Medicines & Healthcare products Regulatory Agency (MHRA)

医薬品・ヘルスケア製品規制庁

(MHRA)

‘GXP’ Data Integrity Guidance and Definitions

「GXP」データインテグリティのガイダンスと定義

1 Background 背景

The way regulatory data is generated has continued to evolve in line with the ongoing development of supporting technologies such as the increasing use of electronic data capture, automation of systems and use of remote technologies; and the increased complexity of supply chains and ways of working, for example, via third party service providers. Systems to support these ways of working can range from manual processes with paper records to the use of fully computerised systems. The main purpose of the regulatory requirements remains the same, i.e. having confidence in the quality and the integrity of the data generated (to ensure patient safety and quality of products) and being able to reconstruct activities.

規制データの生成方法は、電子データキャプチャの使用の増加、システムの自動化、リモートテクノロジーの使用、そして例えばサードパーティのサービスプロバイダーを介する等の作業方法およびサプライチェーンの複合性の増加など、テクノロジーを支援する継続的な開発に合わせて進化を続けている。これらの作業方法をサポートするシステムは、紙の記録を使用した手動プロセスから完全にコンピュータ化されたシステムの使用まで多岐にわたる。規制要件の主な目的は変わらない。つまり、（患者の安全と製品の品質を確保するために）生成されたデータの品質と整合性に信頼性があり、アクティビティを再構築できることである。

2 Introduction 前書き

2.1

This document provides guidance for UK industry and public bodies regulated by the UK MHRA including the Good Laboratory Practice Monitoring Authority (GLPMA). Where possible the guidance has been harmonised with other published guidance. The guidance is a UK companion document to PIC/S, WHO, OECD (guidance and advisory documents on GLP) and EMA guidelines and regulations.

この文書は、英国産業省および Good Laboratory Practice Monitoring Authority（GLPMA）を含む英国 MHRA によって規制されている公共機関向けのガイダンスを提供する。可能な限り、ガイダンスは他の公開されたガイダンスと調和を保っている。このガイダンスは、PIC / S、WHO、OECD（GLP に関するガイダンスおよび諮問文書）並びに EMA のガイドラインと規制に対する英国のコンパニオンドキュメントである。

2.2

This guidance has been developed by the MHRA inspectorate and partners and has undergone public consultation. It is designed to help the user facilitate compliance through education, whilst clarifying the UK regulatory interpretation of existing requirements.

このガイダンスは、MHRA の検査官とパートナーによって開発され、公開協議を受けた。 これは、ユーザが教育を通じてコンプライアンスを促進できるように設計されている一方で、既存の要件の英国の規制解釈を明確にする。

2.3

Users should ensure their efforts are balanced when safeguarding data from risk with their other compliance priorities.

ユーザは、データをリスクから保護する際に、他のコンプライアンスの優先事項と自身の取組みとのバランスを保つ必要がある。

2.4

The scope of this guidance is designated as 'GXP' in that everything contained within the guide is GXP unless stated otherwise. The lack of examples specific to a GXP does not mean it is not relevant to that GXP just that the examples given are not exhaustive. Please do however note that the guidance document does not extend to medical devices.

このガイダンスの範囲は、特に明記されていない限り、ガイド内に含まれるすべてが GXP であるという点で「GXP」と指定されている。GXP に固有の例が不足してことは、与えられた例が網羅的ではないというだけで GXP に関係がないわけではない。ただし、ガイダンス文書は医療機器には適用されないことに注意すること。

2.5

This guidance should be considered as a means of understanding the MHRA's position on data integrity and the minimum expectation to achieve compliance. The guidance does not describe every scenario so engagement with the MHRA is encouraged where your approach is different to that described in this guidance.

このガイダンスは、データインテグリティに関する MHRA の立場と、コンプライアンスを達成するための最低限の期待を理解する手段として考慮する必要がある。このガイダンスではすべてのシナリオを説明しているわけではないため、MHRA との連携は、このガイダンスで説明されているアプローチと異なる場合に推奨される。

2.6

This guidance aims to promote a risk-based approach to data management that includes data risk, criticality and lifecycle. Users of this guidance need to understand their data processes (as a lifecycle) to identify data with the greatest GXP impact. From that, the identification of the most effective and efficient risk-based control and review of the data can be determined and implemented.

このガイダンスは、データリスク、重要度、ライフサイクルを含むデータ管理に対するリスクベースのアプローチを促進することを目的としている。このガイダンスのユーザは、GXP への影響が最も大きいデータを識別するために、データプロセスを（ライフサイクルとして）理解する必要がある。 そのことから、最も効果的かつ効率的なリスクベースの制御とデータのレビュの特定を決定し、実装することができる。

2.7

This guidance primarily addresses data integrity and not data quality since the controls required for integrity do not necessarily guarantee the quality of the data generated.

このガイダンスは、データの品質ではなく、主にデータインテグリティに対処する。それは、整合性に必要な制御は、生成されるデータの品質を必ずしも保証するものではないためである。

2.8

This guidance should be read in conjunction with the applicable regulations and the general guidance specific to each GXP. Where GXP-specific references are made within this document (e.g. ICH Q9), consideration of the principles of these documents may provide guidance and further information.

このガイダンスは、適用される規制および各 GXP に固有の一般的なガイダンスと併せて読む必要がある。本文書内で GXP 固有の参照がなされている場合(例：ICH Q9)、これらのドキュメントの原則を考慮することで、ガイダンスと詳細情報が提供される場合がある。

2.9

Where terms have been defined; it is understood that other definitions may exist and these have been harmonised where possible and appropriate.

用語が定義されている場合、他の定義が存在する可能性があり、可能かつ適切な場合にはこれらは調和していると理解される。

3 The principles of data integrity　データインテグリティの原則

3.1

The organisation needs to take responsibility for the systems used and the data they generate. The organisational culture should ensure data is complete, consistent and accurate in all its forms, i.e. paper and electronic.

組織は、使用されるシステムとそれらが生成するデータに対して責任を負う必要がある。 組織文化は、データがすべての形式、つまり紙と電子で完全で、一貫性があり、正確であることを保証する必要がある。

3.2

Arrangements within an organisation with respect to people, systems and facilities should be designed, operated and, where appropriate, adapted to support a suitable working environment, i.e. creating the right environment to enable data integrity controls to be effective.

人、システム、および施設に関する組織内の取り決めは、適切な作業環境をサポートするように設計、運用、および必要に応じて調整する必要がある。つまり、データインテグリティの制御を有効にする適切な環境を作りだすことである。

3.3

The impact of organisational culture, the behaviour driven by performance indicators, objectives and senior management behaviour on the success of data governance measures should not be underestimated. The data governance policy (or equivalent) should be endorsed at the highest levels of the organisation.

データガバナンス対策の成功に対する組織文化、パフォーマンス指標、目標、および上級管理職の行動によってもたらされる作用の影響を過小評価してはならない。 データガバナンスポリシー（または同等のもの）は、組織の最高レベルで承認される必要がある。

3.4

Organisations are expected to implement, design and operate a documented system that provides an acceptable state of control based on the data integrity risk with supporting rationale. An example of a suitable approach is to perform a data integrity risk assessment (DIRA) where the processes that produce data or where data is obtained are mapped out and each of the formats and their controls are identified and the data criticality and inherent risks documented.

組織は、データインテグリティリスクに基づいて許容可能な制御状態を提供する文書化されたシステムを実装し、設計し、運用することが期待されている。適切なアプローチの例は、データインテグリティリスク評価（DIRA）を実行することである。データインテグリティリスク評価（DIRA）では、データを生成するプロセスまたはデータを取得するプロセスをマッピングし、各形式とそのコントロールを特定し、データの重要性と固有のリスクを文書化する。

3.5

Organisations are not expected to implement a forensic approach to data checking on a routine basis. Systems should maintain appropriate levels of control whilst wider data governance measures should ensure that periodic audits can detect opportunities for data integrity failures within the organisation’s systems.

組織は、日常的にデータチェックに法医学的アプローチを実装することは期待されていない。システムは適切なレベルの制御を維持する必要があるが、より広範なデータガバナンス対策では、定期的な監査で組織のシステム内のデータインテグリティ障害の機会を検出できるようにする必要がある。

3.6

The effort and resource applied to assure the integrity of the data should be commensurate with the risk and impact of a data integrity failure to the patient or environment. Collectively these arrangements fulfil the concept of data governance.

データインテグリティを保証するための労力とリソースは、データインテグリティ障害が患者や環境に与えるリスクと影響に見合う必要がある。これらの取り決めは集合的に、データガバナンスの概念を満たす。

3.7

Organisations should be aware that reverting from automated or computerised systems to paper-based manual systems or vice-versa will not in itself remove the need for appropriate data integrity controls.

組織は、自動化されたシステムまたはコンピュータ化されたシステムから紙ベースの手動システムに戻す、またはその逆の場合でも、適切なデータインテグリティ制御の必要性がなくなるわけではないことに注意する必要がある。

3.8

Where data integrity weaknesses are identified, companies should ensure that appropriate corrective and preventive

actions are implemented across all relevant activities and systems and not in isolation.

データインテグリティの弱点が特定された場合、企業は、関連するすべてのアクティビティとシステムにわたって適切な是正措置と予防措置を単独で実装しないようにする。

3.9

Appropriate notification to regulatory authorities should be made where significant data integrity incidents have been identified.

重要なデータインテグリティのインシデントが特定された場合は、規制当局に適切な通知を行う必要がある。

3.10

The guidance refers to the acronym ALCOA rather than 'ALCOA +'. ALCOA being Attributable, Legible, Contemporaneous, Original, and Accurate and the '+' referring to Complete, Consistent, Enduring, and Available. ALCOA was historically regarded as defining the attributes of data quality that are suitable for regulatory purposes. The '+' has been subsequently added to emphasise the requirements. There is no difference in expectations regardless of which acronym is used since data governance measures should ensure that data is complete, consistent, enduring and available throughout the data lifecycle.

