証跡の形式を検証する。

- 監査証跡には以前のすべての値が含まれるべきであり、記録の変更によって以前に記録された情報が上書きされたり、不明瞭になったりしてはならない。
- 監査証跡の記録は、活動の実際の時間を反映した真の時間で記録されるべきである。多数の連続したやりとりに対して同じ時間を記録するシステムや、すべてのやりとりが完了した後にのみ監査証跡のエントリを作成するシステムは、特に各個別のやりとりやシーケンスが重要である場合、データの整合性に対する期待に準拠していない可能性がある。
添加の順番が重要なプロセスパラメータ（CPP）である場合、各添加はタイムスタンプ付きで個別に記録されるべきである。添加の順番が CPP でない場合は、4 つの材料の添加を 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することができる。

9.7 Data capture/entry for computerized systems
Item:　Data capture/entry
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 authorized 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 computerized means.
- Changes to entries should be captured in the audit trail and reviewed by an appropriately authorized and independent person.
For automated data capture: (refer also to table 9.3)
- The interface between the originating system, data acquisition and recording systems should be validated to ensure the accuracy of data.
- Data captured by the system should be saved into memory in a format that is not vulnerable to manipulation, loss or change.
- The system software should incorporate validated checks to ensure the completeness of data acquired, as well as any relevant metadata associated with the data.
Potential risk of not meeting expectations/items to be checked
・ Ensure that manual entries of critical data made into computerized 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.

9.7 コンピュータ化システムのためのデータ取り込み／入力
項目　データキャプチャー（データの記録・保存）/エントリー（入力）
1. 期待されること
システムは、手動または自動のいずれかの方法で取得されたデータを正しく取り込むように設計されるべきである。
手動入力の場合
- 重要なデータの入力は、権限のある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、および入力が行われた日時を記録すべきである。
- データはソフトウェアによって制御される指定のフォーマットで入力されるべきであり、検証活動は無効なデータフォーマットがシステムによって受け入れられないことを検証するべきである。
- 重要なデータを手動で入力した場合は、第 2 のオペレータによる検証、または検証されたコンピュータによる検証のいずれかを行うこと。
- 入力内容の変更は、監査証跡に記録し、適切な権限を持つ独立した人物が確認すること。
自動データ収集の場合（表 9.3 も参照のこと）
- データの正確性を確保するために、発信システム、データ収集・記録システム間のインター フェースを検証すること。
- システムによって取り込まれたデータは、操作、紛失、変更に対して脆弱ではない形式でメモリに保存されるべきである。
- システムのソフトウェアには、取得したデータの完全性、およびデータに関連するメタデータを確認するための有効なチェック機能が組み込まれていること。
期待値を満たさない場合の潜在的リスク／チェックすべき項目
- コンピュータ化されたシステムに重要なデータを手動で入力する際には、適切な二次チェックが行われるようにする。
- 自動データ収集を使用しているシステムの検証記録を確認し、データの検証および整合性を確保する。例えば、自動保存機能が検証されているため、ユーザーが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が生成される可能性がないかどうかを検証する。

2. Expectation
Any necessary changes to data should be authorized and controlled in accordance with approved procedures.
For example, manual integrations and reprocessing of laboratory results should be performed

in an approved and controlled manner. The firm's quality unit should establish measures to ensure that changes to data are performed only when necessary and by designated individuals. Original (unchanged) data should be retained in its original context.
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.
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.

2. 期待すること
データへの必要な変更は、承認された手順に従って認可され、管理されるべきである。
例えば、検査結果の手動による統合及び再処理は、承認され、管理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、指定された個人によって行われることを確実にするための手段を確立すべきである。オリジナル (変更されていない) データは、元の状況で保持されるべきである。
生データに対するすべての変更および修正は、完全に文書化され、少なくとも 1 人の適切な訓練を受けた有資格者によってレビューおよび承認されるべきである。

期待を満たさない場合の潜在的リスク／チェックすべき項目
- データの修正または再処理を管理するための適切な手順が存在することを検証する。提案された変更に対する正式な承認、管理された/制限された/定義された変更、および行われた変更の正式なレビューの適切なプロセスを示す証拠が必要である。

9.8 Review of data within computerized systems
Item:　Review of electronic data
1. Expectation
The regulated user should perform a risk assessment in order to identify all the GMP/GDP relevant electronic data generated by the computerized 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 authorized.
An SOP should describe the process by which data is checked by a second operator. These SOPs should outline the critical raw data that is reviewed, a review of data summaries, review of any associated log-books and hard-copy records, and explain how the review is performed,

recorded and authorized.

9.8 コンピュータ化システムにおけるデータのレビュー
項目　電子データのレビュー
1. 期待されること
規制対象ユーザーは、コンピュータシステムで生成される GMP/GDP 関連の電子データをすべて特定するためにリスクアセスメントを行い、そのデータの重要性を確認すること。識別された重要なデータは、規制対象ユーザーによって監査され、操作が正しく行われたか、変更（修正、削除、上書き）が行われたかどうかを検証する必要がある。
または上書き）が行われていないか、または関連する未報告のデータが生成されていないかを検証しなければならない。すべての変更は正式に認可されるべきである。
SOP は、データが第二のオペレータによってチェックされるプロセスを記述すべきである。これらの SOP は、レビューされる重要な生データ、データサマリーのレビュー、関連するログブックおよびハードコピー記録のレビューについて概説し、レビューがどのように実行され、記録され、承認されるかを説明すべきである。

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 computerized 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.
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 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.

