管理番号: BZLib-128
改訂番号: 1.1
名称: **Guideline on computerised systems and electronic data in clinical trials**
ページ数: 全 125ページ

EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

9 March 2023
EMA/INS/GCP/112288/2023
Good Clinical Practice Inspectors Working Group (GCP IWG)

Guideline on computerised systems and electronic data in clinical trials

Adopted by GCP IWG for release for consultation	4 March 2021
Start of public consultation	18 June 2021
End of consultation (deadline for comments)	17 December 2021
Final version adopted by the GCP IWG	7 March 2023
Date of coming into effect	6 months after publication

This guideline replaces the 'Reflection paper on expectations for electronic source data and data transcribed to electronic data collection tools in clinical trials' (EMA/INS/GCP/454280/2010).

株式会社文善

改 1.1　**2024 年 1 月 30 日**

管理番号: BZLib-128
改訂番号: 1.1
名称: **Guideline on computerised systems and electronic data in clinical trials**
ページ数: 全 125ページ

【注記】
本書は、EMA が発行した英語原文を株式会社文善にて和文翻訳したものです。
翻訳文はできるだけ英語原文に忠実になるよう努めましたが、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、意図が伝わるよう意訳している箇所もあります。株式会社文善は翻訳文に誤りがないことについて保証いたしません。
原文の内容をご自身で必ず確認してください。株式会社文善は、本書を利用したことに起因して、何らかの損害が生じたとしても、これについては一切の責任を負いません。

本書に含まれる内容は、予告なしに変更されることがあります。
本書を含め、株式会社文善のサイト (https://bunzen.co.jp) では、電磁的記録・電子署名等に関する規制やガイダンスの翻訳を掲載しています。
本書、株式会社文善のサービス等への質問、コメント等は info1@bunzen.co.jp にお寄せください。

【本書の表記について】
文脈に応じて原文にないことばを補足した場合〔 〕内に記述しています。
読みやすくするため、必要に応じて、原文にない括弧（ ）で文を囲んでいます。
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。
原文で should とある箇所は、「～すること」「～する必要がある」「～すべきである」と訳していますが、いずれも強制力はありません。

目次

Glossary (用語集)

Generally used terms Unless otherwise specified (e.g. '*source data*' or '*source document*') and in order to simplify the text, '*data*' will be used in this guideline in a broad meaning, which may include documents, records or any form of information.	**一般的に使用される用語** (「*source data (原データ)*」や「*source document (原資料)*」のように) 特別に指定しない限り、文章を簡潔にするために、このガイドラインでは「データ」を広い意味で使用し、文書、記録、又はあらゆるフォーマットの情報を含むものとする。
All references to sponsors and investigators in this guideline also apply to their service providers, irrespective of the services provided. When a computerised system is implemented by an institution where the investigator is conducting a clinical trial, any reference to the investigator in this guideline also includes the institution, when applicable.	このガイドラインで治験依頼者及び治験責任医師に言及している箇所はすべて、提供されるサービスにかかわらず、サービスプロバイダにも適用される。 医療機関がコンピュータ化システムを実装し、そこで治験責任医師が治験を行っている場合、このガイドラインで治験責任医師に言及している箇所は、必要に応じて医療機関も含めるものとする。
The term '*trial participant*' is used in this text as a synonym for the term '*subject*', which is defined in Regulation (EU) No 536/2014 as '*an individual who participates in a clinical trial, either as a recipient of the IMP or as a control*'.	「*治験参加者 (trial participant)*」という用語は、本書では「*被験者 (subject)*」という用語と同義として扱う。これは、Regulation (EU) No 536/2014 で「*IMP を投与される者、又は対照群として治験に参加する個人*」として定義されている。
The term '*responsible party*' is frequently used instead of sponsor or principal investigator. Please also refer to section 4.2. and Annex 1.	「*責任のある当事者 (responsible party)*」という用語は、治験依頼者又は治験責任医師の代わりに頻繁に使用される。4.2 章及び附属書 1 も参照のこと。
The term '*agreement*' is used as an overarching term for all types of documented agreements, including contracts.	「*合意書 (agreement)*」という用語は、契約を含む、すべての種類の文書化された合意を表す包括的な用語として使用される。