このガイダンスは、「ALCOA +」ではなく ALCOA の頭字語を指す。ALCOA は帰属性、判読可能性、同時性、オリジナル、正確性であり、「+」は完全性、一貫性、永続性、および利用可能性を指す。ALCOA は、従来、規制目的に適したデータ品質の属性を定義しているとみなされていた。その後、要件を強調するために「+」が追加された。どの頭字語が使用されているかに関係なく、データガバナンス対策では、データのライフサイクル全体でデータが完全で、一貫性があり、永続的で利用可能なことを保証する必要がある。

4 Establishing data criticality and inherent integrity risk　データの重要度と固有の整合性リスクの確立

4.1

Data has varying importance to quality, safety and efficacy decisions. Data criticality may be determined by considering how the data is used to influence the decisions made.

データは、品質、安全性、有効性の決定において重要性が異なる。データの重要度は、データがどのように使用され、意思決定に影響するかを検討することによって判断できる。

4.2

The risks to data are determined by the potential to be deleted, amended or excluded without authorisation and the opportunity for detection of those activities and events. The risks to data may be increased by complex, inconsistent processes with open-ended and subjective outcomes, compared to simple tasks that are undertaken consistently, are well defined and have a clear objective.

データに対するリスクは、許可なしに削除、修正、または除外される可能性と、それらのアクティビティおよびイベントを検出する機会によって決定される。データに対するリスクは、明らかな目的をもち、

一貫して実施される単純なタスクと比較すると、オープンエンドで主観的な結果を伴う、複雑で一貫性のないプロセスによって増加する可能性がある。

4.3

Data may be generated by: (i) Recording on paper, a paper-based record of a manual observation or of an activity or (ii) electronically, using equipment that range from simple machines through to complex highly configurable computerised systems or (iii) by using a hybrid system where both paper-based and electronic records constitute the original record or (iv) by other means such as photography, imagery, chromatography plates, etc.

データは次の方法で生成される。

(i) 紙に記録する、手動観察またはアクティビティの紙ベースの記録、

(ii) 電子的、単純な機械から複雑で高度に構成可能なコンピュータ化されたシステムに及ぶ機器を使用

(iii) 紙ベースの記録と電子記録の両方が元の記録を構成するハイブリッドシステムを使用

(iv) 写真、画像、クロマトグラフィープレートなど他の方法

Paper Data generated manually on paper may require independent verification if deemed necessary from the data integrity risk assessment or by another requirement. Consideration should be given to risk-reducing supervisory measures.

紙

手動で紙に生成されたデータは、データインテグリティリスク評価または別の要件から必要と判断された場合、独立した検証が必要になる場合がある。リスクを軽減する監督措置を検討する必要がある。

Electronic The inherent risks to data integrity relating to equipment and computerised systems may differ depending upon the degree to which the system generating or using the data can be configured, and the potential for manipulation of data during transfer between computerised systems during the data lifecycle.

電子

機器やコンピュータ化されたシステムに関連するデータインテグリティに対する固有のリスクは、データを生成または使用するシステムの構成できる度合い、およびデータライフサイクル中にコンピュータ化されたシステム間での転送中にデータ操作の可能性によって異なる場合がある。

The use of available technology, suitably configured to reduce data integrity risk, should be considered.

データインテグリティリスクを軽減するために適切に構成された、利用可能なテクノロジの使用を検討する必要がある。

Simple electronic systems with no configurable software and no electronic data retention (e.g. pH meters, balances

and thermometers) may only require calibration, whereas complex systems require ‘validation for intended purpose’.

Validation effort increases with complexity and risk (determined by software functionality, configuration, the opportunity for user intervention and data lifecycle considerations). It is important not to overlook systems of apparent lower complexity. Within these systems, it may be possible to manipulate data or repeat testing to achieve the desired outcome with limited opportunity for detection (e.g. stand-alone systems with a user-configurable output such as ECG machines, FTIR, UV spectrophotometers).

構成可能なソフトウェアや電子データ保持(pH メーター、天秤、温度計など)のない単純な電子システムは、キャリブレーションのみが必要な場合があるが、複雑なシステムでは「意図した目的のバリデーション」が必要である。

バリデーションは、複雑さとリスク(ソフトウェアの機能、構成、ユーザ介入の機会、およびデータのライフサイクルの考慮事項によって決定される)によって増加する。明らかに複雑性が低いシステムを見落とさないことが重要である。これらのシステム内では、データの操作や、テストを繰り返すことにより、限られた検出の機会内で、望ましい結果を達成することができる（例：ECG マシン、FTIR、UV 分光光度計などのユーザ設定可能な出力を備えたスタンドアロンシステム）。

Hybrid

Where hybrid systems are used, it should be clearly documented what constitutes the whole data set and all records that are defined by the data set should be reviewed and retained. Hybrid systems should be designed to ensure they meet the desired objective.

ハイブリッド

ハイブリッドシステムを使用する場合、データセット全体を構成するものを明確に文書化する必要があり、データセットによって定義されるすべてのレコードをレビュし、保持する必要がある。ハイブリッドシステムは、目的を確実に満たすように設計する必要がある。

Other

Where the data generated is captured by a photograph or imagery (or other media), the requirements for storage of that format throughout its lifecycle should follow the same considerations as for the other formats, considering any additional controls required for that format. Where the original format cannot be retained due to degradation issues, alternative mechanisms for recording (e.g. photography or digitisation) and subsequent storage may be considered and the selection rationale documented (e.g. thin layer chromatography).

他

生成されたデータが写真や画像 (または他のメディア) によってキャプチャされる場合、そのフォーマット全体を通してそのフォーマットを保存要件は、そのフォーマットに必要な追加の制御を考慮して、他のフォーマットと同じ考慮事項に従う必要がある。劣化の問題が原因で元の形式を保持できない場合は、記録 (写真やデジタル化など) とその後の保存の代替メカニズムを検討し、選択の根拠を文書化する (例：薄層クロマトグラフィーなど)。

4.4

Reduced effort and/or frequency of control measures may be justified for data that has a lesser impact to product, patient or the environment if those data are obtained from a process that does not provide the opportunity for amendment without high-level system access or specialist software/knowledge.

高度なシステムアクセスまたは専門家なソフトウェア/ナレッジを使用せずに修正の機会を提供しないプロセスからデータが取得された場合、製品、患者、または環境への影響がより少ないデータについては、労力および/または管理対策の頻度の削減が正当化される可能性がある。

4.5

The data integrity risk assessment (or equivalent) should consider factors required to follow a process or perform a function. It is expected to consider not only a computerised system but also the supporting people, guidance, training and quality systems. Therefore, automation or the use of a ‘validated system' (e.g. e-CRF; analytical equipment) may lower but not eliminate data integrity risk. Where there is human intervention, particularly influencing how or what data is recorded, reported or retained, an increased risk may exist from poor organisational controls or data verification due to an overreliance on the system's validated state.

データインテグリティリスク評価 (または同等のもの) は、プロセスに従うか、または機能を実行するために必要な要因を考慮する必要がある。コンピュータ化されたシステムだけでなく、支援する人、ガイダンス、トレーニング、品質システムも検討することが期待される。したがって、自動化や「検証済みシステム」(e-CRF、分析機器など)の使用は、データインテグリティリスクを低下させるが、排除されない可能性がある。人間の介入がある場合、特にデータの記録方法、報告方法、保持方法に影響を与える場合、システムの検証済み状態への過度の依存により、不十分な組織制御やデータ検証からリスクが増大する可能性がある。

4.6

Where the data integrity risk assessment has highlighted areas for remediation, prioritisation of actions (including acceptance of an appropriate level of residual risk) should be documented, communicated to management, and subject to review. In situations where long-term remediation actions are identified, risk-reducing short-term measures should be implemented to provide acceptable data governance in the interim.

データインテグリティリスク評価が修復の領域を強調している場合、アクションの優先順位付け(適切なレベルの残留リスクの受け入れを含む)を文書化し、マネジメントに伝え、レビュの対象とする必要がある。長期的な修復アクションが特定された場合、リスク低減の短期的な対策を実施し、暫定的に許容できるデータガバナンスを提供する必要がある。

5 Designing systems and processes to assure data integrity; creating the ‘right environment’.
データインテグリティを保証するシステムとプロセスの設計; 「適切な環境」の作成

5.1

Systems and processes should be designed in a way that facilitates compliance with the principles of data integrity. Enablers of the desired behaviour include but are not limited to:

- At the point of use, having access to appropriately controlled/synchronised clocks for recording timed events to ensure reconstruction and traceability, knowing and specifying the time zone where this data is used across multiple sites.
- Accessibility of records at locations where activities take place so that informal data recording and later transcription to official records does not occur.
- Access to blank paper proformas for raw/source data recording should be appropriately controlled. Reconciliation, or the use of controlled books with numbered pages, may be necessary to prevent recreation of a record. There may be exceptions such as medical records (GCP) where this is not practical.
- User access rights that prevent (or audit trail, if prevention is not possible) unauthorised data amendments. Use of external devices or system interfacing methods that eliminate manual data entries and human interaction with the computerised system, such as barcode scanners, ID card readers, or printers.
- The provision of a work environment (such as adequate space, sufficient time for tasks, and properly functioning equipment) that permit performance of tasks and recording of data as required.
- Access to original records for staff performing data review activities.
- Reconciliation of controlled print-outs.
- Sufficient training in data integrity principles provided to all appropriate staff (including senior management).
- Inclusion of subject matter experts in the risk assessment process.
- Management oversight of quality metrics relevant to data governance.