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環として行われるべきである。
監査証跡のレビューの頻度、役割及び責任は、コンピュータ化されたシステムに記録されたデータの GMP/GDP に関連する価値に応じたリスク評価に基づくべきである。例えば、医薬品の品質に直接影響を与える電子データの変更については、バッチリリースなどの重要な決定を行うためにデータに依存する時点の前に、監査証跡をレビューすることが期待される。
規制対象となるユーザは、監査証跡をレビューする方法、何を探すか、どのように検索を実行するかなどを詳細に記述した SOP を確立するべきである。手順は、監査証跡レビューの担当者が従うべきプロセスを詳細に決定すべきである。監査証跡のレビュー活動は、文書化して記録すべきである。
監査証跡レビュー中に発見された期待される結果からの著しい変動は、完全に調査され記録されるべきである。監査証跡のレビューにより、医薬品の品質やデータの完全性に影響を及ぼす可能性のある重大な問題が特定された場合に取るべき行動を、手順書に記載するべきである。

期待を満たさない潜在的リスク／チェックすべき項目
- 電子データがその重要性（製品の品質および／または意思決定への影響）に基づいてレビューされることを確認するためのローカルな手順を確認する。各レビューの証拠を記録し、検査員が入手できるようにする。
- 内部または外部への報告のためにデータサマリー（データの概要報告書）が使用されている場合は、そのようなサマリーが生データと同様に検証されていることを示す証拠が入手できるべきである。
- 被規制当事者が、二次レビュー及び監査証跡レビューの実施方法と、レビューの過程で問題が発見された場合の手順を概説した詳細な SOP を持っていることを確認する。
- グローバルシステムが使用されている場合、日時の記録には、同時期の記録を証明するためにタイムゾーン注）の記録を含めることが必要な場合がある。
- データの変更、修正、削除が、監査証跡機能によって実際に記録されているかどうかを確

認する。
注）同一の標準時を採用している地域/機器内部の時刻をどの地域の標準時で運用するかを定めた設定項目。

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 program.
Procedures should be in place to address and investigate any audit trail discrepancies, including escalation processes for the notification of senior management and national authorities where necessary. Potential risk of not meeting expectations/items to be checked
・ 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).

2. 会社の品質管理部門は、現行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、潜在的なコンプライアンス違反の問題を検出するために、監査証跡の重要性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べきである。これらのレビューは、会社の自主監査プログラムに組み込まれるべきである。
監査証跡の不一致に対処し、調査するための手順は、必要に応じて上級管理職や国家機関に通知するためのエスカレーションプロセス注）を含むものでなければならない。

期待を満たさないことによる潜在的リスク／チェックすべき項目
- 自己点検プログラムが、既存のコントロールの有効性と、データのレビューに関する内部手順の遵守を検証する目的で、監査証跡のチェックを組み込んでいることを確認する。
- 監査証跡の確認は、無作為（偶然性に基づいて選択される）および対象（重要性またはリスクに基づいて選択される）の両方が必要である。
注）（下位の者が問題を解決できないとき、上位の者に関与を引き上げること）

9.9 Storage, archival and disposal of electronic data
Item:　Storage, archival and disposal of electronica data
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 unauthorized 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.
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.

9.9 電子データの保管、アーカイブおよび廃棄
項目：電子データの保管、アーカイブおよび廃棄
1. 期待されること
データの保管には、安全で検証されたプロセスを用いて、監査証跡を含むオリジナルデータ全体と関連するすべてのメタデータが含まれるべきである。
データがバックアップされているか、またはそのコピーが作成されている場合、データへの不正なアクセス、変更、削除、またはそれらの改変を禁止するように、バックアップおよびコピーにも同じ適切なレベルの管理が行われている必要がある。例えば、データを携帯用ハードディスクにバックアップする会社は、ハードディスクからデータを削除することを禁

止する必要がある。データの保存とバックアップについて、さらに考慮すべき点は以下の通りである。
- 動的な電子記録の真のコピーは、元の記録の内容全体（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ている）と意味が保存されていることを期待して、作成することができる。
- 保存されたデータは、完全に読み取り可能なフォーマットでアクセス可能でなければならない。
企業は、保存期間中に電子的に保存されたデータのバックアップやコピーにアクセスするために、適切なソフトウェアやハードウェアを維持する必要があるかもしれない。
- 定期的なバックアップコピーは、災害時に備えて遠隔地（物理的に分離された場所）に保管すること。
- バックアップデータは、ソフトウェアの新しいバージョンが更新されたり、より性能の良いものに代えられたりした場合でも、定義された規制上の保管期間のすべての期間において読むことができるべきである。
- システムは、メタデータや監査証跡を含むすべてのデータのバックアップと復元を可能にするべきである。

期待を満たさない場合の潜在的リスク／チェックすべき項目
- データストレージ、バックアップ、アーカイブシステム（保管）が、すべてのデータと関連するメタデータを取り込むように設計されていることを確認する。これらのシステムが検証され、確認されたことを文書化した証拠があるべきである。
- メタデータの取得範囲は、リスク管理の原則に基づいて決定されるべきであり、ユーザーは活動やプロセスの再構築に重要なメタデータがすべて取得されていることを確認する必要がある。
- 後継システムまたはアップグレードされたシステムに関連するデータが適切に管理され、アクセス可能であることを確認する。

2. Expectation
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.

2. 期待すること
記録保持手続きには、メタデータを保持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で、バッチに関連して発生した活動を再構築することができる。

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 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 authorized 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.