The term '*validation*' encompasses aspects usually known as '*qualification and validation*'.	「*バリデーション*」という用語は、通常「*適格性評価とバリデーション*」として知られている側面を含む。
Artificial intelligence Artificial intelligence (AI) covers a very broad set of algorithms, which enable computers to mimic human intelligence. It ranges from simple if-then rules and decision trees to machine learning and deep learning.	**人工知能** 人工知能 (AI) は、コンピュータが人間の知性を模倣できるようにする、非常に幅広いアルゴリズムセットをカバーしており、単純な if-then ルールや決定木から、機械学習や深層学習までを含む。
Audit trail In computerised systems, an audit trail is a secure, computer generated, time-stamped electronic record that allows reconstruction of the events relating to the creation, modification, or deletion of an electronic record.	**監査証跡** コンピュータ化システムでは、監査証跡はコンピュータで生成されたタイムスタンプ付きのセキュアな電子記録であり、電子記録の作成／変更／削除に関連するイベントの再構築を可能にするものである。
Clinical outcome assessment Clinical outcome assessment (COA) employs a tool for the reporting of outcomes by clinicians, trial site staff, observers, trial participants and their caregivers. The term COA is proposed as an umbrella term to cover measurements of signs and symptoms, events, endpoints, health-related quality of life (HRQL), health status, adherence to treatment, satisfaction with treatment, etc.	**Clinical outcome assessment** COA には、臨床医、治験実施施設の職員、オブザーバ、治験参加者、及びその介護者が転帰を報告するためのツールが用いられている。COA という用語は、徴候や症状、イベント、エンドポイント、健康関連の生活の質 (HRQL)、健康状態、治療〔計画〕の遵守、治療への満足度などの測定を網羅する包括的な用語として提案されている。
Computerised system life cycle The life cycle of a computerised system includes all phases of the system; i.e. typically 1) the concept phase where the responsible party considers to automate a process and where user requirements are collected,	**コンピュータ化システムライフサイクル** コンピュータ化システムライフサイクルには、システムのすべてのフェーズが含まれる。つまり、一般的に： 1) 概念フェーズ：責任のある当事者がプロセスの自動化を検討し、ユーザー要件を収集する。

2) the project phase where a service provider can be selected, a risk-assessment is made, and the system is implemented and validated, 3) the operational phase where a system is used in a regulated environment and changes are implemented in a manner that maintains data confidentiality, integrity and availability, and finally, 4) a retirement phase, which includes decisions about data retention/archiving, migration or destruction and the management of these processes.	2) プロジェクトフェーズ：サービスプロバイダを選定し、リスクアセスメントを行い、システムを実装し、バリデートする。 3) 運用フェーズ：システムを規制環境下で使用する。変更は、データの機密性、インテグリティ、及び可用性を維持する方法で行われる。 4) リタイアメントフェーズ：データを保持/アーカイブするか、移行するか、又は破棄するかの決定、及びこれらのプロセスの管理が含まれる。
Configuration Configuration sets up a system using existing (out-of-the-box) functionality. It requires no programming knowledge.	**構成設定** 構成設定では、出来合いの (out-of-the-box) 機能を使用してシステムをセットアップする。プログラミングの知識は必要としない。
Customisation Customisation modifies and adds to existing functionality by custom coding. It requires programming knowledge.	**カスタマイズ** カスタマイズでは、カスタムコーディングによって既存の機能を変更したり、追加したりする。〔カスタマイズには〕プログラミングの知識が必要である。
Data governance The total of activities, processes, roles, policies, and standards used to manage and control the data during the entire data life cycle, while adhering to ALCOA++ principles (see section 4.5.).	**データガバナンス** ALCOA++の原則 (4.5 章参照) に従いながら、データライフサイクル全体にわたってデータを管理及びコントロールするために使用される活動、プロセス、役割、ポリシー、及び標準を総称するもの。
Data life cycle All processes related to the creating, recording, processing, reviewing, changing, analysing, reporting, transferring, storing, migrating, archiving, retrieving, and deleting of data.	**データライフサイクル** データの作成、記録、処理、レビュー、変更、分析、報告、転送、保存、移行、アーカイブ、検索、及び削除に関連するすべてのプロセス。