システムとプロセスは、データインテグリティの原則への準拠を促進する方法で設計する必要がある。期待される行動の実現手段には次のものが含まれるが、これらに限定されない。

・使用の時点で、適切に制御/同期されたクロックにアクセスして再構築とトレーサビリティを確保するためのタイミングイベントを記録し、このデータが複数のサイトで使用されるタイムゾーンを把握し、指定する

・アクティビティの実施場所での記録のアクセシビリティ。非公式のデータ記録とその後の公式記録への転記は発生しない。

・生/ソースデータの記録のための空紙の形式へのアクセスは、適切に制御する必要がある。記録の再調整を防ぐために、調整、または番号付きページを持つ管理された書籍の使用が必要な場合がある。医療記録（GCP）など、これが実用的でない例外が存在する場合がある。

・不正なデータ修正を防止するユーザクセス権 (または、防止できない場合は監査証跡)。手動データ入力や、バーコードスキャナー、ID カードリーダー、プリンターなどのコンピュータ化されたシステムとの人とのやり取りを排除する外部デバイスまたはシステムインターフェイス方法の使用。

・必要に応じてタスクの実行とデータの記録を可能にする作業環境（十分なスペース、タスクに十分な時間、適切に機能する機器など）の提供。

・データレビューのアクティビティを実施するスタッフのオリジナルの記録へのアクセス

・制御された印刷の調整。

・適切なスタッフ(経営陣を含む)全員に提供されるデータインテグリティの原則に関する十分なトレーニング

・リスク評価プロセスにおける対象の専門家の関与

・データガバナンスに関連する品質指標の管理監督。

5.2

The use of scribes to record activity on behalf of another operator can be considered where justified, for example: • The act of contemporaneous recording compromises the product or activity e.g. documenting line interventions by sterile operators. • Necropsy (GLP) • To accommodate cultural or literacy/language limitations, for instance where an activity is performed by an operator but witnessed and recorded by a second person.

別のオペレータに代わってアクティビティを記録するためのスクライブの使用は、正当な場合、例として次のように考えることができる。

・同時記録の行為は、製品またはアクティビティを損なう。 無菌オペレータによるライン介入の文書化。

・壊死(GLP)

・文化的または識字/言語の制限の対応。例として、アクティビティはオペレータによって実行され、立会いと記録は第 2 者によって実施される場合。

Consideration should be given to ease of access, usability and location whilst ensuring appropriate control of the activity guided by the criticality of the data.

データの重要度に従ってアクティビティを適切に制御しながら、アクセスの容易さ、ユーザビリティ、および場所を考慮する必要がある。

In these situations, the recording by the second person should be contemporaneous with the task being performed, and the records should identify both the person performing the task and the person completing the record. The person performing the task should countersign the record wherever possible, although it is accepted that this countersigning step will be retrospective. The process for supervisory (scribe) documentation completion should be described in an approved procedure that specifies the activities to which the process applies.

このような状況では、第 2 者による記録は、実行されるタスクと同時に行われるべきであり、記録はタスクを実行する人と記録を完了する人の両方を識別する必要がある。タスクの実施者は、可能な限り記録に副署する必要があるが、この副署手順は遡及的であると認められている。監督（スクライブ）文書作成のプロセスは、プロセスが適用されるアクティビティを指定する承認済みの手順で説明する必要がある。

6 Definition of terms and interpretation of requirements 用語の定義と要件の解釈

In the following section, definitions where applicable, are given in italic text directly below the term.

次のセクションでは、適用可能な場合は、定義は用語の直下に斜体のテキストで示される。

6.1 Data　データ

Facts, figures and statistics collected together for reference or analysis. All original records and true copies of original records, including source data and metadata and all subsequent transformations and reports of these data, that are generated or recorded at the time of the GXP activity and allow full and complete reconstruction and evaluation of the GXP activity.

参照または分析のために一緒に収集された事実、数字、統計。ソースデータとメタデータ、およびこれらのすべて変換とこれらのデータのレポートを含むすべてのオリジナルの記録とオリジナルの記録の新のコピーは、生成され GXP アクティビティの際に記録され、GXP アクティビティの完全かつ完全な再構築と評価を可能にする。

Data should be: A - attributable to the person generating the data L – legible and permanent C – contemporaneous O – original record (or certified true copy) A – accurate

データは以下の通りとなる。

A –データを生成した人に起因

L –判読可能で永続的

C –同時的

O –元の記録（または認定された真のコピー）

A –正確

Data governance measures should also ensure that data is complete, consistent, enduring and available throughout the lifecycle, where; Complete – the data must be whole; a complete set Consistent – the data must be self-consistent Enduring – durable; lasting throughout the data lifecycle Available – readily available for review or inspection purposes

データガバナンス対策では、データは完全で、一貫性があり、永続的であり、ライフサイクルを通じて利用可能であることを保証する必要がある。

完全性 – データは全体である必要がある。完全なセット

一貫性 – データは一貫している必要がある

永続性 – 耐久性; データのライフサイクルを通して持続している

利用可能性 – レビュまたは検査に対してすぐに利用可能

6.2 Raw data (synonymous with ‘source data’ which is defined in ICH GCP)　生データ（ICH GCP で定義されている「ソースデータ」と同義）

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.

生データは、紙に記録されたものであれ電子的に記録されたものであれ、情報の最初のキャプチャとして説明できる元の記録（データ）として定義される。 もともと動的な状態でキャプチャされた情報は、その状態で引き続き利用可能でなければならない。

Raw data must permit full reconstruction of the activities. Where this has been captured in a dynamic state and generated electronically, paper copies cannot be considered as 'raw data'.

生データは、アクティビティの完全な再構築を許可する必要がある。 これが動的な状態でキャプチャされ、電子的に生成された場合、紙のコピーを「生データ」と見なすことはできない。

In the case of basic electronic equipment that does not store electronic data, or provides only a printed data output (e.g. balances or pH meters), then the printout constitutes the raw data. Where the basic electronic equipment does store electronic data permanently and only holds a certain volume before overwriting; this data should be periodically reviewed and where necessary reconciled against paper records and extracted as electronic data where this is supported by the equipment itself.

電子データを保存しない基本的な電子機器の場合、または印刷データ出力（たとえば、天びんまたは pH メーター）のみを提供する場合、印刷出力は生データを構成する。
基本的な電子機器が電子データを永続的に保存し、上書きする前に特定のボリュームのみを保持する場合。 このデータは定期的に見直され、必要に応じて紙の記録と照合され、機器自体でサポートされる電子データとして抽出される必要がある。

In all definitions, the term 'data' includes raw data.

すべての定義において、「データ」という用語には生データが含まれる。

6.3 Metadata *メタデータ*

Metadata are data that describe the attributes of other data and provide context and meaning. Typically, these are data that describe the structure, data elements, inter-relationships and other characteristics of data e.g. audit trails. Metadata also permit data to be attributable to an individual (or if automatically generated, to the original data source).

メタデータは、他のデータの属性を記述し、コンテキストと意味を提供するデータである。通常、これらは、構造、データ要素、相互関係、および監査証跡などのデータの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、個人に起因するデータ(または自動的に生成された場合は、元のデータソース)も認められる。

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

メタデータは、元のレコードの不可欠な部分を形成する。メタデータによって提供されるコンテキストがなければ、データには意味がない。

Example (i) 3.5 metadata, giving context and meaning, (italic text) are: *sodium chloride batch 1234, 3.5mg. J Smith 01/Jul/14*

例 (i) 3.5
コンテキストと意味を示すメタデータ（イタリック体）
塩化ナトリウムバッチ 1234, 3.5*mg. J スミス 01/Jul/14*

Example (ii) 3.5 metadata, giving context and meaning, (italic text) are: *Trial subject A123, sample ref X789 taken 30/06/14 at 1456hrs.* *3.5mg. Analyst: J Smith 01/Jul/14*

例 (ii) 3.5
コンテキストと意味を示すメタデータ（イタリック体）
試験対象者 A123、サンプル ref X789 は 1456 時間で 30/06/14 を採取した。
3.5mg. アナリスト: J スミス 01/Jul/14

6.4 Data Integrity データインテグリティ

Data integrity is 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.

データインテグリティとは、データが完全で、一貫性があり、正確で、信用でき、信頼性があり、データのこれらの特性がライフサイクル全体にわたって維持される度合いである。データは、帰属性があり、判読可能で、同時性があり、オリジナル（または真のコピー）、正確であり、安全な方法で収集および維持する必要がある。データインテグリティを保証するには、適切な科学的原則と適切な文書化の実践を含む、適切な品質およびリスク管理システムが必要である。

。

6.5 Data Governance データガバナンス

The arrangements to ensure that data, irrespective of the format in which they are generated, are recorded, processed, retained and used to ensure the record throughout the data lifecycle.

データの生成形式に関係なく、データを記録、処理、保存、および使用して、データのライフサイクル全体を通じて記録を確保するための取り決め。

Data governance should address data ownership and accountability throughout the lifecycle, and consider the

design, operation and monitoring of processes/systems to comply with the principles of data integrity including control over intentional and unintentional changes to data.

データガバナンスは、ライフサイクル全体を通じてデータの所有権と説明責任に対処し、プロセス/システムの設計、運用、および監視を検討して、データに対する意図的および意図的でない変更の制御を含むデータインテグリティの原則に従う必要がある。

Data Governance systems should include staff training in the importance of data integrity principles and the creation of a working environment that enables visibility, and actively encourages reporting of errors, omissions and undesirable results.

データガバナンスシステムには、データインテグリティの原則の重要性に関するスタッフトレーニングと、可視化を可能にし、エラー、欠落、および望ましくない結果の報告を積極的に促す作業環境の作成を含める必要がある。

Senior management should be accountable for the implementation of systems and procedures to minimise the potential risk to data integrity, and for identifying the residual risk, using risk management techniques such as the principles of ICH Q9.

