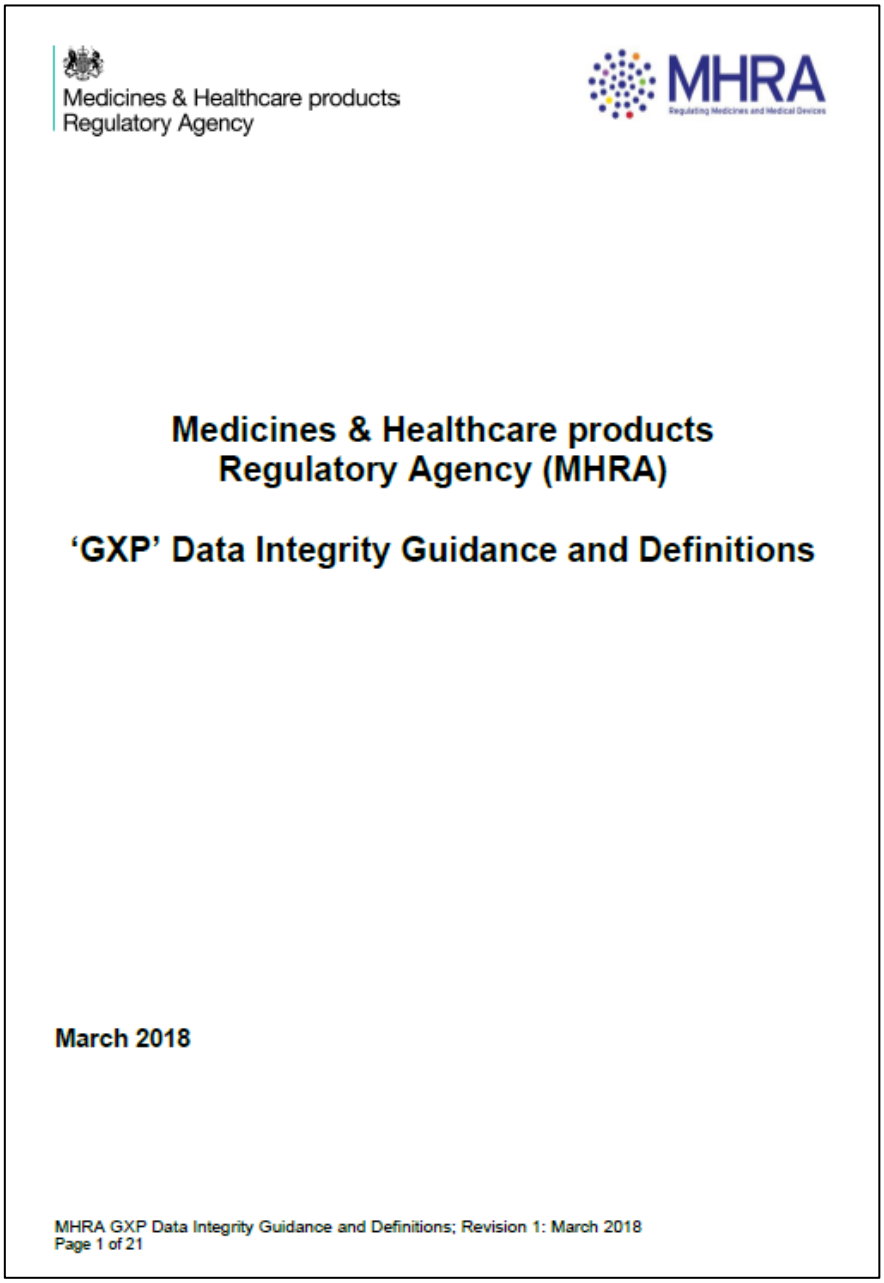
管理番号: BZLib-104

改訂番号: 1

名称: UK MHRA

'GXP' Data Integrity Guidance and Definitions

ﾍﾟｰｼﾞ数: 全 49ページ



Medicines & Healthcare products Regulatory Agency

MHRA

Regulating Medicines and Medical Devices

Medicines & Healthcare products Regulatory Agency (MHRA)

'GXP' Data Integrity Guidance and Definitions

March 2018

MHRA GXP Data Integrity Guidance and Definitions; Revision 1: March 2018
Page 1 of 21

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/687246/MHRA_GxP_data_integrity_guide_March_edited_Final.pdf

株式会社文善

改 1　　**2019 年 5 月 1 日**

管理番号: BZLib-104
改訂番号: 1
名称: UK MHRA
'GXP' Data Integrity Guidance and Definitions
ﾍﾟｰｼﾞ数: 全 49ページ

【注記】

本書は、英国 Medicines and Healthcare products Regulatory Agency (MHRA)が発行した英語原文の和文翻訳文です。本翻訳文はアズビル株式会社にて和文翻訳したものに対して、株式会社文善がアズビル株式会社の許諾を得て一部加筆修正したものです。

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

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

本書に含まれる内容は、予告なしに変更されることがあります。

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

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

【本書の表記について】

文脈に応じ説明を補足した場合、〔 〕内にそれを記述しています。

訳者による注記は段落末尾に【訳注】として追記しています。

目次

'GXP' Data Integrity Guidance and Definitions

1. Background

1. 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、それを支える技術の進歩とともに常に進化し続けている。例えば、EDC の利用が増え、システムがオートメーション化され、リモート技術が利用されるようになってきた；そして、例えばサードパーティサービスプロバイダーを経由する等、サプライチェーン及び働き方がより複雑になってきた。これらの働き方を支援するシステムは、紙の記録を用いる手動プロセスから、完全にコンピュータ化されたシステムまで、広範である。〔しかし〕規制要件の主たる目的は常に変わらない、すなわち（患者の安全と製品の品質を確実にするために）生成されるデータの品質及びインテグリティを信頼のおけるものとし、また活動を再構築できるようにすることである。

2. Introduction

2. はじめに

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.	本ガイダンスは、英国 MHRA の規制下にある、英国の産業及び公共団体（GLPMA を含む）に対してガイダンスを提供するものである。可能な限り、ガイダンスは他の発行済みのガイダンスと整合を取るようにした。本ガイダンスは英国において PIC/S、WHO、OECD（GLP のガイダンス及びアドバイスを提供する文書）及び EMA ガイドライン及び規制とともに利用するものである。

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.	本ガイダンスは MHRA 査察官及びパートナーにより作成され、公衆のコンサルテーションを受けた。本ガイダンスはユーザーが教育を通して準拠するための助けとなるよう設計され、既存の要件に対する英国の規制の解釈を明確にするものである。

2.3.