Dynamic file formats Dynamic files include automatic processing and/or enable an interactive relationship with the user. A certified electronic copy may be retained in electronic file formats that are different from the original record, but the equivalent dynamic nature (including metadata) of the original record should be retained.	**動的ファイルフォーマット** 動的ファイルは、自動処理を含み、及び (又は) ユーザーがインタラクティブに利用できる。電子的な保証付きコピーは、オリジナル記録と異なる電子ファイルフォーマットで保持してもよいが、オリジナル記録と同等の動的な性質 (メタデータを含む) を保持する必要がある。
Event log An automated log of events in relation to the use of a system like system access, alerts or firing of edit checks.	**イベントログ** システムアクセス、アラート、エディットチェック実施などの、システムの使用に関連するイベントの自動ログ。
Patient-reported outcome Any outcome reported directly by the trial participant and based on the trial participant's perception of a disease and its treatment(s) is called patient-reported outcome (PRO). The term PRO is proposed as an umbrella term to cover both single dimension and multi-dimension measurements of symptoms, HRQL, health status, adherence to treatment, satisfaction with treatment, etc. (Source: CHMP '*Reflection paper on the regulatory guidance for the use of HRQL measures in the evaluation of medicinal products*' - EMEA/CHMP/EWP/139391/2004)	**Patient-reported outcome** 治験参加者によって直接報告され、疾患とその治療についての治験参加者の認識に基づくすべてのアウトカムを PRO と呼ぶ。PRO という用語は、症状、HRQL、健康状態、治療〔計画〕の遵守、治療に対する満足度などの、単一次元測定及び多次元測定の両方をカバーする包括的な用語として提案されている。 (出典：CHMP *'Reflection paper on the regulatory guidance for the use of HRQL measures in the evaluation of medicinal products'* - EMEA/CHMP/EWP/139391/2004)
Static file formats Static files containing information or data that are fixed and allow no dynamic interaction.	**静的ファイルフォーマット** 情報又はデータを含む静的ファイル。固定され、動的なインターアクションができない。

Validation *'A process of establishing and documenting that the specified requirements of a computerized system can be consistently fulfilled from design until decommissioning of the system or transition to a new system. The approach to validation should be based on a risk assessment that takes into consideration the intended use of the system and the potential of the system to affect human subject protection and reliability of clinical trial results.'* (ICH E6 R2 1.65)	バリデーション *「コンピュータ化システムの指定された要件について、設計からシステムリタイアメント又は新システムへの移行まで、一貫して満たすことを確立し、文書化するプロセス。バリデーションへのアプローチは、システムの用途や被験者保護及び治験結果の信頼性へ影響を与える可能性を考慮したリスク評価に基づいている必要がある。」*(ICH E6 R2 1.65)

Executive summary (エグゼクティブサマリー)

Computerised systems are being increasingly used in clinical research. The complexity of such systems has evolved rapidly in the last few years from electronic case report forms (eCRF), electronic patient reported outcomes (ePROs) to various wearable devices used to continuously monitor trial participants for clinically relevant parameters and ultimately to the use of artificial intelligence (AI). Hence, there is a need to provide guidance to all stakeholders involved in clinical trials reflective of these changes in data types and trial types on the use of computerised systems and on the collection of electronic data, as this is important to ensure the quality and reliability of trial data, as well as the rights, dignity, safety and wellbeing of the trial participants. This would ultimately contribute to a robust decision-making process based on such clinical data.	治験にますます多くのコンピュータ化システムが使用されるようになってきた。こういったシステムは〔以前の〕eCRF や ePRO から急速に進化を遂げ、治験に有効なパラメータについて治験参加者を連続的にモニターする種々のウェアラブルデバイスを経て、ついには人工知能 (AI) を利用するに至っている。データや治験のフォーマットのこういった変化に鑑み、治験に関与するすべての利害関係者に対してコンピュータ化システムの使用と電子データの収集に関するガイダンスを提供する必要が出てきた。というのは、〔ガイダンスは〕治験データの品質と信頼性、及び治験参加者の権利、尊厳、安全及び健康を確実にするうえで重要であるためである。〔ガイダンスは〕究極的には〔このようにして収集された〕臨床データに基づいて、しっかりと意思決定を行うプロセスに役立つであろう。