経営陣は、ICH Q9 の原則などのリスク管理手法を用いて、データインテグリティに対する潜在的なリスクを最小限に抑え、残留リスクを特定するためのシステムおよび手順の実施に責任を負う必要がある。

Contract Givers should ensure that data ownership, governance and accessibility are included in any contract/technical agreement with a third party. The Contract Giver should also perform a data governance review as part of their vendor assurance programme.

契約者は、第三者との契約/技術契約にデータの所有権、ガバナンス、アクセシビリティが含まれることを確認する必要がある。 契約者は、ベンダー保証プログラムの一環として、データガバナンスレビューも実行する必要がある。

Data governance systems should also ensure that data are readily available and directly accessible on request from national competent authorities. Electronic data should be available in human-readable form.

また、データガバナンスシステムは、各国の管轄当局からの要請に応じて、データが容易に利用可能であり、直接アクセス可能であることを保証する必要がある。電子データは、人間が読める形式で利用できる必要がある。

6.6 Data Lifecycle　データのライフサイクル

All phases in the life of the data from generation and recording through processing (including analysis, transformation or migration), use, data retention, archive/retrieval and destruction.

生成および記録から処理(分析、変換、移行を含む)、使用、データ保存、アーカイブ/取得、破壊まで、データのライフサイクルにおける全てのフェーズ。

Data governance, as described in the previous section, must be applied across the whole data lifecycle to provide assurance of data integrity. Data can be retained either in the original system, subject to suitable controls, or in an appropriate archive.

前のセクションで説明したように、データガバナンスは、データインテグリティを保証するために、データのライフサイクル全体にわたって完全に適用する必要がある。データは、適切な管理下にある元のシステムまたは適切なアーカイブのいずれかに保存できる。

6.7 Recording and collection of data　データの記録と収集

No definition required.

定義は必要ない。

Organisations should have an appropriate level of process understanding and technical knowledge of systems used for data collection and recording, including their capabilities, limitations and vulnerabilities.

組織は、能力、制限、脆弱性など、データの収集と記録に使用されるシステムの適切なレベルのプロセス理解と技術知識を持っている必要がある。

The selected method should ensure that data of appropriate accuracy, completeness, content and meaning are collected and retained for their intended use. Where the capability of the electronic system permits dynamic storage, it is not appropriate for static (printed / manual) data to be retained in preference to dynamic (electronic) data.
As data are required to allow the full reconstruction of activities the amount and the resolution (degree of detail) of data to be collected should be justified.

選択された方法は、適切な正確性、完全性、内容、および意味のデータが収集され、意図された使用のために保持されることを保証する必要がある。電子システムの機能が動的記憶を可能にする場合、静的（印刷/手動）データが動的（電子）データに優先して保持されるのは適切ではない。
アクティビティを完全に再構築するにはデータが必要であり、収集するデータの量と解像度（詳細度）を正当化する必要がある。

When used, blank forms (including, but not limited to, worksheets, laboratory notebooks, and master production and control records) should be controlled. For example, numbered sets of blank forms may be issued and reconciled upon completion. Similarly, bound paginated notebooks, stamped or formally issued by a document control group allow detection of unofficial notebooks and any gaps in notebook pages.

使用する場合は、空白のフォーム（ワークシート、ラボノート、マスタの生産および管理レコードを含むがこれらに限定されない）を制御する必要がある。たとえば、番号付きの空白フォームのセットが発行され、完了時に照合される。同様に、ドキュメント管理グループによってスタンプまたは正式に発行された、バインドされたページ番号付きノートブックのページでは、非公式のノートブックやノートブックページのギャップを検出できる。

6.8 Data transfer / migration データ転送/移行

Data transfer is the process of transferring data between different data storage types, formats, or computerised systems.

*データ転送は、異なるデータストレージタイプ、フォーマット、またはコンピュータ化されたシステム間でデータを*転送するプロセスである。

Data migration is the process of moving stored data from one durable storage location to another. This may include changing the format of data, but not the content or meaning.

データ移行とは、保存されたデータを永続的な保管場所から別の保管場所に移動するプロセスである。これには、データの形式の変更が含まれるが、内容や意味の変更は含まれない。

Data transfer is the process of transferring data and metadata between storage media types or computerised systems. Data migration where required may, if necessary, change the format of data to make it usable or visible on an alternative computerised system.

データ転送は、ストレージメディアタイプまたはコンピュータ化されたシステム間でデータとメタデータを転送するプロセスである。必要な場合は、必要に応じてデータの形式を変更し、別のコンピュータ化されたシステムでデータの使用または表示が可能になる。

Data transfer/migration procedures should include a rationale, and be robustly designed and validated to ensure that data integrity is maintained during the data lifecycle. Careful consideration should be given to understanding the data format and the potential for alteration at each stage of data generation, transfer and subsequent storage. The challenges of migrating data are often underestimated, particularly regarding maintaining the full meaning of the migrated records.

データ転送/移行手順には理論的根拠が含まれ、データのライフサイクル中にデータインテグリティが維持されるように堅牢に設計および検証する必要がある。データの生成、転送、および後続の保存の各段階で、データ形式および変更の可能性を理解する際には、慎重に検討する必要がある。データ移行の課題は、多くの場合、特に移行されたレコードの完全な意味を維持することに関して過小評価されている。

Data transfer should be validated. The data should not be altered during or after it is transferred to the worksheet or other application. There should be an audit trail for this process. Appropriate Quality procedures should be followed if the data transfer during the operation has not occurred correctly. Any changes in the middle layer software should be managed through appropriate Quality Management Systems.

データ転送を検証する必要がある。データは、ワークシートまたは他のアプリケーションに転送中または転送後に変更しないこと。このプロセスには監査証跡が必要である。操作中にデータ転送が正しく行われなかった場合は、適切な品質手順に従う必要がある。中間層ソフトウェアの変更は、適切な品質管理システムを通じて管理する必要がある。

Electronic worksheets used in automation like paper documentation should be version controlled and any changes in the worksheet should be documented/verified appropriately.

紙のドキュメントなどの自動化に使用される電子ワークシートはバージョン管理され、ワークシートの変更は適切に文書化/検証される必要がある。

6.9 Data Processing　データ処理

A sequence of operations performed on data to extract, present or obtain information in a defined format. Examples might include: statistical analysis of individual patient data to present trends or conversion of a raw electronic signal to a chromatogram and subsequently a calculated numerical result.

*データに対して実行される一連の操作で、定義された形式で情報を抽出、提示、または取得する。例としては、個々の患者データの統計分析による傾向の表示、生電子信号のクロマトグラムへの変換およびその後計算された数値結果の表示*が含まれる。

There should be adequate traceability of any user-defined parameters used within data processing activities to the raw data, including attribution to who performed the activity.

生データに対するデータ処理アクティビティ内で使用されるすべてのユーザ定義パラメータは、アクティビティの実行者の属性を含め、適切なトレーサビリティが必要である。

Audit trails and retained records should allow reconstruction of all data processing activities regardless of whether the output of that processing is subsequently reported or otherwise used for regulatory or business purposes. If data processing has been repeated with progressive modification of processing parameters this should be visible to ensure that the processing parameters are not being manipulated to achieve a more desirable result.

監査証跡および保存された記録は、その処理の出力が後で報告されるか、規制またはビジネスの目的で使用されるかどうかに関係なく、すべてのデータ処理アクティビティの再構築を可能にする必要がある。処理パラメータの漸進的な変更でデータ処理が繰り返されている場合、処理パラメータがより望ましい結果を達成するために操作されていないことを確認するために可視化する必要がある。

6.10 Excluding Data (not applicable to GPvP):　データの除外(GPvPには非適用)

Note: this is not applicable to GPvP; for GPvP refer to the pharmacovigilance legislation (including the GVP modules) which provide the necessary requirements and statutory guidance.

注: これは GPvP には適用されない。GPvP については、必要な要件と法定ガイダンスを提供するファーマコビジランス法(GVP モジュールを含む)を参照すること。

Data may only be excluded where it can be demonstrated through valid scientific justification that the data are not representative of the quantity measured, sampled or acquired. In all cases, this justification should be documented and considered during data review and reporting. All data (even if excluded) should be retained with the original data set, and be available for review in a format that allows the validity of the decision to exclude the data to be confirmed.

データは、そのデータが測定、サンプリング、取得された量を表していないという有効な科学的正当性を通じて実証できる場合にのみ除外できる。
いずれの場合も、データのレビュおよび報告時に、この妥当性は文書化し、検討する必要がある。すべてのデータは（除外されている場合でも）元のデータセットと共に保持され、確認されたデータを除外する決定の有効性を認める形式でレビュできる必要がある。

6.11 Original record and true copy 元のレコードと真のコピー

6.11.1 Original record オリジナルの記録

The first or source capture of data or information e.g. original paper record of manual observation or electronic raw data file from a computerised system, and all subsequent data required to fully reconstruct the conduct of the GXP activity. Original records can be Static or Dynamic.

データまたは情報の最初またはソースのキャプチャ、例えば 手動観察のオリジナルの紙の記録またはコンピュータ化されたシステムからの電子生データファイル、および GXP アクティビティの実施を完全に再構築するために必要なすべての後続データ。 オリジナルの記録は静的または動的である。

A static record format, such as a paper or electronic record, is one that is fixed and allows little or no interaction between the user and the record content. For example, once printed or converted to static electronic format chromatography records lose the capability of being reprocessed or enabling more detailed viewing of baselines.