Users should ensure their efforts are balanced when safeguarding data from risk with their other compliance priorities.	データをリスクから保護するための労力は、他の適合のための優先度とバランスを取るようにすべきである。

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.	本ガイダンスの範囲は「GXP」としており、本ガイダンスに含まれる全てのものは、そうでないと明記しない限り、GXP である。特定の GXP に即した例が無くても、それはその GXP に対して有効ではないということではない。単に挙げられた例が網羅的でないだけである。ただし、本ガイダンスは医療機器には適用されないことに留意すること。

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.	本ガイダンスはデータインテグリティに関する MHRA の立場、及び準拠するための最低限の期待を理解するための手段であると考えるべきである。本ガイダンスは全てのシナリオを記載しているわけではなく、自分たちのアプローチが本ガイダンスの記載内容と異なるのであれば、MHRA へ問合せることを勧める。

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.	本ガイダンスは（データリスク、重要性、ライフサイクルを含む）データ管理において、リスクベースアプローチを推進することを目的としている。本ガイダンスのユーザーは、自分たちの一連のデータ処理を（１つのライフサイクルとして）理解し、GXP に最大の影響を与えるデータを特定する必要がある。これにより、何が最も効果的かつ効率的な、リスクベースのコントロール及びデータレビューなのかを決定し、実行する。

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.	本ガイダンスはデータ品質というよりは、主にデータインテグリティについて述べるものである。データインテグリティに必要なコントロールを設けても、データの品質を保証できるとは限らないからである。

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.	本ガイダンスを読む際には、関連する各 GXP の規制やガイダンスも併せて読むべきである。本ガイダンスで各 GXP に固有の参照（例：ICH Q9）がある場合、それらの〔参照された〕文書の基本的な考え方を考察することで、指針及びさらに深い情報が得られるであろう。

2.9.

Where terms have been defined; it is understood that other definitions may exist and these have been harmonised where possible and appropriate.	〔本ガイダンスで〕用語が定義されているが、他の定義が存在している場合、それが適切であれば、できる限りそれらの定義と整合性を取るようにした。

3. The principles of data integrity

3. 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、利用するシステム及び〔システムで〕生成されるデータに責任を持つ必要がある。データが、いかなる形式（紙、電子）であっても、完全で、一貫性があり、正確であることを確実にするような組織風土を醸成すべきである。

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.	適切な作業環境（すなわちデータインテグリティのコントロールが効果を発揮するような正しい環境）を支えるために、人、システム、設備に関する組織内の仕組みを設計し、運用し、必要に応じて変えていくべきである。

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.	組織風土、業績評価指標による行動、目的、及び上級経営層の行動が、データガバナンスの各方策の成否に与える影響を決して過小評価すべきではない。データガバナンス方針（または同等なもの）は組織の最高レベルで承認されるべきである。

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.	理論的根拠に裏打ちされたデータインテグリティリスクに基づくコントロールを受け入れ可能な状態にするような、文書化されたシステムを実装し、設計し、運用することが、組織には期待されている。適切なアプローチの 1 つの例は、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。DIRA は、データを生成またはデータを収集するプロセスを洗い出し、それぞれの形式とコントロールを特定し、データの重要度と本質的なリスクを文書化するものである。

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.	日常的にデータをチェックするために、犯罪を捜査するようなアプローチを実装することは期待していない。個々のシステムにおいては適切なレベルのコントロールを維持し、対象範囲の広いデータガバナンス方策において、定期的監査により、組織のシステム内に存在するデータインテグリティが損なわれる機会を、確実に見つけ出せるようにすべきである。

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に費やされる努力とリソースは、患者や環境に対するデータインテグリティの欠陥のリスクと影響に見合ったものとすべきである。データガバナンスのコンセプトはこれらの計画／準備を組み合わせることで実現される。

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.	自動化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したとしても、またはその逆を行ったとしても、適切なデータインテグリティコントロールが必要なことに変わりはない。

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明らかになったら、関連する全ての活動やシステムにおいて、適切な是正措置・予防措置が（単発で終わらないよう）確実に実施されるようにすべきである。

3.9.

Appropriate notification to regulatory authorities should be made where significant data integrity incidents have been identified.	重大なデータインテグリティのインシデントが明らかになった場合は、規制当局への適切な通知を行うべきである。

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.	本ガイダンスは、頭字語「ALCOA +」ではなく、「ALCOA」について述べている。ALCOA は、帰属性、見読性、同時性、原本性、正確性を示し、「+」部分は完全性、一貫性、耐久性、利用可能性を示す。 ALCOA は、歴史的に、規制目的に適したデータ品質の属性を定義するものとみなされてきた。 その後、要件を強調するために「+」が追加された。 データガバナンスの方策は、データが、データライフサイクルを通して、完全性、一貫性、耐久性、利用可能性があることを確実にすべきであることから、どちらの頭字語を用いたとしても期待することに違いはない。

4. Establishing data criticality and inherent integrity risk

データの重要度と本質的なインテグリティリスクの確立

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、有効性について意思決定するうえで、さまざまな意味で重要である。データの重要性は、データがどのように用いられ、意思決定に影響を与えているのかを考慮して決められる。

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.	データへのリスクは、〔データが〕承認されずに削除、変更、除外される可能性と、それらの活動や事象を検出できる機会によって決まる。同じようなことを繰り返す、明確に定義された、はっきりとした単一の目的を持つ単純なタスクと比較すると、制限のない、主観的な結果を伴う、複雑で、一貫しないプロセスの方が、データへのリスクは高くなると言える。

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： (i) 紙に記録されることで生成される（人による観察結果や活動の紙ベースの記録）、または (ii) 電子的に、簡単な機械から複雑な、高度に構成設定可能なコンピュータ化システムまで、広範囲にわたる機器を用いて生成される、または (iii) 紙ベースの記録と電子記録の両方がオリジナル記録を構成するようなハイブリッドシステムを用いて生成される、または (iv) 写真、画像、クロマトグラフィプレート等のような他の方式により生成される。

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 人により紙に記録されたデータは、データインテグリティリスク評価により、または他の要件により必要と判断されるならば、独立した検証を行う必要がある。リスクを低減するために〔作業を〕監督する方策を検討すべきである。
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 機器またはコンピュータ化システムに関連するデータインテグリティの本質的なリスクは、データを生成または利用するシステムがどの程度構成設定できるか、及びデータライフサイクルを通してコンピュータ化システム間でのデータ転送時にデータ操作できる可能性によって異なる。
The use of available technology, suitably configured to reduce data integrity risk, should be considered.	入手可能な技術を用いて、データインテグリティリスクを低減するように適切な構成設定にすることを検討すべきである。
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’.	構成設定できないソフトウェアで、電子データを保持しない単純な電子システム（例： pH 計、天秤、温度計）は、キャリブレーションするだけでよいが、複雑なシステムは、「意図した目的に対するバリデーション」が必要になる。

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).	（ソフトウェアの機能、構成設定、ユーザーの介入の機会、及びデータライフサイクルの検討によって決定される）複雑さとリスクに伴い、バリデーション作業が増える。複雑性が低いように見えるシステムを侮らないことは重要である。 このようなシステム（例えば、心電図計、FTIR、UV 分光光度計等のユーザーが構成設定可能な出力を持つスタンドアロンシステム）では、望ましい結果を得るためにデータを操作したり、試験を繰り返すことが可能であり、かつそのことを検出する機会が限られている。
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利用する場合、何がデータ集合全体を構成しているのかを明確に文書化し、データ集合に含まれるすべての記録をレビューして保管すべきである。ハイブリッドシステムは、期待される目的を確実に満たすように設計すべきである。
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).	その他 生成されたデータが写真や画像（または他のメディア）によって取り込まれる場合、ライフサイクルにわたってその形式を保存しておくための要件は、他の形式と同じ留意事項に従うとともに、さらにその形式に必要な追加コントロールを検討すべきである。 劣化の問題のために元の形式を保持することができない場合、記録を残すための代わりの仕組み（例えば、写真やデジタル化）及びその後の保存について検討し、選択した根拠を文書化すべきである。（例えば、薄層クロマトグラフィ）。