3. 期待すること

データは定期的にバックアップされ、文書化された手順に従ってアーカイブされるべきである。アーカイブコピーは、バックアップおよびオリジナルデータが保存されている場所とは別の遠隔地に、物理的に（または必要に応じて仮想的に）確保されるべきである。

アーカイブ期間中、データにアクセスして読み取ることができ、その完全性が維持されること。

調査が必要な場合に備えて、アーカイブされたデータを復元するための手順を定めておくこと。アーカイブされたデータを復元するための手順は、定期的にテストされるべきである。

アーカイブ・プロセスのために施設が必要な場合は、故意または不注意による改ざんや損失から記録を確実に保護するために、特定の環境制御を行い、許可された人員のみがアクセスできるようにする必要がある。データへの長期的なアクセスに関する問題が想定されるため、施設内のシステムを廃棄しなければならない場合、以下の手順を踏まなければならない。

アーカイブされたデータの継続的な読みやすさを保証する。例えば、データを別のシステムに移すことを確立することができる。

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 utilized 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.

期待を満たさない潜在的リスク／チェックすべき項目
- アーカイブされたデータは、ソフトウェア・アプリケーションの更新や機器の老朽化により、データへのアクセスや可読性が失われるリスクがある。会社がアーカイブされたデータへのアクセス権を持っていること、およびアーカイブされたデータのレビューを可能にするために必要なソフトウェアへのアクセスを維持していることを確認する。
- データのアーカイブに外部または第三者の施設を利用する場合、これらのサービス・ プロバイダは評価の対象となり、すべての責任は品質技術契約に記録されるべきである。契約書および評価記録を確認し、アーカイブされた記録の完全性を確保するために十分な配慮がなされていることを検証する。

4. Expectation
It should be possible to print out a legible and meaningful record of all the data generated by a computerized system (including metadata).
If a change is performed to records, it should be possible to also print out the change of the record, indicating when and how the original data was changed.
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.

4. 期待すること
コンピュータ化されたシステムで生成されたすべてのデータ（メタデータを含む）について、読みやすく意味のある記録を印刷できること。
記録に変更が加えられた場合、元のデータがいつ、どのように変更されたかを示す記録の変更も印刷できるべきである。

期待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
- 読みやすく完全な記録を作成するためにシステムが検証されていることを確認するために、システムの検証文書を確認する。
- プリントアウトのサンプルを確認してもよい。

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.

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.

5. 期待すること
電子的に保存されたデータの廃棄のプロセスを記述した手順を整備すること。これらの手順では、データの評価および保存期間の割り当てに関するガイダンスを提供し、不要になったデータの処分について説明する必要がある。

期待を満たさない場合の潜在的リスク／チェックすべき項目
- 手順書にデータの廃棄条件が明確に規定されているか、またデータのライフサイクル中に必要なデータが不用意に廃棄されないように配慮されているかを確認する。

9.10 Management of Hybrid Systems
Item:　Management of Hybrid Systems
1. Hybrid systems require specific and additional controls in reflection of their complexity and potential increased vulnerability to manipulation of data. 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 qualified and controlled in accordance with the guidance relating to manual and computerized 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 computerized systems;
- transcription (including manual) of data generated by automated systems onto paper records; and
- automated detection and transcription of printed data into computerized systems.

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 computerized 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 computerized and manual systems. Particular attention should be paid to verifying:
o The extent of qualification and/or validation of the computerized system; and,
o The robustness of controls applied to the management of the manual element of the hybrid system due to the difficulties in consistent application of a manual process.

9.10 ハイブリッド・システムの管理
項目　ハイブリッド・システムの管理
1. ハイブリッド・システムは、その複雑さと、データ操作に対する潜在的な脆弱性の増大を反映して、特定の追加的な管理を必要とする。このような理由から、ハイブリッド・システムの使用は推奨されず、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。
ハイブリッド・システムの各要素は、上述の手動及びコンピュータ化されたシステムに関するガイダンスに従って、適格性が確認され、管理されるべきである。

システムに適用される管理手段の有効性を評価、定義、実証する際には、適切な品質リスク管理の原則に従うべきである。
システムのすべての主要な構成要素、各構成要素の機能、データ管理と整合性のための管理、およびシステム構成要素の相互作用の方法を概説した、システム全体の詳細なシステム記述が利用可能であるべきである。

手動システムと自動システムの間のインターフェース、特に以下に関連する手順を管理し、適切に制御するための手順と記録が利用可能でなければならない。
- 手動で生成されたデータのコンピュータ化されたシステムへの手動入力。
- 自動化システムで生成されたデータの紙記録への転記（手動を含む）。
- 印刷されたデータの自動検出とコンピュータシステムへの転記。
期待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、識別されていること、およびシステムの各構成要素が検証されていることを確認する。
- 手動システムとコンピュータ・システムの間のインターフェースに注意を払うべきである。

検査員は、システム間で手作業による転記が行われる場合、適切な管理と二次的なチェックが行われていることを確認する。
- 転写および処理後のオリジナルデータは保持されるべきである。
- ハイブリッド・システムは、通常、コンピュータ化されたシステムとマニュアル・システムの組み合わせで構成される。検証には特に注意を払う必要がある。
o コンピュータ化されたシステムの適格性および／または妥当性の程度、ならびに
o 手動プロセスを一貫して適用することは困難であるため、ハイブリッド・システムの手動要素の管理に適用されるコントロールの堅牢性。

2. 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

Potential risk of not meeting expectations/items to be checked
・ Verify that instructions for the review of hybrid system data is in place.