This guideline will describe some generally applicable principles and definition of key concepts. It also covers requirements and expectations for computerised systems, including validation, user management, security, and electronic data for the data life cycle. Requirements and expectations are also covered related to specific types of systems, processes, and data.	本ガイドラインでは、一般的に適用可能な原則と重要な概念の定義をいくつか説明する。また、コンピュータ化システムに対する要件及び期待 (そこには、バリデーション、ユーザー管理、セキュリティ、データライフサイクルにわたっての電子データ〔の管理〕を含む) についても説明する。また、特定のタイプのシステム、プロセス、及びデータに関連する要件と期待についても述べる。

1. Introduction (はじめに)

As described above, the change in data and trial types and thereby the use of computerised systems presents new challenges. The European Medicines Agency (EMA) *'Reflection Paper on expectations for electronic source data and data transcribed to electronic data collection tools in clinical trials*' started to address these when it was published in 2010. However, the development of and experience with such systems has progressed. A more up-to-date guideline is needed to replace the Reflection Paper.	前述のように、データや治験のフォーマットが変化しており、そこにコンピュータ化システムを使用することで新たな課題が生じる。European Medicines Agency (EMA) の *'Reflection Paper on expectations for electronic source data and data transcribed to electronic data collection tools in clinical trials*' は、2010 年に発行された時点でこれらの課題を取扱い始めたが、こういったシステムの開発や経験が進歩しているため、より時代に即したガイドラインにより Reflection Paper を置き換える必要が出てきた。
There is no requirement or expectation that the sponsors and investigators use computerised systems to collect data; however, the use of data acquisition tools if implemented and controlled to the described standard, offers a wide variety of functions to improve data completeness, consistency and unambiguity, e.g. automatic edit checks, automated data transfers, validation checks, assisting information and workflow control.	治験依頼者や治験責任医師がデータを収集するうえでコンピュータ化システムを使用しなければならないという要件はないが、〔本書で〕説明されている基準に従って〔データ収集ツールを〕実装し、コントロールすることにより、データの完全性、一貫性、及び明瞭性を向上させるデータ収集ツールのさまざまな機能 (例：自動エディットチェック、自動データ転送、バリデーションチェック、補助情報及びワークフロー制御) が利用できるようになる。

2. Scope (適用範囲)

The scope of this guideline is computerised systems, (including instruments, software and '*as a service*') used in the creation/capture of electronic clinical data and to the control of other processes with the potential to affect participant protection and reliability of trial data, in the conduct of a clinical trial of investigational medicinal products (IMPs). These include, but may not be limited to the following:	本ガイドラインの適用範囲は、コンピュータ化システム (機器、ソフトウェア、及び「*as a service*」を含む) であり、治験薬 (IMP) の治験の実施において、電子臨床データの作成/収集に使用されるもの、及び参加者保護や治験データの信頼性に影響し得るプロセスのコントロールに使用されるものである。これらには以下が含まれるが、それに限定されるものではない。
• Electronic medical records, used by the investigator to capture of all health information as per normal clinical practice.	• 電子医療記録〔システム〕。治験責任医師が通常の臨床業務を通して、すべての健康情報を取得するために使用する。
• Tools supplied to investigators/trial participants for recording clinical data via data entry (e.g. electronic clinical outcome assessments [eCOAs]).	• 治験責任医師/治験参加者に提供されるツールで、データ入力を介して臨床データを記録するもの (例：eCOA)。
- Electronic trial participant data capture devices used to collect ePRO data, e.g. mobile devices supplied to trial participants or applications for use by the trial participant on their own device i.e. bring your own device (BYOD).	- 電子的な治験参加者のデータを収集するデバイスで、ePRO データを収集するために使用されるもの。例：治験参加者に提供されるモバイルデバイス、又は治験参加者が自分のデバイス上で使用するアプリケーション。つまり Bring Your Own Device (BYOD)。
- Electronic devices used by clinicians to collect data e.g. mobile devices supplied to clinicians.	- 臨床医がデータを収集するために使用する電子機器。例：臨床医に提供されるモバイルデバイス。
• Tools supplied for the automatic capture of data for trial participants such as biometrics, e.g. wearables or sensors.	• 治験参加者のデータを自動収集するために提供されるツール。バイオメトリクスなど。例：ウェアラブル又はセンサー。