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.	高レベルのシステムアクセス権限または専門的ソフトウェア／知識を持たない限り〔データを〕変更できないようなプロセスから得られたデータで、データの製品／患者／環境への影響が小さいものでは、コントロール方策を軽くしたり、コントロール頻度を下げることを正当化できるかもしれない。

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（または同等なもの）では、プロセスに従ったり、機能を実行したりするために、何が必要となるのかを考える。コンピュータ化システム単体だけでなく、それを支える人、ガイダンス、トレーニング、品質システムも考慮することが期待される。従って、オートメーションや「バリデートされたシステム」（例えば、e-CRF、分析機器）の利用により、データインテグリティリスクを低減させることはできるが、全く無くすことはできない。 人が介入する場合、とりわけ、どのように、どのデータを記録、報告、保管するのか〔の決定〕に〔人が〕影響を及ぼせるような場合、システムがバリデート済みであることに過度に信頼していると、不適切な組織のコントロールやデータ検証によりリスクが高くなってしまうことがある。

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により是正すべき領域が明らかになったところで、アクションの優先付け（適切なレベルの残存リスクの受容を含む）を文書化し、経営層に伝え、レビューの対象とすべきである。長期的な是正措置が特定されたら、リスクを低減するための短期的措置を実施し、受け入れ可能なデータガバナンスを暫定的に提供すべきである。

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ようなシステム及びプロセスを設計する；'適正な環境を作る'

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:	システムとプロセスは、データインテグリティの原則に準拠するように設計すべきである。望ましい行動がとられるようにするための実現要素には以下が含まれるが、これに限定されるものではない。
• 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.	• 再構築及びトレーサビリティを可能とするために、適切にコントロールされた／同期されたクロックを用い、〔データを〕利用した時点で、時刻の付されたイベントを記録すること。このデータが複数のサイトにまたがって利用される場合、タイムゾーンを認識し、指定すること。
• Accessibility of records at locations where activities take place so that informal data recording and later transcription to official records does not occur.	• データを非公式に記録し、後でそれを公式記録に転記することのないように、活動が行われる場所で記録にアクセスできるようにすること。
• 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.	• 生データ／原データ記録用のブランク書式へのアクセスを適切にコントロールすべきである。記録をねつ造されないようにするには、員数チェック、つまりページ付の管理されたブックの利用が必要であろう。これには例外があるかもしれない。例えば、医療記録（GCP）ではこれが現実的ではない。

• 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.	• ユーザーアクセス権により、認可されていないデータ変更を防止する（または防止が不可能な場合は、監査証跡を残す)。コンピュータ化システムへの手動のデータ入力やコンピュータ化システムと人とのやりとりを無くすための外部装置またはシステムインターフェース方式（バーコードスキャナー、ID カードリーダー、プリンター等）を利用する。
• 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.	• 要求されるタスクを実行し、データを記録することができるような作業環境（適度な空間、作業のための十分な時間、適切に機能する機器等）を提供する。
• Access to original records for staff performing data review activities.	• データレビュー活動を行うスタッフがオリジナル記録へアクセスできるようにする。
• Reconciliation of controlled print-outs.	• コントロールされた印刷結果について員数チェックを行う。
• Sufficient training in data integrity principles provided to all appropriate staff (including senior management).	• 全ての適切なスタッフ（上級経営層も含む）に対して、データインテグリティの原則について十分なトレーニングを実施する。
• Inclusion of subject matter experts in the risk assessment process.	• リスク評価プロセスへ対象分野の専門家（SME）が参加する。
• Management oversight of quality metrics relevant to data governance.	• データガバナンスに関する品質メトリクスを経営層が監督する。

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.	活動を記録する記録者を、操作者の代わりに用いることは、正当性があれば検討してもよい。 例えば： • 〔操作者が、活動と〕同時に記録を取ることで、製品または活動を損なってしまう場合。 例えば、無菌医薬品製造の運転員がラインへ介入したことを文書化する。 • 剖検（GLP） • 文化やリテラシー／言語の制限に対応する場合。 例えば、操作者が活動を行い、第二者が立ち会い、記録する。
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.	その活動について、データの重要性に応じた適切なコントロールを確実にするとともに、アクセスのしやすさ、使いやすさ、及び場所に配慮すべきである。
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〔活動を第二者が記録する〕状況で、第二者による記録作成は、実行されるタスクと同時に行われるべきであり、記録には、タスクを実行する者と記録を完成させる者の両方を明記すべきである。〔また、〕可能な限り、タスクを実行する者が記録に連署すべきであるが、この連署は事後に行うことが認められている。監視者（記録者）が文書を完成させるプロセスは、そのプロセスに係る活動を記載する、承認された手順書に記載すべきである。

6. Definition of terms and interpretation of requirements

用語の定義と要件の解釈

6.1. Data

6.1. 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.	*参照または解析のために集められた事実、数値、統計。すべてのオリジナル記録及びオリジナル記録の真正コピーであり、原データとメタデータを、及びそれらのデータのその後の変換結果及びレポートを含む。これらは、GXP 活動実施時に生成・記録され、GXP 活動を完全無欠に再構築及び評価に利用することができるものである。* 【訳注：原文では、定義を斜体字で示している。以下同様。】
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	データは以下のようであるべきである： A - データ生成者へ帰属することができる L – 見読性があり、永続的である C – 同時性がある O – オリジナル記録（または保証付きの真正コピー）である A - 正確である
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	また、データガバナンス方策によりデータが complete で、consistent で、enduring で、かつライフサイクルを通じて available であるべきである。ここで； Complete – データは〔部分でなく〕全てであり、全部そろった一式でなければならない Consistent - データは自己一貫性を持たなければならない Enduring – 耐久性があり、データライフサイクルを通じて存続する Available – レビューや査察のために、すぐに入手可能である

6.2. Raw data (synonymous with 'source data' which is defined in ICH GCP)

6.2. 生データ（ICH　GCP で定義される原データと同義）

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、（紙または電子的のいずれに記録されたかに依らず）情報を最初に収集したものとでも説明できるような、オリジナルな記録（データ）である。もともと動的状態で収集された情報は、動的状態で利用できるようにしておくべきである。*
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'.	生データを使って、活動を完全に再構築できなければならない。〔生データが〕動的状態で収集され、かつ電子的に生成された場合、紙のコピーは「生データ」と考えることはできない。
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.	電子データを格納しない、またはデータを印刷するだけの基本的な電子機器（例：天秤、pH 計）の場合、印刷されたものが生データとなる。〔余分な機能を持たない〕基本的な電子機器が、データを永続的に格納せず、一定量のデータが上書きされるまで保持されるような場合、データを定期的にレビューし、必要に応じて紙の記録と照合するとともに、（機器がサポートしていれば）電子データとして抽出すべきである。
In all definitions, the term 'data' includes raw data.	全ての定義において、「データ」という言葉は生データを含むものとする。