紙や電子記録などの静的な記録形式は固定されており、ユーザと記録内容の間のやり取りをほとんどまたはまったく許可されない。例えば、印刷または静的な電子形式のクロマトグラフィー記録に変換された場合、再処理またはベースラインをより詳細に表示する機能が失われる。

Records in dynamic format, such as electronic records, allow an interactive relationship between the user and the record content. For example, electronic records in database formats allow the user to track, trend and query data; chromatography records maintained as electronic records allow the user or reviewer (with appropriate access permissions) to reprocess the data and expand the baseline to view the integration more clearly. Where it is not practical or feasibly possible to retain the original copy of source data, (e.g. MRI scans, where the source machine is not under the study sponsor's control and the operator can only provide summary statistics) the risks and mitigation should be documented.

電子記録などの動的形式の記録により、ユーザと記録内容とのインタラクティブな関係が可能になる。たとえば、データベース形式の電子記録を使用すると、ユーザはデータを追跡、傾向、およびクエリを行うことができる。 電子記録として保持されるクロマトグラフィー記録により、ユーザまたは（適切なアクセス許可を持つ）レビュ担当者はデータを再処理し、ベースラインを拡張して統合をより明確に表示できる。
ソースデータの元のコピーを保持することが実用的または実行可能でない場合（たとえば、MRI スキャン、ソースマシンが治験依頼者の管理下になく、オペレータが要約統計のみを提供できる場合)、リスクと軽減策を文書化する必要がある。

Where the data obtained requires manual observation to record (for example results of a manual titration, visual interpretation of environmental monitoring plates) the process should be risk assessed and depending on the criticality, justify if a second contemporaneous verification check is required or investigate if the result could be captured by an alternate means.

取得したデータを記録するために手動観察が必要な場合（たとえば、手動滴定の結果、環境モニタリングプレートの視覚的解釈)、プロセスをリスク評価し、重要度に応じて 2 回目の同時検証チェックが必要かどうかを正当化し、別の方法で結果はキャプチャできるかどうかを調査する必要がある。

6.11.2 True copy　真のコピー

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

コンテキスト、コンテンツ、および構造を記述するデータなど、オリジナルと同じ情報を持つことが検証された(すなわち、日付付きの署名または検証済みのプロセスを通じて生成された)元の記録の（使用するメディアのタイプに関係ない）コピー。

A true copy may be stored in a different electronic file format to the original record if required, but must retain the metadata and audit trail required to ensure that the full meaning of the data are kept and its history may be reconstructed.

真のコピーは、必要に応じて元の記録とは異なる電子ファイル形式で保存される場合があるが、メタデータと監査証跡を保持して、データの完全な意味を保持し、その履歴を再構築できるようにする必要がある。

Original records and true copies must preserve the integrity of the record. True copies of original records may be retained in place of the original record (e.g. scan of a paper record), if a documented system is in place to verify and record the integrity of the copy. Organisations should consider any risk associated with the destruction of original records.

元の記録と真のコピーは、記録の完全性を保持する必要がある。文書化されたシステムがコピーの完全性を検証し、記録する場合、元の記録の真のコピーが元の記録の代わりに保持される場合がある（紙のレコードのスキャンなど)。組織は、元の記録の破棄に関連するリスクを考慮する必要がある。

It should be possible to create a true copy of electronic data, including relevant metadata, for the purposes of review, backup and archival. Accurate and complete copies for certification of the copy should include the meaning of the data (e.g. date formats, context, layout, electronic signatures and authorisations) and the full GXP audit trail. Consideration should be given to the dynamic functionality of a ‘true copy’ throughout the retention period (see ‘archive’).

レビュ、バックアップ、アーカイブの目的で、関連するメタデータを含む電子データの真のコピーを作

成することが可能である。コピーの認証するための正確かつ完全なコピーには、データの意味(例えば、日付形式、コンテキスト、レイアウト、電子署名および承認)と完全な GXP 監査証跡を含める必要がある。保存期間を通じて「真のコピー」の動的機能に配慮する必要がある(「アーカイブ」を参照)。

Data must be retained in a dynamic form where this is critical to its integrity or later verification. If the computerised system cannot be maintained e.g., if it is no longer supported, then records should be archived according to a documented archiving strategy prior to decommissioning the computerised system. It is conceivable for some data generated by electronic means to be retained in an acceptable paper or electronic format, where it can be justified that a static record maintains the integrity of the original data. However, the data retention process must be shown to include verified copies of all raw data, metadata, relevant audit trail and result files, any variable software/system configuration settings specific to each record, 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. To enable a GXP compliant record this approach is likely to be demanding in its administration.

データは動的な形式で保持する必要があり、データインテグリティまたは後の検証に不可欠である。コンピュータ化されたシステムを維持できなくなった場合、たとえばサポートされなくなった場合、コンピュータ化されたシステムを廃止する前に、文書化されたアーカイブ戦略に従って記録をアーカイブする必要がある。電子的手段によって生成された一部のデータは、許容可能な紙または電子形式で保持され、静的なレコードが元のデータの完全性を維持することが正当化される可能性がある。ただし、データ保存プロセスでは、特定の生データセットの再構築に必要なものとして、すべての生データ、メタデータ、関連する監査証跡および結果ファイル、各レコードに固有の可変ソフトウェア/システム構成設定、およびすべてのデータ処理実行（メソッドおよび監査証跡を含む）の検証済みコピーが含まれていることが表示されなければならない。また、印刷された記録が正確な表現であることを検証するための文書化された手段も必要である。GXP 準拠の記録を有効にするために、このアプローチはその管理において要求される可能性がある。

Where manual transcriptions occur, these should be verified by a second person or validated system.

手動の転写が発生した場合、これらは第二者または検証されたシステムによって検証される必要がある。

6.12 Computerised system transactions: コンピュータ化されたシステムトランザクション

A computerised system transaction is a single operation or sequence of operations performed as a single logical 'unit of work'. The operation(s) that makes a transaction may not be saved as a permanent record on durable storage until the user commits the transaction through a deliberate act (e.g. pressing a save button), or until the system forces the saving of data.

コンピュータ化されたシステムトランザクションは、単一の論理「作業単位」として形成される単一の操作または一連の操作である。トランザクションを作成する操作は、ユーザが意図的な操作（たとえば、保存ボタンを押す）を使用してトランザクションをコミットするまで、または system が強制的にデ

*ータを保存*するまで、永続ストレージに永続的なレコードとして保存されない場合がある。
コンピュータ化されたシステムトランザクションは、単一の論理的な「作業単位」として実行される単一の操作または操作のシーケンスである。 トランザクションを行う操作は、ユーザが意図的な行為（保存ボタンを押すなど）でトランザクションをコミットするか、システムがデータの保存を強制するまで、永続ストレージとして永続ストレージとして保存されない場合がある。

The metadata (e.g. username, date, and time) are not captured in the system audit trail until the user saves the transaction to durable storage. In computerised systems, an electronic signature may be required for the record to be saved and become permanent.

メタデータ（ユーザ名、日付、時刻など）は、ユーザがトランザクションを永続ストレージに保存するまで、システム監査証跡に取り込まれない。コンピュータ化されたシステムでは、記録を保存して永続的にするために電子署名が必要になる場合がある。

A critical step is a parameter that must be within an appropriate limit, range, or distribution to ensure the safety of the subject or quality of the product or data. Computer systems should be designed to ensure that the execution of critical steps is recorded contemporaneously. Where transactional systems are used, the combination of multiple unit operations into a combined single transaction should be avoided, and the time intervals before saving of data should be minimised. Systems should be designed to require saving data to permanent memory before prompting users to make changes.

クリティカルステップとは、被験者の安全性もしくは製品またはデータの品質を確保するために、適切な制限、範囲、または分布内に収まる必要があるパラメータである。コンピューターシステムは、クリティカルステップの実行が同時に記録されるように設計する必要がある。トランザクションシステムを使用する場合は、複数のユニット操作を組み合わせて 1 つのトランザクションにまとめることを避け、データを保存するまでの時間間隔を最小限に抑える必要がある。システムは、ユーザに変更を促す前に、データを永続メモリに保存するように設計する必要がある。

The organisation should define during the development of the system (e.g. via the user requirements specification) what critical steps are appropriate based on the functionality of the system and the level of risk associated. Critical steps should be documented with process controls that consider system design (prevention), together with monitoring and review processes. Oversight of activities should alert to failures that are not addressed by the process design.

組織は、システムの開発中に（たとえば、ユーザ要件仕様書を介して)、システムの機能および関連するリスクのレベルに基づいて、どのようなクリティカルステップが適切であるかを定義する必要がある。クリティカルステップは、システム設計（予防）を考慮したプロセス制御と、監視およびレビュプロセスと共に文書化する必要がある。アクティビティの監視は、プロセス設計で対処されていない障害について警告する必要がある。

6.13 Audit Trail　監査証跡

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

監査証跡は、GXP レコードの作成、変更、または削除に関連するアクションに関連付けられた情報を含むメタデータの形式である。監査証跡は、オリジナルの記録を隠す、または上書きすることなく、紙または電子的な記録の情報の作成、追加、削除または変更などのライフサイクルの詳細を安全に記録する。監査証跡は、その媒体に関係なく、アクションの「誰が、何を、いつ、なぜ」をふくむ、記録に関連するイベントの履歴の再構築を容易にする。

Where computerised systems are used to capture, process, report, store or archive raw data electronically, system design should always provide for the retention of audit trails to show all changes to, or deletion of data while retaining previous and original data. It should be possible to associate all data and changes to data with the persons making those changes, and changes should be dated and time stamped (time and time zone where applicable). The reason for any change, should also be recorded. The items included in the audit trail should be those of relevance to permit reconstruction of the process or activity.