• eCRFs (e.g. desktop or mobile device-based programs or access to web-based applications), which may contain source data directly entered, transcribed data, or data transferred from other sources, or any combination of these.	• eCRF (例：デスクトップ又はモバイルデバイス上のプログラム又は Web ベースのアプリケーションへのアクセス) には、直接入力された原データ、転記されたデータ、又は他のソースから転送されたデータ、又はこれらの組み合わせが含まれる。
• Tools that automatically capture data related to the transit and storage temperatures for investigational medicinal product (IMP) or clinical samples.	• 治験薬 (IMP) 又は臨床サンプルの輸送及び保管温度に関連するデータを自動的に収集するツール。
• Tools to capture, generate, handle, or store data in a clinical environment where analysis, tests, scans, imaging, evaluations, etc. involving trial participants or samples from trial participants are performed in support of clinical trials (e.g. LC-MS/MS systems, medical imaging and related software).	• 臨床環境でデータを取得、生成、処理、又は保存するためのツールで、治験をサポートするために、治験参加者又は治験参加者のサンプルの分析、テスト、スキャン、イメージング、評価などを行うもの (例：LC-MS/ MS システム、医用画像及び関連ソフトウェア) 。
• eTMFs, which are used to maintain and archive the clinical trial essential documentation.	• eTMF。治験の必須文書を維持管理及びアーカイブするために使用される。
• Electronic informed consent, for the provision of information and/or capture of the informed consent when this is allowed according to national legislation, e.g. desktop or mobile device- based programs supplied to potential trial participants or applications for use by the potential trial participants on their BYOD or access to web-based applications.	• 情報提供、及び (又は) インフォームドコンセント取得を行うための電子的インフォームドコンセント。ただし、国内法で許可されている場合に限る。例えば、潜在的な治験参加者に提供されるデスクトップ又はモバイルデバイスベースのプログラム、潜在的な治験参加者による BYOD 上でのアプリケーションの利用又は Web ベースアプリケーションへのアクセス。

• Interactive Response Technologies (IRT), for the management of randomisation, supply and receipt of IMP, e.g. via a web-based application.	• IMP の無作為化、供給及び受領の管理のための IRT。例えば Web ベースのアプリケーションとして提供される。
• Portals or other systems for supplying information from the sponsor to the sites (e.g. investigator brochures (IBs), suspected unexpected serious adverse reactions (SUSARs) or training material), from the sites to the sponsor (e.g. the documentation of the investigator's review of important safety information), or from the sponsor or the site to adjudication committees and others.	• 情報提供するためのポータル又はその他のシステム。治験依頼者から治験実施施設への情報提供 (例：治験薬概要書 (IB)、suspected unexpected serious adverse reactions (SUSAR)、又はトレーニング資料)、治験実施施設から治験依頼者への情報提供 (例：治験責任医師による重要な安全性情報のレビュー文書)、又は治験依頼者や治験実施施設から審査委員会などへの情報提供。
• Systems/tools used to conduct remote activities such as monitoring or auditing.	• モニタリングや監査などのリモート活動を実施するために使用されるシステム/ツール。
• Other computerised systems implemented by the sponsor holding/managing and/or analysing or reporting data relevant to the clinical trial e.g. clinical trial management systems (CTMS), pharmacovigilance databases, statistical software, document management systems, test management systems and central monitoring software.	• その他、治験依頼者が実装するコンピュータ化システムで、治験に関連するデータを、保持/管理、及び (又は) 分析又は報告するもの。例：治験管理システム (CTMS)、ファーマコビジランスデータベース、統計ソフトウェア、文書管理システム、治験管理システム、及び中央監視ソフトウェア。
• AI used in clinical trials e.g. for trial participant recruitment, determination of eligibility, coding of events and concomitant medication, data clarification, query processes and event adjudication. Requirements to AI beyond the generally applicable expectations to all systems will not be covered in this guideline initially. This may be covered in a future Annex.	• 治験に使用される AI。例えば、治験参加者の募集、適格性の決定、イベントや併用薬のコーディング、データクラリフィケーション、クエリプロセス、イベントの判定など。すべてのシステムに対して一般的に適用できそうもない AI の要件は、当面このガイドラインでは触れないが、いずれ附属書としてカバーする可能性はある。