2. 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に、電子データと紙ベースのデータの評価と承認のプロセスを明確に示す手順を導入する必要がある。手続きには以下が含まれる。
- 電子データと紙ベースのデータをどのように関連づけて完全な記録を形成するかの指示。
- 各システムで出力されるデータの承認に関する期待値。
- 統制の効果的な適用の検証に焦点を当てた、ハイブリッド・システムで特定されるリスク

期待値を満たさないことによる潜在的なリスク／チェックすべき項目
- ハイブリッド・システム・データのレビューに関する指示が実施されていることを検証する。

10 DATA INTEGRITY CONSIDERATIONS FOR OUTSOURCED ACTIVITIES

10 アウトソーシング活動におけるデータインテグリティに関する考慮事項項

10.1 General supply chain considerations

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 organizations, often from differing organizations and locations. These supply chains are often supported by additional organizations, providing outsourced services, IT services and infrastructure, expertise or consulting services.

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 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を確保するために、複数のパートナー企業が協力して構成されることが多い。典型的なサプライチェーンでは、原薬製造者、製剤製造者、分析機関、卸売り及び流通組織が関与し、多くの場合、異なる組織や場所からの参加を必要とする。これらのサプライチェーンは、しばしば、外部委託サービス、IT サービス、インフラ、専門知識、コンサルティングサービスを提供する組織によって支えられている。

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

10.1.2 データの完全性は、サプライチェーンのセキュリティ及び完全性を確保する上で重要な役割 を果たす。契約締結者によるデータガバナンス対策は、サプライチェーンのパートナーから提供される信頼性のない、または改ざんされたデータや資料によって著しく弱められる可能性がある。この原則は、原材料の供給者、製造委託先、分析サービス、卸売業者、契約サービスプロバイダー、コンサルタントなど、すべてのアウトソース活動に適用される。

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

10.1.3 サプライチェーンパートナーおよびアウトソース活動の初期および定期的な再確認には、データインテグリティリスクおよび適切な管理手段の検討が含まれるものとする。

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

10.1.4 組織は、サプライチェーンから得られる情報（概略記録、コピー／プリントアウトなど）の データインテグリティの限界と、遠隔監視の課題を理解することが重要である。これらの限界は、本ガイダンスの 8.11 項で述べられているものと同様である。これにより、品質リスクマネジメント手法を用いた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

10.2.1 The supply chain relies upon the use of documentation and data passed from one organization 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.

10.2 定期的な文書検証

10.2.1 サプライチェーンは、ある組織から別の組織に渡される文書およびデータの使用に依存している。契約締結者が、報告された結果に関連するすべての生データを確認することは、多くの場合、現実的ではない。品質リスクマネジメントの原則を用いて、外部委託された供給者及び請負業者の堅固な資格認定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

10.3.1 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:

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

10.3 サプライチェーンにおけるデータインテグリティを評価するための戦略

10.3.1 企業は、必要とされるデータインテグリティコントロールの範囲を評価するサプライチェーン及びアウトソー シング活動のリスクレビューを定期的に行うものとする。このようなレビューの頻度は、リスク管理の原則を用いて、契約の受諾者が提供するサービスの重要性に基づくべきである。
- データガバナンス対策に焦点を当てたサイト監査の結果
- データの完全性及びセキュリティに関連する国際的な基準又はガイドラインに準拠していることの証明
- ルーチンレポートなどで提出されたデータのレビュー。

レビューの対象範囲 根拠
・コントラクターまたはサプライヤーから報告された分析データと、同じ材料を分析した社内データとの比較
・同一物質の分析から得られたデータとの比較
・偽装の指標となりうる矛盾したデータを探す。

10.3.2 Quality agreements (or equivalent) should be in place between manufacturers and suppliers of materials, service providers, contract manufacturing organizations (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.

10.3.2 製造業者と材料の供給者、サービスプロバイダー、製造受託機関（CMO）及び（流通の場合）医薬品の供給者との間には、サプライチェーン全体でデータの完全性を確保するための具体的な規定を含む品質協定（又は同等のもの）が結ばれるものとする。これは、データガバナンスの期待値を設定し、契約の受諾者から契約の提供者への透明性のあるエラ

ー／逸脱の報告を行うことで達成できるかもしれない。また、コントラクトアクセプターのサイトで確認されたデータインテグリティの失敗をコントラクトギバーに通知する要件も必要である。

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 organization. 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.

10.3.3 製造者(又は製造者に代わって第三者が行う)が行う原薬の供給者及び製造者、重要な中間体の供給者、 一次及び印刷された包装材の供給者、製造委託先及びサービス提供者の監査には、契約組織におけるデータインテグリティ対策の検証が含まれるものとする。契約の受諾者は、データの完全性及び管理の原則の遵守状況を評価及び実証できるように、監査の際に契約の受諾者に代わって生成されたデータへの合理的なアクセスを提供することが期待される。

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

Quality monitoring Quality and performance monitoring may indicate incentive for data

falsification (e.g. raw materials which marginally comply with specification on a frequent basis.