6.3. Metadata

6.3. *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).	*メタデータとは、あるデータの属性を説明し、そのデータのコンテキストや意味を示すものである。一般的に、これらはデータの構成、データ要素、データの相互関係等の特性を示すデータである。一例を挙げれば監査証跡である。メタデータにより、データを個人（または自動的に生成された場合、元のデータ源）に帰属させることもできる。*
Metadata form an integral part of the original record. Without the context provided by metadata the data has no meaning.	メタデータはオリジナル記録の不可欠な一部分である。メタデータが提供する補足情報が無ければ、データは何の意味を持たない。
Example (i) 3.5 metadata, giving context and meaning, (italic text) are: *sodium chloride batch* 1234, 3.5*mg. J Smith 01/Jul/14*	例 (i) 3.5 メタデータが（斜体字で示される）補足情報と意味を与えている： *sodium chloride batch* 1234, 3.5*mg. J Smith 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.* 3.5*mg. Analyst: J Smith 01/Jul/14*	例 (ii) 3.5 メタデータが（斜体字で示される）補足情報と意味を与えている： *Trial subject A123, sample ref X789 taken 30/06/14 at 1456hrs.* 3.5*mg. Analyst: J Smith 01/Jul/14*

6.4. Data Integrity

6.4. 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、矛盾無く、正確で、信用でき、信頼でき、かつデータのこれらの特性がデータライフサイクルを通じて維持される程度である。データを、帰属性があり、見読性があり、同時性があり、オリジナル（または真正コピー）であり、かつ正確であるようにするために、データをセキュアな方法で収集、維持すべきである。データインテグリティを保証するためには、適切な品質とリスクの管理システム（健全な科学的な原則と優良文書化実践規範 (Good Documentation Practice)を遵守することを含む）が必要である。*

6.5. Data Governance

6.5. 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.	*データライフサイクルを通して、データが、形式に拘わらず、完全で矛盾なく正確であることを保証するように、データを確実に記録、処理、保管、使用するための計画／準備すること。*
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.	データガバナンスでは、ライフサイクルを通してデータオーナーシップと責任を明らかにするとともに、データインテグリティの原則に適合するためのプロセス／システム（故意または意図しないデータ変更に対するコントロールを含む）の設計、運用及び監視について検討すべきである。
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、以下を含むべきである。 • データインテグリティ原則の重要さに関するスタッフへのトレーニング、及び • 見通しがよく〔透明性のある〕、かつエラー／作業漏れ／望ましくない結果を積極的に報告するような作業環境の構築

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.	上級経営層はデータインテグリティの潜在的なリスクを最小化するようなシステムや手順書を実装し、ICH Q9 の原則のようなリスク管理手法を用いて残存リスクを特定することに責任を持つべきである。
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.	契約の委託者は、サードパーティとの全ての契約／技術合意書に、データのオーナーシップ、ガバナンス、及びアクセス可能性を盛り込むようにすべきである。さらに契約の委託者は、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を実施すべきである。
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により、当局からの求めに応じ、確実にデータをすぐに取り出すことができ、かつ直接アクセスできるようにすべきである。電子データは見読性のある形式で入手できるようにすべきである。

6.6. Data Lifecycle

6.6. データライフサイクル

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・記録されてから、（分析、変換、移行等の）処理、利用、データ保管、アーカイブ／取出し、破棄に至るまでのデータライフ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.	前章で述べたように、データインテグリティを保証するためには、データガバナンスをデータライフサイクル全体に対して適用しなければならない。データは適切なコントロール下にあるオリジナルシステム【訳注】または適切なアーカイブにおいて保管される。 【訳注】上記「オリジナルシステム」は、データが最初に生成されたシステムである。

6.7. Recording and collection of data

6.7. データの記録及び収集

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.	組織において、データ収集及び記録のために用いるシステムについて、適切なレベルのプロセスの理解と技術的知識（能力、限界、脆弱性を含む）を持つべきである。
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.	選択された方法を用いて、適切な正確性、完全性、内容と意味を持つデータが、意図した用途のために収集され、保管されるようにすべきである。電子システムが動的に格納できる場合、動的（電子）データの代わりに静的（印刷／手書き）データを保持することは適切ではない。データを用いて活動を完全に再構築する必要があり、収集するデータの量及び粒度（詳細さの程度）が妥当であるとする根拠を示すべきである。
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.	ブランク書式（ワークシート、ラボラトリノートブック、マスター生産／管理記録を含む）を用いるときは、コントロールすべきである。例えば、番号を付したブランク書式のセットを発行し、利用終了後に〔全て揃っているか〕照合チェックする。同様に、ページの振られた、綴じられたノートブックに、文書管理グループがスタンプを押したり、正式に発行したりすることで、非公式なノートブックやノートブックのページ欠落を検出することができる。

6.8. Data transfer / migration

6.8. 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、異なるデータ格納タイプ、異なる形式または異なるコンピュータ化システムの間で、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.	*データ移行は、ある永続的な格納ロケーションから他へ移動するプロセスである。このとき、データ形式は変わるかもしれないが、内容や意味は変わらない。*
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、異なる格納媒体タイプまたは異なるコンピュータ化システムの間で、データ及びメタデータを転送するプロセスである。データ移行は、必要な場合、代替となるコンピュータ化システムにおいて利用可能または閲覧可能とするために必要に応じてデータ形式を変更する。
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／移行の手順書には、なぜやるのかの理由を明確にする。データ転送／移行の手順は、堅固に設計し、バリデートすることで、データライフサイクルを通してデータインテグリティが確実に維持されるようにする。十分検討して、データの形式、及びデータの生成、転送から格納に至る各段階で〔データが〕変更される可能性、を理解すること。データ移行における課題、特に移行される記録の意味を完全に保つうえでの課題は過小評価されがちである。
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.	データ転送はバリデートすべきである。データは、ワークシートや他のアプリケーションに転送される間もその後も、変更されるべきではない。このプロセスには監査証跡が必要である。業務の中でデータ転送が正しく行われなかった場合、適切な品質手順に従うべきである。中間階層のソフトウェアにおける〔データ〕変更は、適切な品質管理システムにより管理されるべきである。
Electronic worksheets used in automation like paper documentation should be version controlled and any changes in the worksheet should be documented/verified appropriately.	オートメーションで利用される電子ワークシートは、紙の文書同様に、版管理されるべきであり、ワークシートにおける変更は適切に記録され、検証されるべきである。

6.9. Data Processing

6.9. 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	*情報を、定義された形式で抽出、提示、入手するためにデータに対して行われる連続した操作。例としては、傾向を提示するための患者データの統計解析、生電子シグナルからクロマトグラムへ、及びその後の計算された数値結果への変換、等が挙げられる。*
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活動において使われるユーザー定義パラメータについては、適切なトレーサビリティ（誰がその活動を実施したかという属性を含む）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.	処理結果が後でレポートに用いられるか否か、または規制や業務の目的で利用されるか否かに拘わらず、監査証跡及び保管された記録により、全てのデータ処理活動を再構築できるようにすべきである。処理パラメータを逐次変更して、データ処理を繰り返す場合、それを可視化することにより、望ましい結果を得るための処理パラメータ操作をしていないことを確認すること。