コンピュータ化されたシステムを使用して生データを電子的に取込み、処理、レポート、保存、またはアーカイブする場合、システム設計では、データのすべての変更または削除を表示するために、以前およびオリジナルのデータを保持しながら、監査証跡の保持を常に提供する必要がある。すべてのデータとデータの変更をそれらの変更を行う人に関連付けることができ、変更には日付とタイムスタンプ（該当する場合はタイムゾーン）が必要である。変更の理由も記録する必要がある。監査証跡に含まれる項目は、プロセスまたはアクティビティの再構築を可能にする関連性のある項目でなければならない。

Audit trails (identified by risk assessment as required) should be switched on. Users should not be able to amend or switch off the audit trail. Where a system administrator amends, or switches off the audit trail a record of that action should be retained.

監査証跡（必要に応じてリスク評価で特定）をオンにする必要がある。ユーザは、監査証跡を修正したり、切り替えたりすることはできない。システム管理者が監査証跡を修正またはスイッチオフする場合、そのアクションの記録を保持する必要がある。

The relevance of data retained in audit trails should be considered by the organisation to permit robust data review/verification. It is not necessary for audit trail review to include every system activity (e.g. user log on/off, keystrokes etc.).

監査証跡に保持されるデータの関連性は、堅牢なデータのレビュ/検証を可能にするために組織によって考慮される必要がある。監査証跡のレビュにすべてのシステムアクティビティ（ユーザのログオン/オフ、キーストロークなど）を含める必要はない。

Where relevant audit trail functionality does not exist (e.g. within legacy systems) an alternative control may be achieved for example defining the process in an SOP, and use of log books. Alternative controls should be proven to be effective.

関連する監査証跡機能が存在しない場合（たとえば、レガシーシステム内)、SOP でのプロセスの定義、ログブックの使用などの代替制御が実現される場合がある。代替制御が効果的であることが有効であることが証明される必要がある。

Where add-on software or a compliant system does not currently exist, continued use of the legacy system may be justified by documented evidence that a compliant solution is being sought and that mitigation measures temporarily support the continued use. [1]

アドオンソフトウェアまたは準拠システムが現在存在しない場合、準拠するソリューションが探索中であり、緩和策が継続した使用を一時的に支援していることを文書化された証拠により、レガシーシステムの継続的な使用が正当化される場合がある。 [1]

[1] It is expected that GMP facilities with industrial automation and control equipment/ systems such as programmable logic controllers should be able to demonstrate working towards system upgrades with individual login and audit trails (reference: Art 23 of Directive 2001/83/EC).

プログラム可能なロジックコントローラーなどの産業オートメーションおよび制御機器/システムを備えた GMP 設備は、個々のログインおよび監査証跡を使用したシステムアップグレードに向けた作業を実証できることが期待される（参照：Art 23 of Directive 2001/83/EC）

Routine data review should include a documented audit trail review where this is determined by a risk assessment. When designing a system for review of audit trails, this may be limited to those with GXP relevance. Audit trails may be reviewed as a list of relevant data, or by an ‘exception reporting' process. An exception report is a validated search tool that identifies and documents predetermined ‘abnormal’ data or actions, that require further attention or investigation by the data reviewer.

定期的なデータレビューには、文書化された監査証跡レビュを含める必要があり、これは、リスク評価によって決定される。監査証跡のレビュ用にシステムを設計する場合、これは GXP に関連するものに限定される場合がある。監査証跡は、関連データのリストとして、または「例外報告」プロセスによってレビュされる場合がある。例外レポートは、事前に決定された「異常な」データまたはアクションを識別および文書化し、データレビューアによる深く注意又は調査を要求する検証済みの検索ツールである。

Reviewers should have sufficient knowledge and system access to review relevant audit trails, raw data and metadata (see also ‘data governance’).

レビュ担当者には、関連する監査証跡、生データ、メタデータをレビュするための十分な知識とシステムアクセスが要求される（「データガバナンス」も参照)。

Where systems do not meet the audit trail and individual user account expectations, demonstrated progress should

be available to address these shortcomings. This should either be through add-on software that provides these additional functions or by an upgrade to a compliant system. Where remediation has not been identified or subsequently implemented in a timely manner a deficiency may be cited.

システムが監査証跡および個々のユーザカウントの予想に適合しない場合、これらの欠点に対処できる進化が実証される必要がある。そのためには、これらの追加機能を提供するアドオンソフトウェアを使用する、または準拠システムにアップグレードことが必要である。是正が特定されなかった場合、またはその後タイムリーに実施されなかった場合は、欠陥とされることがある。

6.14 Electronic signatures　電子署名

A signature in digital form (bio-metric or non-biometric) that represents the signatory. This should be equivalent in legal terms to the handwritten signature of the signatory.

署名者を表すデジタル形式の署名（バイオメトリックまたは非バイオメトリック)。これは、署名者の手書きの署名と法的に同等でなければならない。

The use of electronic signatures should be appropriately controlled with consideration given to:

- How the signature is attributable to an individual.
- How the act of 'signing' is recorded within the system so that it cannot be altered or manipulated without invalidating the signature or status of the entry.
- How the record of the signature will be associated with the entry made and how this can be verified.
- The security of the electronic signature i.e. so that it can only be applied by the 'owner' of that signature.

電子署名の使用は、以下を考慮して適切に制御する必要がある。

•署名が個人に帰属する方法。

•署名またはエントリのステータスを無効にすることなく変更または操作できないように、「署名」行為をシステム内で記録する方法。

•署名の記録が作成されたエントリにどのように関連付けられるか、およびこれを検証する方法。

•電子署名のセキュリティ。つまり、その署名の「所有者」のみが適用できるようにすること。

It is expected that appropriate validation of the signature process associated with a system is undertaken to demonstrate suitability and that control over signed records is maintained.

Where a paper or pdf copy of an electronically signed document is produced, the metadata associated with an electronic signature should be maintained with the associated document.

システムに関連する署名プロセスの適切なバリデーションが適合性を実証するために行われ、署名された記録の制御が維持されることが期待される。

電子署名されたドキュメントの紙または pdf コピーが作成される場合、電子署名に関連付けられたメタデータは、関連付けられたドキュメントと共に維持される必要がある。

The use of electronic signatures should be compliant with the requirements of international standards. The use of

advanced electronic signatures should be considered where this method of authentication is required by the risk assessment. Electronic signature or E-signature systems must provide for “signature manifestations” i.e. a display within the viewable record that defines who signed it, their title, and the date (and time, if significant) and the meaning of the signature (e.g. verified or approved).

電子署名の使用は、国際標準の要件に準拠する必要がある。この認証方法がリスク評価で必要な場合は、高度な電子署名の使用を検討する必要がある。電子署名または電子署名システムは、「署名の明示」、つまり署名者、タイトル、日付（重要な場合は時刻）および署名の意味（検証済みまたは承認済み）を提供する必要がある。

An inserted image of a signature or a footnote indicating that the document has been electronically signed (where this has been entered by a means other than the validated electronic signature process) is not adequate. Where a document is electronically signed then the metadata associated with the signature should be retained.

文書が電子署名されたことを示す署名または脚注の挿入画像（検証済みの電子署名プロセス以外の方法で入力された場合）は不十分である。文書が電子署名される場合、署名に関連付けられたメタデータは保持される必要がある。

For printed copies of electronically signed documents refer to True Copy section.

電子署名文書の印刷コピーについては、True Copy セクションを参照すること。

Expectations for electronic signatures associated with informed consent (GCP) are covered in alternative guidance (MHRA/HRA DRAFT Guidance on the use of electronic consent).

インフォームドコンセント（GCP）に関連する電子署名への期待は、代替ガイダンスでカバーされている（電子同意の使用に関する MHRA / HRA DRAFT ガイダンス）。

6.15 Data review and approval　データのレビュと承認

The approach to reviewing specific record content, such as critical data and metadata, cross-outs (paper records) and audit trails (electronic records) should meet all applicable regulatory requirements and be risk-based.

重要なデータやメタデータ、取り消し線（紙の記録）、監査証跡（電子記録）などの特定の記録内容をレビュするアプローチは、適用されるすべての規制要件を満たし、リスクに基づくものでなければならない。

There should be a procedure that describes the process for review and approval of data. Data review should also include a risk-based review of relevant metadata, including relevant audit trails records. Data review should be documented and the record should include a positive statement regarding whether issues were found or not, the date that review was performed and the signature of the reviewer.

データのレビュと承認のプロセスを説明する手順が必要である。データレビュには、関連する監査証跡記録を含む、関連するメタデータのリスクベースのレビュも含める必要がある。データのレビュを文書

化し、記録に問題が見つかったかどうか、レビュが実行された日付、およびレビュ担当者の署名に関する肯定的な声明を含める必要がある。

A procedure should describe the actions to be taken if data review identifies an error or omission. This procedure should enable data corrections or clarifications to provide visibility of the original record, and traceability of the correction, using ALCOA principles (see 'data' definition).

手順では、データのレビュでエラーまたは省略が特定された場合に実行するアクションを説明する必要がある。この手順により、ALCOA の原則（「データ」の定義を参照）を使用して、元の記録の可視性と修正のトレーサビリティを提供するためのデータ修正または明確化が可能になる。

Where data review is not conducted by the organisation that generated the data, the responsibilities for data review must be documented and agreed by both parties. Summary reports of data are often supplied between organisations (contract givers and acceptors). It must be acknowledged that summary reports are limited and critical supporting data and metadata may not be included.

データを生成した組織によってデータレビュが実施されない場合、データレビュの責任を文書化し、双方が合意する必要がある。データの要約レポートは、多くの場合、組織（委託者と受託者）の間で提供される。要約レポートは限られており、重要なサポートデータとメタデータが含まれていない可能性があることを認識しておく必要がある。

Many software packages allow configuration of customised reports. Key actions may be incorporated into such reports provided they are validated and locked to prevent changes. Automated reporting tools and reports may reduce the checks required to assure the integrity of the data.