10.3.4 監査及び定期的な監視には，品質リスクマネジメント手法を用いて，契約書提供者の品質ユ ニットによるソース電子データ及びメタデータの適切な検証が含まれるものとする。これは，以下のような手段で達成できる。
サイト監査契約締結者の組織行動及びデータガバナンス、データライフサイクル、リスク及びクリティカリティに関する理解をレビューする。
材料試験と CoA 分析試験の結果とサプライヤーが報告した CoA を比較する。正確さ、精度、純度の結果の不一致を調査する。これは、日常的に、定期的に、または不定期に行われる。
これは、材料やサプライヤーのリスクに応じて、日常的、定期的、または抜き打ちで行われる。必要に応じて、サンプルの定期的な技能試験を検討する。
遠隔データレビュー 契約の提供者は、バッチ製造及び試験に使用するために、契約施設／サプライヤーに独自のハード ウェア及びソフトウェアシステム（ワイドエリアネットワーク上に配置）の使用を提供することを考慮してもよい。契約の提供者は、契約施設の要員が生成したデータの品質及び完全性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、契約の受諾者が生成したデータを修正することができないように、契約の受諾者によるデータの監視を確実にするために、職務を分離する必要がある。

品質モニタリング 品質及びパフォーマンスのモニタリングは、データ改ざんの誘因となる可能性がある（例：規格にギリギリ準拠した（あるいはわずかに準拠していない）原材料が頻繁に使用されている場合など)。

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.

10.3.5 契約の提供者は、契約の受諾者と協力して、すべてのクライアントの機密情報がクライアントを 識別できないようにエンコードされることを保証することができる。これにより、他の顧客に対する守秘義務を破ることなく、契約の受諾者のサイトで ソース電子データ及びメタデータのレビューが容易になる。より多くのデータセットをレビューすることで、契約締結者のデータガバナンス対策をより強固に評価することができる。また、繰り

返されるデータセットや期待される変動性を示さないデータなど、データの完全性が損なわれる指標を探すことができる。
期待される変動性を示さないデータなど、データの完全性が損なわれている指標を探すことができる。

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.

10.3.6 提供された文書の真正性および正確性を確保するための注意が払われるものとする（8.11 項を参照)。契約者及びサプライチェーンの適格性を判断する際には、「トゥルーコピー」と「サマリーレポート」のデータの整合性及びトレーサビリティのリスクの違いを考慮する必要がある。

11 REGULATORY ACTIONS IN RESPONSE TO DATA INTEGRITY FINDINGS
11 データインテグリティに関する調査結果に応じた規制対応

11.1 Deficiency references

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

ALCOA principle PIC/S Guide to Good Manufacturing Practice for Medicinal products, PE 009 (Part I):

PIC/S Guide to Good Manufacturing Practice for Medicinal products, PE 009 (Part II):

Annex 11 (Computerized Systems)

PIC/S Guide to Good Distribution Practice for Medicinal products, PE 011:

11.1 不備の参照

11.1.1 データの完全性は、適正製造規範の基本であり、適正なデータ管理の要件は、現行の PIC/S Guides to GMP/GDP for Medicinal Products に組み込まれている。次の表は、これらの既存の要求事項のいくつかを強調する参照点を提供する。

アルコア原則 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):
PIC/S Guide to Good Manufacturing Practice for Medicinal Products, PE 009 (Part II):

附属書 11（コンピュータ化されたシステム

PIC/S Guide to Good Distribution Practice for Medicinal Products, PE 011:

Attributable
[4.20, c & f], [4.21, c & i], [4.29 point 5]

[5.43], [6.14], [6.18], [6.52]

[2], [12.1], [12.4], [15]

[4.2.4], [4.2.5]

Legible
[4.1], [4.2], [4.7], [4.8], [4.9], [4.10]

[6.11], [6.14], [6.15], [6.50]

[4.8], [7.1], [7.2]
[8.1], [9], [10], [17]

[4.2.3], [4.2.9]

Contemporaneous
[4.8]

[6.14]
[12.4], [14]

[4.1], [4.2.9]

Original
[4.9], [4.27], [Paragraph "Record"]

[6.14], [6.15], [6.16]

[8.2], [9]

[4.2.5]

Accurate
[4.1], [6.17]

[5.40], [5.42], [5.45], [5.46], [5.47], [6.6]

[Paragraph "Principles"] [4.8], [5], [6], [7.2], [10], [11]

[4.2.3]

Complete
[4.8]

[6.16], [6.50], [6.60], [6.61]

[4.8], [7.1], [7.2], [9]

[4.2.3], [4.2.5]

Consistent
[4.2]

[6.15], [6.50]

[4.8], [5]

[4.2.3]

Enduring
[4.1], [4.10]

[6.11], [6.12], [6.14]

[7.1], [17]

[4.2.6]

Available
[Paragraph “Principle”], [4.1]

[6.12], [6.15], [6.16]

[3.4], [7.1], [16], [17]

[4.2.1]

帰属
[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]

読みやすい
[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]

同時期
[4.8]

[6.14]
[12.4], [14]

[4.1], [4.2.9]

オリジナル
[4.9], [4.27], [パラグラフ「記録」].