6.10. Excluding Data (not applicable to GPvP):

6.10. データの除外 (GPvP は適用外)

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的ガイダンスを提供する医薬品安全性の法律（GVP モジュールを含む）を参照する。

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.	データが、計測、サンプリングまたは取得した数量を表すものではないことを、有効で科学的な正当性を示せる場合に限り、そのデータを除外してもよい。 そのようなときは必ず、その正当性を文書化し、データレビュー、及び報告時に検討すべきである。全てのデータ（除外されたものも含めて）をオリジナルデータセットとともに保管すべきであり、レビュー時に、データを除外するという判断が正しかったのか確認できるような形式で利用できるようにすべきである。

6.11. Original record and true copy

6.11. オリジナル記録と真正コピー

6.11.1. Original Record

6.11.1. オリジナル記録

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.	*最初に、またはデータ源として収集されるデータや情報である、例えば、手動〔プロセスにおける手書き〕観察結果のオリジナルの紙の記録、コンピュータ化システムからの電子生データファイル、及びその後に作成される GXP 活動を完全に再構築するために必要な全てのデータ。オリジナル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.	紙や静的形式の電子記録【訳注】などの静的記録形式は、〔内容が〕固定されており、ユーザーと記録内容との間のやりとりをほとんど、または全く受け付けない形式である。例えば、一度印刷または静的電子記録に変換されたクロマトグラフィの記録では、再処理する能力やベースラインをさらに詳細に見る能力が失われている。 【訳注】冒頭の原文をそのまま訳すと「紙や電子記録のような静的記録形式」となるが、電子記録は静的記録形式とは限らないため、上記のように意訳した。

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.	動的形式の電子記録【訳注】は、ユーザーが記録内容に対してやりとりができる。例えばデータベース形式の電子記録では、ユーザーは、データを追跡し、トレンドを取り、問合せることができる。電子記録として維持されているクロマトグラフィの記録は、（適切なアクセス権限を持つ）ユーザーやレビュー者が、データを再処理したり、ベースラインを拡大して積分をはっきりと見ることができる。原データのオリジナルコピーを保持することが現実的ではない、または不可能な場合（例：データ源となる機器が治験依頼者の管理下になく、操作者がサマリ統計データのみを提供する場合の MRI スキャン）、リスクとその低減策を文書化すべきである。 【訳注】冒頭の原文をそのまま訳すと「電子記録のような動的記録形式」となるが、電子記録は動的記録形式とは限らないため、上記のように意訳した。
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.	データを取得するに当たって、人が観察し記録する必要がある場合（例えば、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、重大さに応じて、第二の同時的な検証チェックの必要性を証明すべきである、またはその検証結果を別の方法で取得することができるか調査すべきである。

6.11.2. True copy

6.11.2. 真正コピー

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.	*オリジナルと同じ情報（補足情報、内容、及び構造を示すデータを含む）を持つことが検証された（すなわち、日付入りで署名された、またはバリデートされたプロセスで生成された）オリジナル記録の（用いられる媒体の種類に依らない）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.	真正コピーは、必要であれば、オリジナル記録とは異なる電子ファイル形式で格納してもよいが、データの意味が完全に維持され、その履歴が再構築できることを確実にするために、メタデータ及び監査証跡を保持しなければならない。
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.	オリジナル記録と真正コピーは、記録のインテグリティを保存しなければならない。コピーのインテグリティを検証し、記録する、文書化されたシステムを用いるのであれば、オリジナル記録に代えて、オリジナル記録の真正コピーを保管してもよい（例：紙の記録のスキャン）。オリジナル記録を破棄した場合のリスクは、組織において検討すべきである。
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')	レビュー、バックアップ、アーカイブを行うために、電子データ（関連するメタデータを含む）の真正コピーを作成できるべきである。〔真正〕コピー〔であること〕を保証するような正確かつ完全なコピーには、データの意味（データ形式、補足情報、レイアウト、電子署名、及び認可等）と完全な GXP 監査証跡を含むべきである。〔また〕保存期間を通しての「真正コピー」の動的機能について検討すべきである。（「アーカイブ」参照のこと。）

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.	インテグリティを確保するため、または後で検証するために〔動的形式であることが〕重要となる場合、データは動的形式で保管しなければならない。コンピュータ化システムを維持管理できない場合（例えば、サポート期間が終わった場合）、コンピュータ化システムを廃棄する前に、記録を文書化されたアーカイビング方策に基づきアーカイブすべきである。 静的記録であってもオリジナルデータのインテグリティが維持されることを証明できる場合、電子的な手段で生成されたデータを、受入可能な紙または電子形式で保管することが考えられる。しかしながら、データ保管プロセスに以下が含まれていることを示さなければならない。 • 全ての生データ、メタデータ、関連する監査証跡とその結果のファイルの検証されたコピー、 • 各記録に関するソフトウェア／システムの構成設定の変数、及び • 任意の生データセットの再構築に必要な全てのデータ処理実行（メソッド及び監査証跡を含む） また、印刷された記録が〔記録を〕正確に表わすものであることを検証する、文書化された方法が必要である。GXP に適合する記録とするためには、このアプローチは管理的に実施が難しいかもしれない。
Where manual transcriptions occur, these should be verified by a second person or validated system.	人が転記する場合、第二者またはバリデートされたシステムにより検証すべきである。

6.12. Computerised system transactions:

6.12. コンピュータ化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.	*コンピュータ化システムトランザクションは、1 つの論理的な「作業単位」として実行される単一の操作または連続した操作である。トランザクションを構成する各操作は、ユーザーがその処理を意図的な行為（例：保存ボタン押下）によりコミットするか、システムがデータ保存を強制するまでは、耐久性のある格納装置に、永続的な記録として保存されない。*
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.	ユーザーが処理を耐久性のある格納装置に保存するまでは、メタデータ（例：ユーザー名、日付・時刻）はシステムの監査証跡に記録されない。コンピュータ化システムによっては、記録を保存し、永続的なものにする際に電子署名が必要な場合がある。
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は、被験者の安全、または製品やデータの品質を確実にするために適切な限界、範囲、分布に収まっていなければならない。コンピュータシステムは、クリティカルステップの実行を遅滞なく確実に記録するよう設計すべきである。トランザクションシステムを利用する場合、複数の単位操作を組み合わせて 1 つのトランザクションとすることは避けるべきであり、データ保存するまでの時間間隔は最小限にすべきである。システムは、ユーザーに変更を促す前に、データを永続的メモリへ保存することを促すように設計すべきである。

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.	組織において、システムの開発期間中に、（例えばユーザー要求仕様書を用いて）システム機能と関連するリスクレベルに基づき、どれをクリティカルステップにすることが適切であるかを決めるべきである。クリティカルステップは、システム設計（防止策）、プロセス監視、及びレビューを考慮したプロセスコントロールとともに文書化すべきである。活動を監視することで、プロセス設計で対応していない不適合を見つけ出すようにすべきである。

6.13. Audit Trail

6.13. 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 記録の生成、変更、削除に関するアクションに係る情報を含むメタデータの一形態である。監査証跡は、紙か電子に拘わらず、記録に含まれる情報についての生成、追加、削除、変更等のライフサイクルにわたる詳細を、オリジナルな記録を不明瞭にしたり、上書きすることなく、セキュアに書き留めるものである。監査証跡により、記録の媒体を問わず、記録に関連する事象（「誰が、何を、いつ、なぜ」アクションを行ったのかといった情報を含む）の履歴を再構築することができる。*