The approach towards computerised systems used in clinical practice (e.g. regarding validation) should be risk proportionate (please also refer to section 4.6.).	臨床業務で使用されるコンピュータ化システムの (例えばバリデーションに関する) アプローチ はリスクに応じたものとすること (4.6 章も参照のこと) 。

3. Legal and regulatory background (法律及び規制の背景)

• Regulation (EU) No 536/2014, or Directive 2001/20/EC and Directive 2005/28/EC • ICH Guideline for good clinical practice E6 R2 (EMA/CHMP/ICH/135/1995 Revision 2)	• Regulation (EU) No 536/2014、又は Directive 2001/20/EC 及び Directive 2005/28/EC • ICH Guideline for good clinical practice E6 R2 (EMA/CHMP/ICH/135/1995 Revision 2)
This guideline is intended to assist the sponsors, investigators, and other parties involved in clinical trials to comply with the requirements of the current legislation (Regulation (EU) No 536/2014, Directive 2001/20/EC and Directive 2005/28/EC), as well as ICH E6 Good Clinical Practice (GCP), regarding the use of computerised systems and the collection of electronic data in clinical trials.	本ガイドラインは、治験依頼者、治験責任医師、及び治験に関与するその他の関係者が、治験におけるコンピュータ化システムの使用と電子データの収集について、現在の法律 (Regulation (EU) No 536/2014、Directive 2001/20/EC 及び Directive 2005/28/EC)、また ICH E6 Good Clinical Practice (GCP) を遵守できるよう支援するものである。
The risk-based approach to quality management also has an impact on the use of computerised systems and the collection of electronic data.	品質管理にリスクベースアプローチを用いることもコンピュータ化システムの使用と電子データの収集に影響を与える。
Consideration should also be given to meeting the requirements of any additional current legal and regulatory framework that may in addition apply to the medicinal product regulatory framework, depending on the digital technology. These may include e.g. medical devices, data protection legislation, and legislation on electronic identification and electronic signatures.	さらに、デジタル技術にもよるが、新たに医薬品の規制体系に適用されそうな、追加的な最新の法律・規制体系の要件を満たすことも考慮すべきである。例えばこれらには、医療機器、データ保護法、電子識別及び電子署名に関する法律が含まれる。

Further elaboration of the expectations of the EU GCP Inspectors' Working group (GCP IWG) on various topics, including those on computerised systems, can be found as GCP IWG Q&As published on the EMA website.	コンピュータ化システムを含む、さまざまなトピックに関する EU GCP Inspectors' Working Group (GCP IWG) の期待事項の詳細は EMA の Web サイトで公開されている GCP IWG Q&A を参照のこと。

4. Principles and definition of key concepts (原則と主要概念の定義)

The following sections outline the basic principles that apply to all computerised systems used in clinical trials.	以下の章では、治験で使用されるすべてのコンピュータ化システムに適用される基本的な原則について概説する。

4.1. Data integrity (データインテグリティ)

Data integrity is achieved when data (irrespective of media) are collected, accessed, and maintained in a secure manner, to fulfil the ALCOA++ principles of being attributable, legible, contemporaneous, original, accurate, complete, consistent, enduring, available when needed and traceable as described in section 4.5. in order for the data to adequately support robust results and good decision making throughout the data life cycle. Assuring data integrity requires appropriate quality and risk management systems as described in section 4.6., including adherence to sound scientific principles and good documentation practices.	データ (媒体は問わない) が安全な方法で収集、アクセス、維持管理され、ALCOA++原則を満たすときにデータインテグリティが確保される。ALCOA++原則とは、4.5 章で述べるように、帰属性、判読性、同時性、原本性、正確性、完全性、一貫性、永続性、必要時の可用性、追跡可能性があるということであり、これによりデータライフサイクル全体を通じて、データが、疑いようのない結果と良い意思決定を適切にサポートできるようになる。データインテグリティを確保するためには、4.6 章で述べる適切な品質管理システム及びリスク管理システムが必要であり、そこには健全な科学的原則及び good documentation practice への準拠が含まれる。