[6.14], [6.15], [6.16]

[8.2], [9]

[4.2.5]

正確さ
[4.1], [6.17]

[5.40], [5.42], [5.45], [5.46], [5.47], [6.6]

原則」の項）［4.8］、［5］、［6］、［7.2］、［10］、［11］。

[4.2.3]

完全な
[4.8]

[6.16], [6.50], [6.60], [6.61]

[4.8], [7.1], [7.2], [9]

[4.2.3], [4.2.5]

一貫性
[4.2]

[6.15], [6.50]

[4.8], [5]

[4.2.3]

耐えること
[4.1], [4.10]

[6.11], [6.12], [6.14]

[7.1], [17]

[4.2.6]

利用可能
[原則], [4.1]

[6.12], [6.15], [6.16]

[3.4], [7.1], [16], [17]

[4.2.1]

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

11.2 不備の分類
注：以下のガイダンスは、データインテグリティ欠陥の報告と分類の一貫性を助けることを目的としており、検査当局がその内部方針または国内の規制フレームワークに従って行動する能力に影響を与えることを意図していない。

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

11.2.1 データインテグリティの不具合に関する欠陥は、製品品質に様々な影響を及ぼす可能性がある。また、不備の広がりは、一人の従業員の行動から検査対象組織全体の風土的な不備まで様々である。

11.2.2 The PIC/S guidance12 on classification of deficiencies states:
“A critical deficiency is a practice or process that has produced, or leads to a significant risk of producing either a product which is harmful to the human or veterinary patient or a product which could result in a harmful residue in a food producing animal. A critical deficiency also occurs when it is observed that the manufacturer has engaged in fraud, misrepresentation or falsification of products or data”.

11.2.2 欠陥の分類に関する PIC/S ガイダンス 12 は次のように述べている。
"重大な欠陥とは、人や獣医の患者に有害な製品、または食品を生産する動物に有害な残留物を 生じさせる可能性のある製品を製造した、または製造する重大なリスクにつながる慣行または工程をいう。重大な欠陥とは、製造者が製品やデータの不正、不実表示、改ざんに関与していることが認められる場合にも発生する。“

11.2.3 Notwithstanding the “critical” classification of deficiencies relating to fraud, misrepresentation or falsification, it is understood that data integrity deficiencies can also relate to:
・ Data integrity failure resulting from bad practice,
・ Opportunity for failure (without evidence of actual failure) due to absence of the required data control measures.

11.2.3 不正行為、虚偽の陳述、または改ざんに関連する欠陥を「重要」に分類するにもかかわらず、データインテグリティの欠陥は以下にも関連すると理解する。

- 不良行為に起因するデータインテグリティの不具合。
- 必要なデータ管理手段がないことによる失敗の機会（実際の失敗の証拠はない）。

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

11.2.4 このような場合には、以下を考慮して欠陥の分類を割り当てることが適切であろう（参考リストのみ）。

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

・ Product failing to meet Marketing Authorization 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.

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

・ Data being misreported, e.g. original results 'in specification', but altered to give a more favourable trend.

・ Reporting of a 'desired' result rather than an actual out of specification result when reporting of data which does not relate to QC tests, critical product or process parameters.

・ Failures arising from poorly designed data capture systems (e.g. using scraps of paper to record info for later transcription).

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.

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.

患者の健康に実際または潜在的なリスクを伴う製品への影響。致命的不備。

- 発売時または保存期間内に製品が製造販売承認の仕様に適合しないこと。
- QC テスト、重要な製品またはプロセスパラメータの報告において、実際の規格外の結果ではなく、「望ましい」結果を報告すること。
- 上級管理者の知識や支援の有無にかかわらず、広範囲にわたるデータの虚偽表示または改ざん。このような行為は、医薬品品質システムの信頼性を決定的に損ない、当該事業所で製造または取り扱われる医薬品の品質および安全性に対するすべての信頼を損なう。
製品への影響はあっても患者の健康へのリスクはない。重大な欠陥がある。
- 例えば、当初の結果は「規格通り」であったが、より好ましい傾向を示すように変更されたデータが誤って報告されている。
- QC テスト、重要な製品またはプロセスパラメータに関連しないデータを報告する際に、実際の規格外の結果ではなく「望ましい」結果を報告すること。
- 不適切に設計されたデータ収集システムに起因する失敗（例：後で転記するために情報を記録するために紙の切れ端を使用する）。
製品への影響はないが、中程度の欠陥の証拠。重大な欠陥。
- 限られた機能領域（QA、製造、QC など）において、データの整合性の問題やトレーサビリティの喪失を引き起こす可能性のある悪しき慣習やシステム設計の不備。それぞれが独立していても、製品品質には直接影響しない。
製品への影響はなく、不具合の証拠も限られている。その他の欠陥。
- その他の欠陥：不正行為やシステム設計の不備により、個別の領域でデータの整合性に問題が生じたり、トレーサビリティーが失われたりする可能性がある。
- 重要でないデータを個人が操作した場合など、他の点では問題のないシステムの限定的な障害。

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

11.2.5 全社的な障害があるのか、または範囲や影響が限定的な欠陥があるのかについて堅実な評価を行うためには、 主要な要素（データガバナンスプロセス、準拠したデータ記録を容易にするためのシステム設計、監査証跡 の使用および検証、IT ユーザーアクセスなど）の妥当性について全体像を構築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.