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.	生データを電子的に収集、処理、報告、格納、アーカイブするためにコンピュータ化システムを用いる場合、システムが常に監査証跡を保持し、それによりデータへの全ての変更または削除を示すことができ、かつ以前のデータ及びオリジナルのデータも保持しておくよう設計すべきである。全てのデータ及びデータへの変更は、その変更を行った者に関連づけられるようにすべきであり、変更は日付、及びタイムスタンプ（時刻、及び必要に応じてタイムゾーン）を付すべきである。また、変更の理由も記録すべきである。監査証跡に含める項目は、プロセスや活動を再構築するために有効なものとすべきである。
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.	（リスク評価で必要と判断されたならば）監査証跡を起動しておくべきである。ユーザーが監査証跡の記録を変更できたり、監査証跡を停止できたりしてはいけない。システムアドミニストレーターが監査証跡を変更または停止したときは、そのアクションの記録を保持すべきである。
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.).	組織において、監査証跡にどのデータを記録すべきかを検討し、強固なデータレビュー／検証ができるようにすべきである。監査証跡のレビューにおいて、全てのシステムに関する活動（例：ユーザーログオン／ログオフ、キー操作等）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.	（レガシーシステム等で）有効な監査証跡機能が無い場合、例えば SOP でプロセスを定め、ログブックを用いる等の代替的コントロールを設けてもよい。代替的コントロールは、それが効果的であることを証明すべきである。

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]	現時点でアドオンソフトウェアまたは適合するシステムが存在しない場合、レガシーシステムを使い続けるためには、適合するソリューションを探索中であり、一時的に講じたリスク低減策によりシステムを継続利用していることを、文書化された証拠で示すことで、正当化できるかもしれない[1]。
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	日常的なデータレビューには、文書化された監査証跡レビューを含むべきであり、これはリスク評価によって決定する。監査証跡レビューの仕組みを設計する際、GXP 関連のものに絞ってもよい。監査証跡は関連するデータの一覧としてレビューしてもよいし、「例外報告」プロセスを用いてもよい。例外報告はバリデートされた検索ツールであり、予め定められた「異常」なデータやアクションを特定し、書き出すものであり、それを後でデータレビュー者が注意深く見たり、調査したりする。
Reviewers should have sufficient knowledge and system access to review relevant audit trails, raw data and metadata (see also 'data governance').	レビュー者は、関連する監査証跡、生データ及びメタデータをレビューできるよう、十分な知識及びシステムへのアクセス権限を持つべきである。（「データガバナンス」も参照のこと）

[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).
[1] 産業オートメーション、プログラマブルロジックコントローラーのような制御機器／システムを持つ GMP 施設は、個人別のログイン及び監査証跡ができるようなシステムへアップグレードしようとしていることを実証することが期待されている。(Art 23 of Directive 2001/83/EC 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やユーザーアカウントについての期待に応えられない場合、これらの欠点に対する取り組みの進捗を示すことができるようにすべきである。この取り組みとは、追加的機能を提供するアドオンソフトウェア、または適合するシステムへのアップグレードのいずれかである。是正措置が定められていない、または〔是正措置が定められた〕後でタイムリに実施されていない場合、不適合と指摘される可能性がある。

6.14. Electronic Signatures

6.14. 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.	署名したことを表す、デジタル形式（バイオメトリックまたは非バイオメトリック）の署名。これは法律用語として、署名として用いる手書き署名と同等である。
The use of electronic signatures should be appropriately controlled with consideration given to:	電子署名の利用にあたって以下を考慮し、適切にコントロールすべきである。
• How the signature is attributable to an individual.	• 署名がどのように個人に帰属するか。
• 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.	• どのように「署名」行為をシステムに記録すれば、署名〔された記録〕を変更したり、操作しようとしたときに、署名または入力状態を無効にすることができるか。
• How the record of the signature will be associated with the entry made and how this can be verified.	• どのように署名の記録が入力と関連付けられ、どのようにそのことが検証できるか。
• The security of the electronic signature i.e. so that it can only be applied by the 'owner' of that signature.	• 電子署名のセキュリティ、すなわち署名の「オーナー」のみにより実行される。

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.	署名された記録が適切であり、コントロールが維持されていることを示すために、当該システムに関連する署名プロセスを適切にバリデートすることが期待される。電子的に署名された文書の紙または PDF のコピーが生成された場合、この文書とともに、電子署名に関連するメタデータが維持管理されるべきである。
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).	電子署名の利用にあたっては国際標準の要件に適合すべきである。高度電子署名を利用する場合、リスク評価によりその認証方法の必要性を検討すべきである。 電子署名または E-サインは「署名の明示情報」、すなわち見読性のある記録の中に、署名者名、その肩書、日付（それが重要であれば時刻も）、及び署名の意味（例：検証、承認）を示す表示、を含まなければならない。
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.	署名のイメージを挿入したり、脚注で文書が電子的に署名されたことを示すことは（それがバリデートされた電子署名プロセス以外の方法で入力された場合）適切ではない。文書が電子的に署名された場合、署名に係るメタデータが保管されるべきである。
For printed copies of electronically signed documents refer to True Copy section.	電子的に署名された文書を印刷したコピーについては真正コピーの章を参照。
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に係る電子署名への期待 (GCP) については別のガイダンス (MHRA/HRA DRAFT Guidance on the use of electronic consent) で述べる。

6.15. Data review and approval

6.15. データのレビュー及び承認

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、（紙の記録の）取り消し線、（電子記録の）監査証跡等、特定の記録内容をレビューするためのアプローチは、全ての適用される規制要件を満たし、かつリスクに基づくべきである。
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.	データをレビュー、及び承認するためのプロセスを説明する手順書を設けるべきである。データレビューでは、関連するメタデータ（関連する監査証跡も含む）もリスクに基づいてレビューすべきである。データレビュー結果は文書で残し、そこには見つかった課題の有無に関する事実の記述、レビュー実施日付及びレビュー者の署名を記載すべきである。
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).	手順書には、データレビューで誤りまたは抜けを見つけたときに取るべきアクションを記載すべきである。この手順により、ALCOA 原則（「データ」の定義参照のこと）に沿って、オリジナル記録が何であったかを知ることができ、かつ変更を追跡できるようにすべきである。
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.	データ生成組織内でデータレビューを行わない場合、データレビューの責任を、文書により〔データ生成組織とデータレビュー組織の〕両者で合意すべきである。組織（契約委託者と受託者）間でデータのサマリレポートが提供されることが多いが、サマリレポートは〔内容が〕限定されており、重要なデータやメタデータが含まれないことがあることに留意すべきである。