多くのソフトウェアパッケージでは、カスタマイズされたレポートを構成できる。主要なアクションが変更を防ぐために検証およびロックされている場合、そのようなレポートに組み込むれる場合がある。自動レポートツールとレポートにより、データインテグリティを保証するために必要なチェックが削減される場合がある。

Where summary reports are supplied by a different organisation, the organisation receiving and using the data should evaluate the data provider's data integrity controls and processes prior to using the information.

別の組織から概要レポートが提供される場合、データを受け取って使用する組織は、情報を使用する前にデータプロバイダーのデータ整合性の制御とプロセスを評価する必要がある。

- Routine data review should consider the integrity of an individual data set e.g. is this the only data generated as part of this activity? Has the data been generated and maintained correctly? Are there indicators of unauthorised changes?

•定期的なデータレビュでは、個々のデータセットの整合性を考慮する必要がある。このアクティビティの一部として生成されるデータはこれだけであるか？データは正しく生成および維持されているか？不正な変更の指標はあるか？

• Periodic audit of the data generated (encompassing both a review of electronically generated data and the broader organisational review) might verify the effectiveness of existing control measures and consider the possibility of unauthorised activity at all interfaces, e.g. have there been IT requests to amend any data post review? Have there been any system maintenance activities and has the impact of that activity been assessed?

•生成されたデータの定期的な監査（電子的に生成されたデータのレビュと広範な組織レビュの両方を含む）は、既存の制御手段の有効性を検証し、すべてのインターフェースでの不正な活動の可能性を検討する。レビュ後のデータを修正する IT 要求があるか？システムメンテナンスアクティビティがあり、そのアクティビティの影響が評価されたか？

6.16 Computerised system user access/system administrator roles コンピュータ化されたシステムユーザアクセス/システム管理者の役割

Full use should be made of access controls to ensure that people have access only to functionality that is appropriate for their job role, and that actions are attributable to a specific individual. Companies must be able to demonstrate the access levels granted to individual staff members and ensure that historical information regarding user access level is available. Where the system does not capture this data, then a record must be maintained outside of the system. Access controls should be applied to both the operating system and application levels. Individual login at operating system level may not be required if appropriate controls are in place to ensure data integrity (e.g. no modification, deletion or creation of data outside the application is possible).

ユーザが自身の職務に適した機能にのみアクセスし、アクションは特定の個人に帰属することを確実にするために、アクセス制御を完全に使用する必要がある。企業は、個々のスタッフメンバーに付与されたアクセスレベルを実証し、ユーザアクセスレベルに関する履歴情報を確実に入手できるようにする必要がある。システムがこのデータをキャプチャしない場合、システムの外部で記録を保持する必要がある。アクセス制御は、オペレーティングシステムレベルとアプリケーションレベルの両方に適用する必要がある。データインテグリティを確保するために適切な制御が行われている場合、オペレーティングシステムレベルでの個別のログインは必要ない場合がある（例、アプリケーション外でのデータの変更、削除、作成が不可能である場合)。

For systems generating, amending or storing GXP data shared logins or generic user access should not be used. Where the computerised system design supports individual user access, this function must be used. This may require the purchase of additional licences. Systems (such as MRP systems) that are not used in their entirety for GXP purposes but do have elements within them, such as approved suppliers, stock status, location and transaction histories that are GXP applicable require appropriate assessment and control.

GXP データを生成、修正、または保存するシステムでは、共有ログインまたは汎用ユーザアクセスを使用してはいけない。コンピュータ化されたシステム設計が個々のユーザアクセスをサポートする場合、この機能を使用する必要がある。これには、追加のライセンスの購入が必要になる場合がある。 GXP の目的には完全に使用されていないが、承認済みのサプライヤ、在庫状況、場所、GXP に該当する取引履歴などの要素を含むシステム（MRP システムなど）には、適切な評価と制御が必要である。

It is acknowledged that some computerised systems support only a single user login or limited numbers of user logins. Where no suitable alternative computerised system is available, equivalent control may be provided by third-party software or a paper-based method of providing traceability (with version control). The suitability of alternative systems should be justified and documented. Increased data review is likely to be required for hybrid systems because they are vulnerable to non-attributable data changes. It is expected that companies should be implementing systems that comply with current regulatory expectations[2].

コンピュータ化システムによっては、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のみをサポートしているものがあることが知られている。適切な代替のコンピュータ化システムが利用できない場合、サードパーティのソフトウェアまたはトレーサビリティを提供する紙ベースの方法（バージョン管理）によって同等の制御を提供できる。代替システムの適合性を正当化し、文書化する必要がある。ハイブリッドシステムは、帰属しないデータの変更に対して脆弱であるため、データレビュの増加が必要になる可能性がある。企業は、現在の規制上の期待に準拠したシステムを実装することが期待されている[2]。

[2] It is expected that GMP facilities with industrial automation and control equipment/ systems such as programmable logic controllers should be able to demonstrate working towards system upgrades with individual login and audit trails (reference: Art 23 of Directive 2001/83/EC).

プログラム可能なロジックコントローラーなどの産業オートメーションおよび制御機器/システムを備えた GMP 設備は、個々のログインおよび監査証跡を使用したシステムアップグレードに向けた作業を実証できることが期待される（参照：Art 23 of Directive 2001/83/EC）。

System administrator access should be restricted to the minimum number of people possible taking account of the size and nature of the organisation. The generic system administrator account should not be available for routine use. Personnel with system administrator access should log in with unique credentials that allow actions in the audit trail(s) to be attributed to a specific individual. The intent of this is to prevent giving access to users with potentially a conflict of interest so that they can make unauthorised changes that would not be traceable to that person.

システム管理者のアクセスは、組織の規模と性質を考慮し、可能な限り最小限の人数に制限する必要がある。一般的なシステム管理者アカウントを日常的に使用することはできない。システム管理者のアクセス権を持つ担当者は、監査証跡のアクションを特定の個人に帰属させる固有の資格情報でログインする必要がある。この目的は、利益相反の可能性があるユーザで、追跡が及ばない不正な変更ができる者にアクセス権を与えることを防ぐことである。

System Administrator rights (permitting activities such as data deletion, database amendment or system configuration changes) should not be assigned to individuals with a direct interest in the data (data generation, data review or approval).

システム管理者権限（データの削除、データベースの修正、システム構成の変更などのアクティビティを

許可すること）は、データに直接利害のある個人（データの生成、データのレビュー、承認）には割り当ててはいけない。

Individuals may require changes in their access rights depending on the status of clinical trial data. For example, once data management processes are complete, the data is ‘locked’ by removing editing access rights. This should be able to be demonstrated within the system.

臨床試験データのステータスに応じて、アクセス権の変更が必要になる場合がある。たとえば、データ管理プロセスが完了すると、編集アクセス権を削除することでデータが「ロック」される。これは、システム内で実証できる必要がある。

6.17 Data retention データ保持

Data retention may be for archiving (protected data for long-term storage) or backup (data for the purposes of disaster recovery).

データ保持は、アーカイブ（長期保存用の保護されたデータ）またはバックアップ（災害復旧目的のデータ）の場合がある。

Data and document retention arrangements should ensure the protection of records from deliberate or inadvertent alteration or loss. Secure controls must be in place to ensure the data integrity of the record throughout the retention period and should be validated where appropriate (see also data transfer/migration).

データおよびドキュメントの保存の取り決めでは、意図的または不注意による変更または損失から記録を保護する必要がある。保持期間を通じて記録のデータインテグリティを確保するために、保護された制御を実施する必要があり、必要に応じて検証する必要がある（データ転送/移行も参照)。

Data (or a true copy) generated in paper format may be retained by using a validated scanning process provided there is a documented process in place to ensure that the outcome is a true copy.

紙形式で生成されたデータ（または真のコピー）は、結果が真のコピーであることを保証する文書化されたプロセスがある場合、検証済みのスキャンプロセスを使用して保持できる。

Procedures for destruction of data should consider data criticality and where applicable legislative retention requirements.

データの破棄手順では、データの重要性と、必要に応じて法的保存要件を考慮する必要がある。

6.17.1 Archive アーカイブ

A designated secure area or facility (e.g. cabinet, room, building or computerised system) for the long term, retention of data and metadata for the purposes of verification of the process or activity.

プロセスまたはアクティビティの検証を目的とした、データおよびメタデータの長期保存用の指定された安全な領域または施設（キャビネット、部屋、建物、またはコンピュータ化システムなど)。

Archived records may be the original record or a ‘true copy’ and should be protected so they cannot be altered or deleted without detection and protected against any accidental damage such as fire or pest.

アーカイブされた記録は、オリジナルの記録または「真のコピー」である可能性があり、検出せずに変更または削除できないように保護し、火災または害虫などの偶発的な損傷から保護する必要がある。

Archive arrangements must be designed to permit recovery and readability of the data and metadata throughout the required retention period. In the case of archiving of electronic data, this process should be validated, and in the case of legacy systems the ability to review data periodically verified (i.e. to confirm the continued support of legacy computerised systems). Where hybrid records are stored, references between physical and electronic records must be maintained such that full verification of events is possible throughout the retention period.

アーカイブの配置は、必要な保存期間全体にわたってデータとメタデータのリカバリと可読性を確保するように設計する必要がある。電子データのアーカイブの場合、このプロセスを検証する必要がある。レガシーシステムの場合、定期的に検証されたデータをレビュする機能（つまり、レガシーコンピュータ化システムの継続的なサポートの確認）が必要である。ハイブリッド記録を保存する場合、物理的記録と電子的記録の間の参照を維持し、保持期間を通してイベントの完全な検証を可能にする必要がある。

When legacy systems 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). It is recognised that the need to maintain accessibility may require migration to a file format that loses some attributes and/or dynamic data functionality (see also ‘Data Migration’).