11.2.6 個々の状況（悪化要因／緩和要因）も、最終的な分類または規制措置に影響を与えることがある。欠陥の分類及び準拠問題の当局内報告に関する更なるガイダンスは、PIC/S Guidance on the classification of deficiencies PI 040 に記載されている。

12 REMEDIATION OF DATA INTEGRITY FAILURES

12.1 Responding to Significant Data Integrity issues

12 データインテグリティ障害の修正

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:

12.1.1 特定された当面の問題を解決し、データの完全性の問題に関連するリスクを評価することを主に考慮するものとする。
当該企業の回答は、改善計画の一環として実施された措置の概要を示すべきである。関係するメーカーからの回答には以下が含まれるべきである。

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 exclude13;

・ Interviews of current and where possible and appropriate, former employees to identify the nature, scope, and root cause of data inaccuracies. These interviews may be conducted by a qualified third party;

・ An assessment of the extent of data integrity deficiencies at the facility. Identify omissions, alterations, deletions, record destruction, non-contemporaneous record completion, and other deficiencies;

・ Determination of the scope (data, products, processes and specific batches) and timeframe for the incident, with justification for the time-boundaries applied;

・ A description of all parts of the operations in which data integrity lapses occurred,

additional consideration should be given to global corrective actions for multinational companies or those that operate across multiple sites;

・ A comprehensive retrospective evaluation of the nature of the data integrity deficiencies, and the identification of root cause(s) or most likely root cause that will form the basis of corrective and preventative actions, as defined in the investigation protocol. The services of a qualified third-party consultant with specific expertise in the areas where potential breaches were identified may be required;

・ A risk assessment of the potential effects of the observed failures on the quality of the substances, medicines, and products involved.

The assessment should include analyses of the potential risks to patients caused by the release/distribution of products affected by a lapse of data integrity, risks posed by ongoing operations, and any impact on the integrity of data submitted to regulatory agencies, including data related to product registration dossiers.

12.1.1.1 データ記録および報告における不正確さの程度に関する包括的な調査で、以下を含む。

- 詳細な調査プロトコルおよび方法、評価の対象となるすべての研究室、製造業務、製品およびシステムの概要、および規制対象ユーザーが除外することを提案する業務の一部に関する正当な理由。
- データの不正確さの性質、範囲、および根本原因を特定するための、現在および可能かつ適切な場合には、元従業員のインタビュー。これらのインタビューは資格のある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を評価する。省略、変更、削除、記録破壊、非同時記録の完成、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、プロセスおよび特定のバッチ）および時間枠の決定、および適用された時間枠の正当性。
- データインテグリティの欠落が発生した業務のすべての部分の説明。多国籍企業や複数のサイトで業務を行っている企業の場合は、グローバルな是正措置をさらに考慮する必要がある。
- 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、および調査プロトコルに定義されているように、是正措置および予防措置の基礎となる根本原因または最も可能性の高い根本原因の特定。違反の可能性が指摘された分野に特化した専門知識を持つ、有資格の第三者コンサルタントのサービスが必要な場合もある。
- 観察された欠陥が関係する物質、医薬品、製品の品質に及ぼす潜在的な影響のリスクアセスメント。

この評価には、データの完全性の欠如の影響を受けた製品の発売・流通によって引き起こさ

れる患者への潜在的なリスク、進行中の業務によって引き起こされるリスク、製品登録資料に関連するデータを含む規制当局に提出されたデータの完全性への影響などの分析が含まれるべきである。

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

・ Interim measures describing the actions to protect patients and to ensure the quality of the medicinal products, such as notifying customers, recalling product, conducting additional testing, adding lots to the stability program to assure stability, drug application actions, and enhanced complaint monitoring. Interim measures should be monitored for effectiveness and residual risks should be communicated to senior management, and kept under review.
・ Long-term measures describing any remediation efforts and enhancements to procedures, processes, methods, controls, systems, management oversight, and human resources (e.g. training, staffing improvements) designed to ensure the data integrity. Where long term measures are identified interim measures should be implemented to mitigate risks.

12.1.1.2 データインテグリティの脆弱性に対処するために取られた是正措置および予防措置、ならびに実施のための時間枠、およびこれを含む。
- 顧客への通知、製品の回収、追加試験の実施、安定性を保証するための安定性プログラムへのロットの追加、医薬品申請アクション、苦情監視の強化など、患者を保護し、医薬品の品質を確保するためのアクションを記述した暫定措置。中間対策は、その有効性を監視し、残存するリスクを上級管理者に伝え、検討を続けるべきである。
- 長期的な対策：改善のための努力や、手順、プロセス、方法、統制、システム、管理監督、人 的資源（例：研修、人員配置の改善）の強化を記述する。
データの完全性を確保するために設計された、手順、プロセス、方法、コントロール、システム、管理監督、および人的資源（トレーニング、人員配置の改善など）に対する改善努力および強化を記述する。長期的な対策が特定された場合、リスクを軽減するために暫定的な対策を実施する必要がある。

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

12.1.1.3 CAPA 有効性チェックを実施して、実施した処置が問題を解消したかどうかを監視する。

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.

12.1.2 可能な限り、査察官は関与している企業の上級代表者と面会し、指摘された欠陥の内容を伝え、その企業が包括的な調査、問題の完全な開示とその迅速な解決に取り組むことを書面で確認するものとする。グローバルな是正措置及び予防措置計画の詳細を含む管理戦略を規制当局に提出すべきである。

この戦略には以下が含まれるべきである。

- 現在の行動計画の範囲と深さが、調査とリスクアセスメントの結果に見合っているという証拠を含む、データインテグリティの失効の根本原因の包括的な説明。これには、データインテグリティの失策に関与した個人が、GMP/GDP 関連または医薬品申請データに影響を与えることができる状態にあるかどうかを示す必要がある。
- 規制対象ユーザーが、分析データ、製造記録、及び所轄官庁に提出又は提示する全てのデータを含む、生成された全てのデータの「ALOCA+」属性（7.4 項参照）をどのように確保しようとしているかを説明する詳細な是正措置計画。

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

12.1.3 査察機関は、データの完全性の侵害に関連するリスクを管理し、抑制するために、検査で特定された重要なデータの完全性の問題を管理するための方針を実施するものとする。