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.	ソフトウェアパッケージでは設定によりレポートをカスタマイズできるものが多い。バリデート済みで、かつ変更されないようにロックできるのであれば、主要なアクションをレポートに取り込んでもよい。自動レポーティングツール及び〔その結果生成される〕レポートを用いることで、データのインテグリティを保証するためのチェックを軽減できるかもしれない。
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.	別の組織からサマリレポートが提供される場合、レポートを受け取るデータ利用組織は、その情報を利用する前に、データ提供者のデータインテグリティのコントロール及びプロセスを評価すべきである。
• 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?	• 日常的なデータレビューでは、それぞれのデータセットのインテグリティを検討すべきである。例えば： • 当該活動で生成された唯一のデータであるか？ • 正しくデータが生成され維持管理されているか？ • 認可されない変更が行われた形跡が無いか？
• 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?	• 生成されたデータに対する定期的監査（電子的に生成されたデータのレビューと、組織のより広範囲なレビューをカバーする）では、現在のコントロール方策の効果を検証し、全ての〔人の介在する〕場面において認可されない活動が起こり得た可能性を検討すべきである。例えばレビュー後のデータに変更を求める IT 要求があったか？システム保守活動があったか、その活動の影響について評価したか？

6.16. Computerised system user access/system administrator roles

6.16. コンピュータ化システムにおけるユーザーアクセス／システムアドミニストレーターの役割

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).	アクセスコントロールをフルに活用することで、各個人が自分の役割に合った機能のみにアクセスできるようにし、そのアクションを特定の個人に帰属できるようにすべきである。各社は各スタッフに与えたアクセスレベルを提示できるようにし、かつユーザーのアクセスレベルの履歴情報を入手できるようにしなければならない。システムでこのようなデータを収集できない場合、システムの外で記録を維持しなければならない。アクセスコントロールは、オペレーティングシステム、及びアプリケーションの両方のレベルで設けるべきである。データインテグリティを確実にするような適切なコントロールがあれば（例えば、アプリケーションを使わない限り、データの変更、削除、生成ができないようにする）、オペレーティングシステムのレベルで個人別にログインさせる必要はないかもしれない。
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、変更、格納するシステムにおいて、共有ログインや〔'User'のような〕一般名を用いたユーザーアクセスは利用すべきではない。コンピュータ化システムが個人別のユーザーアクセスをサポートするよう設計されているのであれば、その機能は利用しなければならない。これにより追加ライセンスを購入する必要があるかもしれない。（MRP システムのように）全体が GXP 目的に利用されるわけではないものの、GXP が適用される要素（例えば、認定された業者、在庫のステータス、場所、取引履歴）を含むシステムには、適切な評価とコントロールが必要である。

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].	シングルユーザーログインまたは限られた数のユーザーログインしかサポートしていないコンピュータ化システムがあることは承知している。適切な代替コンピュータ化システムが入手できない場合、サードパーティソフトウェアまたはトレーサビリティが取れる（版管理付きの）紙ベースの方法により、同等のコントロールを得られるかもしれない。代替システムの適切さは正当化し、文書化すべきである。ハイブリッドシステムは、帰属の不明瞭なデータ変更が起きやすいことから、データレビューの回数を増やす必要があるかもしれない[2]。
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.	システムアドミニストレーターのアクセス権は、組織の規模と性質を考慮し、最小限の人数に限定すべきである。〔'Admin’ のような〕一般名を用いたシステムアドミニストレーターアカウントは、通常は利用可能とすべきではない。システムアドミニストレーターアクセス権を持つ者は、監査証跡によりアクションを個人に帰属できるように、ユニークな認証情報でログインすべきである。これは、潜在的に相反する利益を持つユーザーがアクセスし、操作者を特定できないような認可されない変更をすることを防ぐためである。
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).	（データ削除、データベースの変更やシステム構成設定の変更等の活動を許可する）システムアドミニストレーターの権限はデータに直接の利害関係を持つ者（データ生成、データレビューまたは承認）には割り当てないこと。

[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).
[2] 産業オートメーション、プログラマブルロジックコントローラーのような制御機器／システムを持つ GMP 施設は、個人別のログイン及び監査証跡ができるようなシステムへアップグレードしようとしていることを実証することが期待されている。(Art 23 of Directive 2001/83/EC 参照)

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.	治験データの状態によって個人のアクセス権限を変更する必要があるかもしれない。例えば、データマネジメントプロセスが完了した後で、データ編集権限を除くことによりデータが「確定」される。このことはシステム内で実証できるようにすべきである。

6.17. Data retention

6.17. データ保管

Data retention may be for archiving (protected data for long-term storage) or backup (data for the purposes of disaster recovery).	データ保管にはアーカイビング（長期保管用の保護されたデータ）とバックアップ（災害復旧のためのデータ）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).	データと文書の保管の計画／準備により、記録を故意または事故による変更や喪失から確実に保護するようにすべきである。記録のデータインテグリティを、保存期間を通して確保するようなセキュアなコントロールを設けなければならず、また必要に応じてバリデートすべきである。（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（または真正コピー）は、出力が確実に真正コピーとなるような、文書化されたプロセスが設けられていれば、バリデートされたスキャンプロセスを用いて保管してもよい。
Procedures for destruction of data should consider data criticality and where applicable legislative retention requirements.	データを破棄するための手順書では、データの重要度、及び必要に応じて法的な保管要件を検討すべきである。

6.17.1. Archive

6.17.1. 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.	*プロセスまたは活動を検証する目的で、データ及びメタデータを長期間にわたって保管するための（キャビネット、部屋、建物、コンピュータ化システム等の）、指定されたセキュアな場所または設備*
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.	アーカイブされる記録はオリジナル記録または「真正コピー」であり、変更または削除したときは必ず検出されるよう保護すべきであり、火事や害虫等の偶発的損傷からも保護されるべきである。
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.	アーカイブの計画／準備では、必要な保管期間を通じて、復元でき、データとメタデータが読めるように設計すべきである。電子データをアーカイビングする場合、プロセスをバリデートすべきである。レガシーシステムの場合、データをレビューできることは定期的に検証（すなわち、レガシーシステムのサポートが継続していることを確認）すべきである。ハイブリッド記録を保存する場合、物理的な記録と電子記録との間の参照関係を維持し、保管期間を通じて事象を完全に検証できるようにしなければならない。
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.	レガシーシステムがサポートされなくなるときに、データにアクセスし続けられるように、ソフトウェアを（保管期間に応じて、できる限り）維持し続けるかどうかを検討すべきである。これはソフトウェアを仮想環境で維持することで達成できるかもしれない。

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').	レガシーデータが古くなるにつれ、「真正コピー」のデータ属性をなるべく多く持つ代替ファイル形式に移行することが必要となるかもしれない。オリジナルデータの機能を完全に移行することが技術的に不可能な場合、将来にわたってのデータのリスクと重要性に基づいて選択肢を評価すべきである。移行するファイル形式は、長期にわたりアクセスできることと、(例えば、データ問合せ、トレンド、再処理、等の) 動的なデータ機能が失われること、のリスクのバランスを考慮して選択すべきである。アクセス性を維持するためには、いくつかの属性、及び／または動的データ機能の無いファイル形式に移行せざるを得ないということは承知している。(「データ移行」も参照のこと)