• Data governance should address data ownership and responsibility throughout the data life cycle, 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. • Data governance systems should include staff training on the importance of data integrity principles and the creation of a working environment that enables visibility, and actively encourages reporting of omissions and erroneous results. Lack of integrity before the expiration of the mandated retention period may render the data unusable and is equivalent to data loss/destruction.	• データガバナンスでは、データライフサイクル全体にわたってのデータの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 (意図的又は誤って行われるデータの変更に対するコントロールを含む) に従うためのプロセス/システムの設計、運用、及び監視を検討する必要がある。 • 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ついての職員へのトレーニング、及び職場の透明性を良くして、作業省略や正しくない結果を積極的に報告することを奨励するような職場環境の醸成が含まれる。 〔データが〕定められた保存期間満了前にインテグリティを失うと、そのデータは利用できなくなり、喪失/破壊したも同然となる。

4.2. Responsibilities (責任)

Roles and responsibilities in clinical trials should be clearly defined. The responsibility for the conduct of clinical trials is assigned via legislation to two parties, which may each have implemented computerised systems for holding/managing data: • Investigators and their institutions, laboratories and other technical departments or clinics, generate and store the data, construct the record, and may use their own software and hardware (purchased, part of national or institutional health information systems, or locally developed).	治験における役割と責任を明確に定義すべきである。治験の実施についての責任は、法律上は 2 つの当事者に割り当てられるが、データを保持/管理するためのコンピュータ化システムをそれぞれで実装している場合がある。 • 治験責任医師と〔治験責任医師の属する〕医療機関、検査室、その他の技術部門、又は診療所は、データを生成／格納し、記録をまとめるが、さらに自分たちのソフトウェアとハードウェア (購入したもの、国や医療機関の医療情報システムの一部、又はローカルで開発したもの) を使用する場合がある。

• Sponsors that supply, store and/or, manage and operate computerised systems (including software and hardware) and the records generated by them. Sponsors may do this directly, or via service providers, including organisations providing e.g. eCOA, eCRF, or IRT that collect and store data on behalf of sponsors. Please refer to Annex 1 regarding the transfer/delegation to service providers of tasks related to the use of computerised systems and services.	• 治験依頼者がコンピュータ化システム (ソフトウェアとハードウェアを含む) とそこで生成された記録を、供給、格納、及び (又は) 管理、運用する。治験依頼者は、これを直接行うこともあるし、サービスプロバイダ (治験依頼者の代わりにデータを収集し格納する、例えば eCOA、eCRF、IRT などを提供する組織を含む) を経由して行うこともある。 サービスプロバイダへのコンピュータ化システムの使用とサービスに関するタスクの移転/委任については付属書 1 を参照のこと。