12.2 Indicators of improvement

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:

12.2 改善の指標
12.2.1 深刻なデータインテグリティ問題に対処するために取られた措置の有効性を検証するために、現地調査を行うことが推奨される。効果的な改善策を検証するための別のアプローチは、リスクマネジメントの原則に従って検討されるかもしれない。改善の指標としては次のようなものがある。

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

12.2.1.1 特定された問題を徹底的かつオープンに評価し、組織レベルでの是正措置および予防措置の適切な実施を含め、効果的な是正措置および予防措置を適時に実施した証拠。

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

12.2.1.2 顧客および他の規制当局との問題のオープンなコミュニケーションの証拠。
調査および修正の段階では、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。規制当局は、詳細な調査の結果、さらなるデータインテグリティの不具合が報告される可能性があることを認識すべきである。これらの報告に対する追加的な対応は、継続的な報告を促すために、公衆衛生リスクに見合ったものでなければならない。

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

12.2.1.3 組織全体でデータインテグリティに関する期待事項を伝え、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;

12.2.1.4 規制対象ユーザーは、データ操作に対する電子システムの脆弱性の適切な評価が行われ、フォローアップ措置がすべての違反を完 全に解決していることを確認するものとする。この評価には、関連する専門知識を有する有資格の第三者コンサルタントのサービスが必要となる場合がある。

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

12.2.1.5 本ガイドの原則に沿ったデータインテグリティポリシーの実施。

12.2.1.6 Implementation of routine data verification practices.

12.2.1.6 日常的なデータ検証作業の実施。

13 Glossary

Archiving

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

13 用語集

アーカイビング

プロセスや活動を再構築する目的で、完成したデータや関連するメタデータを最終的な形で長期的かつ恒久的に保存すること。

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 の重要な情報（例えば、GMP/GDP 関連データの

作成、変更、削除など）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
ディザスタリカバリ（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：分析実行に関連する変数設定）のコピーのこと。

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

コンピュータ化されたシステム
データの入力、電子的な処理、報告または自動制御のために使用す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, irrespective of the format in which it is generated, recorded, processed, retained and used to ensure a complete, consistent and accurate record throughout the data lifecycle.

データガバナンス
データが生成された形式に関わらず、データのライフサイクルを通じて完全で一貫性のある正確な記録を確保するために、データを記録、処理、保持、使用するための取り決めの全体。

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.

データの完全性
データが完全で、一貫性があり、正確で、信頼でき、信頼性があり、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ている度合い。
データは安全な方法で収集され、維持されなければならない。そのためには、データが帰属し、読みやすく、同時期に記録され、オリジナル（または真のコピー）であり、正確であることが必要である。データの完全性を確保するためには、健全な科学的原則や優れた文書作成の実践を含む、適切な品質およびリスク管理システムが必要である。また、データはALCOA+の原則に準拠する必要がある。

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
データ（生データを含む）の最初の生成および記録から、処理（変換または移行を含む）、使用、データの保持、アーカイブ/検索、および破棄までの、データ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.

データ品質
作成されたデータが意図された通りのものであり、意図された目的に適合していることを保証すること。これにはALCOA +の原則が組み込まれている。

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.

データの所有権
データのコントロールに関する責任を特定のプロセスオーナーに割り当てること。
企業は、システムとそのデータに対する責任が適切に割り当てられ、責任が果たされるようなシステムを導入する必要がある。

Dynamic Record
Records, such as electronic records, that allow an interactive relationship between the user and the record content.

ダイナミックレコード
電子記録など、ユーザーと記録内容との間にインタラクティブな関係を可能にする記録。

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.

例外レポート
データレビューアがさらなる注意や調査を必要とする、事前に設定された「異常な」データやアクションを特定し、文書化するための有効な検索ツール。

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、文書がデータ管理と整合性の原則を満たしていることを集合的かつ

個別に確認するための文書管理（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
電子データを生成する電子システムと、紙ベースの記録を生成する定義された手動システムで構成される、データの管理と制御のためのシステム。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が効果的に管理されている必要がある。

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あり、そこから配布または使用のための管理されたコピーを作成することができる。

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).
Metadata form an integral part of the original record. Without the context provided by metadata the data has no meaning.

メタデータ
他のデータの属性を記述し、文脈や意味を提供するファイル内データ。
一般的には、監査証跡などのデータの構造、データ要素、相互関係、その他の特性を記述するデータである。また、メタデータは、データを個人に帰属させることができる（自動生成

された場合は、元のデータソースに帰属させることができる)。
メタデータはオリジナルの記録と一体化している。メタデータによって提供される文脈がなければ、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.

品質ユニット
規制対象となる企業の中で、特に医薬品品質システムの設計、効果的な実施、監視および維持を含む品質の監督に責任を負う部署。

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.

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にかかわらず、情報の最初のキャプチャ（保存・保管）と言えるオリジナルの記録（データ）と定義される。最初に動的な状態で取得された情報は、その状態で利用可能でなければならない。

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.

静的記録
紙や電子記録などの記録形式で、固定されており、ユーザーと記録内容との相互作用がほとんど、あるいは全くないもの。

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
医薬品の品質を、製造から販売・使用の時点までの流通過程で確保するための、製造拠点、卸売拠点、流通拠点間の取り決めの全体。

System Administrator
A person who manages the operation of a computerized system or particular electronic communication service.

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

14 REVISION HISTORY

Date Version Number Reasons for revision

14 改訂履歴

日付 バージョン番号 改訂の理由