6.17.2. Backup

6.17.2 バックアップ

A copy of current (editable) data, metadata and system configuration settings maintained for recovery including disaster recovery.	*現在の (編集可能な) データ、メタデータ及びシステム構成設定情報のコピーであり、災害復旧を含む復元のために維持されるもの。*
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はバリデートし、定期的にテストすべきである。個々のバックアップが正しく機能したことを確実にするために (データサイズがオリジナル記録と一緒であるかを確認する等により) 検証すべきである。
The backup strategies for the data owners should be documented.	データオーナー向けのバックアップ戦略を文書化すべきである。
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.	復元目的のバックアップを持っていても、プロセスや活動の検証のために行う、データ及びメタデータの、最終的な形式による長期間保管の必要性が無くなるわけではない。

6.18. File structure

6.18. 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を実施するためにはファイル構造を明確に理解しておく必要がある。GXP 環境におけるデータ構造の在り方はデータが何に利用されるかによって決まるが、エンドユーザーは利用可能なソフトウェア／コンピュータ化システム〔の制限〕に従っているだけかもしれない。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.	異なるファイル構造には、その属性により、異なるコントロールやデータレビュー方法が必要となり、またメタデータが異なる方法で保持されるかもしれない。

6.19. Validation – for intended purpose (GMP; See also Annex 11, 15)

6.19. バリデーション - 意図した目的に対して（GMP; Annex11, 15 も参照のこと）

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、規制要件及び関連するガイダンスに準拠すべきである。これら〔のシステム〕は、意図した目的に対してバリデートすべきであるが、この目的を決めるためにはプロセスにおけるコンピュータ化システムの機能を理解する必要がある。この理由から、供給者によって提供されるバリデーションデータは、それがシステムの構成設定及びユーザーの意図した用途から切り離されている場合は、受け入れられない。利用するプロセスやエンドユーザーの IT インフラストラクチャから切り離された場合、ベンダーのテストは機能の検証のみとなりがちであり、性能適格性評価の要件を満たさないかもしれない。

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.	機能の検証は、要求された情報が一貫性をもって、完全に提示されることを証明するものである。意図した目的に対するバリデーションは、〔例えば〕カスタムレポートを生成する手順がデータチェック SOP に正確に反映されていること、及びレポートのアウトプットが次工程のレビュー実施のための手順と一貫していることを確実にするものである。

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)).

6.20. IT 供給者及びサービスプロバイダー（クラウド及び仮想サービス／プラットフォーム（ソフトウェア・アズ・ア・サービス (SaaS) ／プラットフォーム・アズ・アサービス (PaaS) ／インフラストラクチャ・アズ・ア・サービス (IaaS) とも呼ぶ）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」サービスを利用する場合、提供されるサービス、オーナーシップ、データの取出し、保管、セキュリティを理解するようにすべきである。
The physical location where the data is held, including the impact of any laws applicable to that geographic location, should be considered.	データを保持する物理的ロケーションは、当該地理的ロケーションに適用されうる法律の影響も含めて、検討すべきである。
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).	契約における委託者及び受託者の責任は、技術的な合意書または契約で定義すべきである。これにより、データオーナー及び当局の求めに応じて、データ（メタデータ及び監査証跡を含む）にタイムリにアクセスができることを確実にすべきである。プロバイダーとの契約では、アーカイビング及び保管期間を通じたデータの見読性の維持についての責任を定義すべきである。（アーカイブ参照）

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.	〔バックアップ取得時の〕元々のバリデーション状態（復元を許可するためのバリデーション情報及び変更管理情報を含む）に基づいてソフトウェア／システムを復元するような適切な計画／準備を行わなければならない。
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.	契約には、ビジネス継続のための手はずが盛り込まれ、テストされるべきである。サービスプロバイダーを監査する必要性は、リスクに基づくべきである。

7. Glossary

Acronym or word or phrase 頭字語、語・句	Definition 定義
eCRF	Electronic Case Report Form
ECG	Electrocardiogram
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
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 生成されたデータが、意図したとおりに生成され、意図した目的に合っていることの保証。これは ALCOA を含む。
ALCOA	Acronym referring to Attributable, Legible, Contemporaneous, Original and Accurate.
ALCOA +	Acronym referring to Attributable, Legible, Contemporaneous, Original and Accurate 'plus' Complete, Consistent, Enduring, and Available.
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. 研究、職業等の主題において特別に技術的に用いられる用語を集めたもの。
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. 一連の記録、テーブルやデータベースから、壊れたり、不正確な記録を検出し、修正（削除）するプロセスであり、データの中の不完全／誤り／不正確／無効である部分を特定し、問題のあるデータを置換、修正、削除することを示す。
Format 書式	The something is arranged or set out 配置されたもの。

Acronym or word or phrase 頭字語、語・句	Definition 定義
Directly accessible 直接アクセスできる	At once; without delay ただちに、遅滞なく
Procedures 手順書	Written instructions or other documentation describing process i.e. standard operating procedures (SOP) 文書化された指示またはプロセスを記載する他の文書、すなわち標準操作手順書（SOP）
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. 署名者の識別とデータインテグリティを検証できるような一連の規則と一連のパラメータを用いて計算されるような、暗号化方式の署名者認証に基づく電子署名。
Validated scanning process バリデートされたスキャンプロセス	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／物がスキャンされるプロセスであり、ロケーション識別機能や OCR などの、重複ページを人がチェックしなくてもよいような追加的コントロールを持つプロセス。

8. References

Computerised systems. In: The rules governing medicinal products in the European Union. Volume 4: Good manufacturing practice (GMP) guidelines: Annex 11. Brussels: European Commission. (http://ec.europa.eu/enterprise/pharmaceuticals/eudralex/vol-4/pdfs-en/anx11en.pdf).

OECD series on principles of good laboratory practice (GLP) and compliance monitoring. Paris: Organisation for Economic Co-operation and Development. (http://www.oecd.org/chemicalsafety/testing/oecdseriesonprinciplesofgoodlaboratorypracticeglp andcompliancemonitoring.htm).

Good Clinical Practice (GCP) ICH E6(R2) November 2016 (http://www.ich.org/products/guidelines/efficacy/article/efficacy-guidelines.html).

Guidance on good data and record management practices; World Health Organisation, WHO Technical Report Series, No.996, Annex 5; 2016. (http://apps.who.int/medicinedocs/en/m/abstract/Js22402en/).

Good Practices For Data Management And Integrity In Regulated GMP/GDP Environments – PIC/S; PI041-1(draft 2); August 2016.
(https://picscheme.org/en/news?itemid=33).

MHRA GMP data integrity definitions and guidance for industry. London: Medicines and Healthcare Products Regulatory Agency; March 2015.
(https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/412735/Data_integrity_definitions_and_guidance_v2.pdf).

MHRA/HRA DRAFT Guidance on the use of electronic consent (http://www.hra-decisiontools.org.uk/consent/)

EU Pharmacovigilance legislation: http://ec.europa.eu/health/human-use/pharmacovigilance

The Human Medicines Regulations 2012 (Statutory Instrument 2012 No. 1916):
http://www.legislation.gov.uk/uksi/2012/1916/contents/made

EU Good Pharmacovigilance Practice Modules:
http://www.ema.europa.eu/ema/index.jsp?curl=pages/regulation/document_listing/document_listing_000345.jsp&mid=WC0b01ac058058f32c

Revision History

Revision	**Publication Month**	**Reason for changes**
Revision 1	March 2018	None. First issue.