レガシーシステムをサポートできなくなった場合は、データのアクセシビリティのためにソフトウェアを保守することを検討する必要がある。(特定の保持要件に応じて可能な限り)。これは、仮想環境でソフトウェアを保守することで実現できる。

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は、レガシーデータの経過時間の増加に伴って必要になる場合がある。完全なオリジナルのデータ機能を使用した移行が技術的に不可能な場合、リスクと長期にわたる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（データ調査、傾向分析、再処理など)。移行ファイル形式は、長期的なアクセス可能性と動的データ機能の低下の可能性のリスクのバランスを考慮して選択する必要がある。アクセシビリティを維持するために、一部の属性や動的データ機能を失うファイル形式への移行が必要になる場合があることが認識されている（「データ移行」も参照)。

6.17.2 Backup　バックアップ

A copy of current (editable) data, metadata and system configuration settings maintained for recovery including disaster recovery.

災害復旧などの復旧のために維持されている現在の（編集可能な）データ、メタデータ、およびシステム構成設定のコピー。

Backup and recovery processes should be validated and periodically tested. Each back up should be verified to ensure that it has functioned correctly e.g. by confirming that the data size transferred matches that of the original record.

バックアップと復元のプロセスを検証し、定期的にテストする必要がある。各バックアップは、正しく機能していることを確認するために検証する必要がある。例えば、転送されたデータサイズが元のレコードのデータサイズと一致することを確認する。

The backup strategies for the data owners should be documented.

データ所有者のバックアップ戦略を文書化する必要がある。

Backups for recovery purposes do not replace the need for the long term, retention of data and metadata in its final form for the purposes of verification of the process or activity.

リカバリを目的としたバックアップは、プロセスまたはアクティビティの検証を目的としてデータおよびメタデータを最終的な形式で長期保存する必要性に代わるものではない。

6.18　File structure　ファイル構造

Data Integrity risk assessment requires a clear understanding of file structure. The way data is structured within the GXP environment will depend on what the data will be used for and the end user may have this dictated to them by the software/computerised system(s) available. There are many types of file structure, the most common being flat files and relational databases.

データインテグリティリスク評価では、ファイル構造を明確に理解する必要がある。 GXP 環境内でデータを構造化する方法は、データの使用目的によって異なるが、エンドユーザは、使用可能なソフトウェア/コンピュータ化システムによってそのデータを指示できる場合がある。
ファイル構造には多くの種類があり、最も一般的なものはフラットファイルとリレーショナルデータベースである。

Different file structures due to their attributes may require different controls and data review methods and may retain meta data in different ways.

属性によりファイル構造が異なると、異なる制御とデータレビュ方法が必要になる場合があり、メタデータが異なる方法で保持される場合がある。

6.19 Validation – for intended purpose (GMP; See also Annex 11, 15)　検証–意図された目的のため（GMP。付録11、15も参照）

Computerised systems should comply with regulatory requirements and associated guidance. These should be validated for their intended purpose which requires an understanding of the computerised system's function within a process. For this reason, the acceptance of vendor-supplied validation data in isolation of system configuration and users intended use is not acceptable. In isolation from the intended process or end-user IT infrastructure, vendor testing is likely to be limited to functional verification only and may not fulfil the requirements for performance qualification.

コンピュータ化システムは、規制要件および関連するガイダンスに準拠する必要がある。これらは、プロセス内のコンピュータ化されたシステムの機能の理解を必要とする意図された目的のために検証する必要がある。このため、システム構成とユーザの使用目的を切り離してベンダー提供の検証データを受け入れることはできない。意図されたプロセスまたはエンドユーザの IT インフラストラクチャから隔離されているため、ベンダーのテストは機能検証のみに限定される可能性が高く、、稼働性能適格性確認の要件を満たしていない場合がある。

Functional verification demonstrates that the required information is consistently and completely presented. Validation for intended purpose ensures that the steps for generating the custom report accurately reflect those described in the data checking SOP and that the report output is consistent with the procedural steps for performing the subsequent review.

機能検証により、必要な情報が一貫して完全に提示されていることが実証される。意図された目的の検証により、カスタムレポートを生成する手順がデータチェック SOP で説明されている手順を正確に反映し、レポート出力が後続のレビュを実行する手順と整合することが確認される。

6.20 IT Suppliers and Service Providers (including Cloud providers and virtual service/platforms (also referred to as software as a service SaaS/platform as a service (PaaS) / infrastructure as a service (IaaS)).　ITサプライヤおよびサービスプロバイダー（クラウドプロバイダーおよび仮想サービス/プラットフォーム（ソフトウェアとしてのサービスSaaS /サービスとしてのプラットフォーム（PaaS）/インフラストラクチャとしてのサービス（IaaS）とも呼ばれる）を含む）。

Where 'cloud' or 'virtual' services are used, attention should be paid to understanding the service provided, ownership, retrieval, retention and security of data.

「クラウド」または「仮想」サービスを使用する場合、提供されるサービス、所有権、取得、保持、データのセキュリティを理解することに注意を払う必要がある。

The physical location where the data is held, including the impact of any laws applicable to that geographic location, should be considered

データが保持されている物理的な場所（その地理的な場所に適用される法律の影響を含む）を考慮する必要がある。

The responsibilities of the contract giver and acceptor should be defined in a technical agreement or contract. This should ensure timely access to data (including metadata and audit trails) to the data owner and national competent authorities upon request. Contracts with providers should define responsibilities for archiving and continued readability of the data throughout the retention period (see archive).

契約の委託者と受諾者の責任は、技術的な契約または契約で定義する必要がある。これにより、要求に応じて、データ所有者および国内の権限ある当局へのデータ（メタデータおよび監査証跡を含む）へのタイムリーなアクセスが確保される必要がある。プロバイダーとの契約では、保存期間中のデータのアーカイブと継続的な可読性の責任を定義する必要がある（アーカイブを参照）。

Appropriate arrangements must exist for the restoration of the software/system as per its original validated state, including validation and change control information to permit this restoration.

この復元を許可するためのバリデーションおよび変更制御情報を含む、元の検証された状態に従って、ソフトウェア/システムの復元に適切な取り決めが存在する必要がある。

Business continuity arrangements should be included in the contract, and tested. The need for an audit of the service provider should be based upon risk.

事業継続の取り決めを契約に含め、テストする必要がある。サービスプロバイダーの監査の必要性は、リスクに基づいている必要がある。

7　Glossary　　用語集

Acronym or word or phrase　頭字語または単語またはフレーズ	Acronym or word or phrase　頭字語または単語またはフレーズ
eCRF　eCRF	Electronic Case Report Form　電子症例報告書
ECG　心電図	Electrocardiogram　心電図
GXP　GXP	Good ‘X’ Practice where ‘X’ is used as a collective term for GDP – Good Distribution Practice, GCP – Good Clinical practice, GLP – Good Laboratory Practice GMP – Good Manufacturing Practice GPvP – Good Pharmacovigilance Practice 「X」の総称として「X」を使用する適切な「X」プラクティス GDP –医薬品の物流に関する基準 GCP –医薬品の臨床試験の実施の基準

	GLP –医薬品安全性試験実施基準 GMP –製造管理および品質管理に関する基準 GPvP –医薬品安全性監視の基準
Data Quality　データ品質	The assurance that data produced is exactly what was intended to be produced and fit for its intended purpose. This incorporates ALCOA 作成されたデータが、作成され、意図された目的に適合することを意図したものであるという保証。これには ALCOA が組み込まれている
ALCOA　アルコア	Acronym referring to Attributable, Legible, Contemporaneous, Original and Accurate. 帰属性（Attributable）、判読可能性（Legible）、同時性（Contemporaneous）、オリジナル（Original）、正確性（Accurate）を指す頭字語。
ALCOA＋　アルコア+	Acronym referring to Attributable, Legible, Contemporaneous, Original and Accurate 'plus' Complete, Consistent, Enduring, and Available. 帰属性（Attributable）、判読可能性（Legible）、同時性（Contemporaneous）、オリジナル（Original）、正確性（Accurate）に加えて、完全で（Complete）、一貫性があり（Consistent）、絵永続性があり（Enduring）、有用性がある（Available）の頭字語。
DIRA　DIRA	Data Integrity Risk Assessment　データインテグリティリスク評価
Terminology　用語	The body of terms used with a particular technical application in a subject of study, profession, etc.　学科、職業などの特定の技術アプリケーションで使用される用語集。
Data cleaning　データクリーニング	The process of detecting and correcting (or removing) corrupt or inaccurate records from a record set, table, or database and refers to identifying incomplete, incorrect, inaccurate or irrelevant parts of the data and then replacing, modifying, or deleting the dirty or coarse data. レコードセット、テーブル、またはデータベースから破損または不正確なレコードを検出および修正（または削除）し、データの不完全、不正確、または無関係な部分を識別して参照し、疑わしいまたは粗いデータを置換、変更、または削除するプロセス。。
Format　フォーマット	The something is arranged or set out　何かが整理されている
Directly accessible　直接アクセス可能	At once; without delay　すぐに;遅滞なく
Procedures　手順	Written instructions or other documentation describing process i.e. standard operating procedures (SOP) プロセス、つまり標準操作手順（SOP）を説明する書面による指示またはその他の文書
Advanced electronic signatures　高度電子署名	an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.　発信者認証の

	暗号化方式に基づく電子署名。一連のルールと一連のパラメータを使用して計算され、署名者の身元とデータインテグリティを検証できる。
Validated scanning process　検証済みのスキャンプロセス	A process whereby documents / items are scanned as a process with added controls such as location identifiers and OCR so that each page duplicated does not have to be further checked by a human. 文書/アイテムがロケーション識別子や OCR などのコントロールが追加されたプロセスとしてスキャンされ、複製された各ページを人間がさらにチェックする必要がないようにするプロセス。