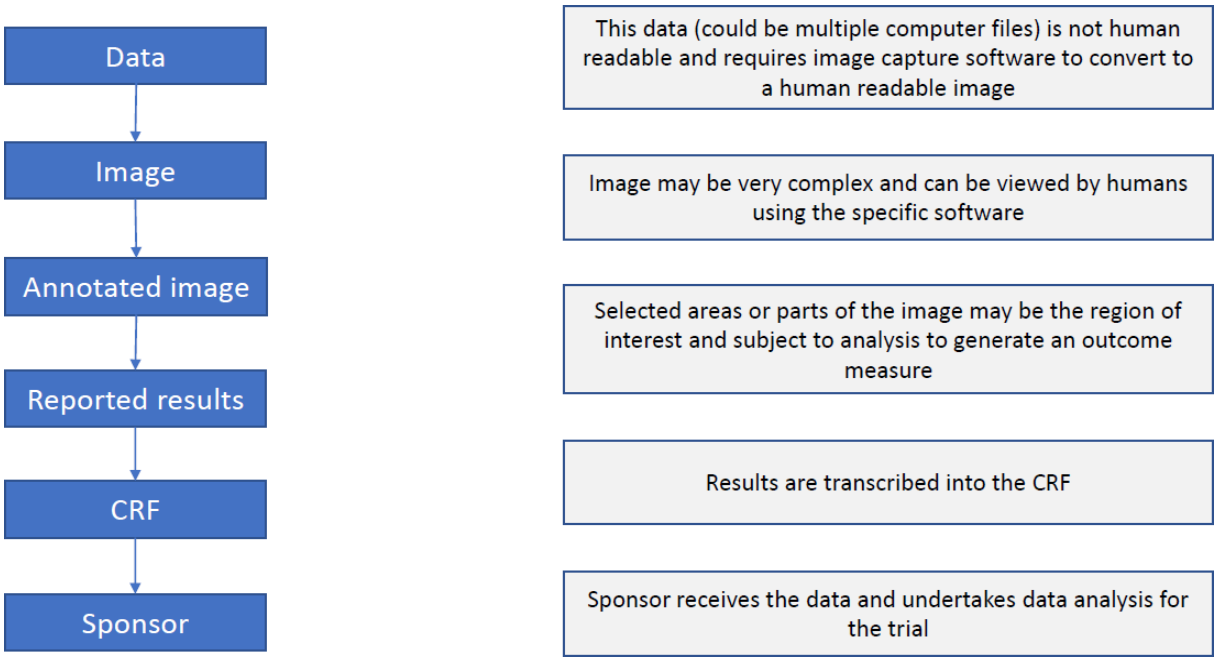
4.3. Data and metadata (データとメタデータ)

Electronic data consist of individual data points. Data become information when viewed in context. Metadata provide context for the data point. Different types of metadata exist such as: variable name, unit, field value before and after change, reason for change, trial master file (TMF) location document identifier, timestamp, user. Typically, these are data that describe the characteristics, structure, data elements and inter-relationships of data e.g. audit trails. Metadata also permit data to be attributable to an individual entering or taking an action on the data such as modifying, deleting, reviewing, etc. (or if automatically generated, to the original data source). Metadata form an integral part of the original record. Without the context provided by metadata, the data have no meaning. Loss of metadata may result in a lack of data integrity and may render the data unusable.	電子データは、個々のデータポイントから構成される。データをコンテキストで捉えると情報になる。メタデータは、データポイントに対してコンテキストを提供するものである。メタデータには様々な種類があり、例えば、変数、単位、変更前後のフィールド値、変更理由、TMF の場所を示す文書識別子、タイムスタンプ、ユーザーなどがある。一般的に、これらは、データの特性、構造、データ要素、及びデータ間の相互関係 (例：監査証跡) を記述するデータである。メタデータは、データに個人への帰属性を持たせる。すなわち、データを入力したり、データに対して変更、削除、レビューなどのアクションを実行した個人　(又は自動的に生成された場合は、オリジナルデータソース) を示す。メタデータは、オリジナル記録には不可欠である。メタデータによって提供されるコンテキストが無いと、データは意味を持たない。メタデータが失われると、データインテグリティが確保できなくなり、データが使用できなくなる可能性がある。

4.4. Source data (原データ)

The term source data refers to the original reported observation in a source document. Source documents could be e.g. hospital records, clinical and office charts, laboratory notes. Other examples are emails, spreadsheets, audio and/or video files, images, and tables in databases.	原データという用語は、原資料で報告されたオリジナルの観察結果を指す。原資料は、例えば、医療機関の記録、臨床及び業務に関する図表、実験ノートなどである。その他の例としては、電子メール、スプレッドシート、オーディオ、及び (又は) ビデオファイル、画像、及びデータベースのテーブルがある。

The location of source documents and the associated source data they contain, should be clearly identified at all points within the data capture process. Below is an outline (figure 1) of the data processing stages, starting with the data capture. The correct identification of source data is important for adequate source data verification and archiving. Data at different processing stages can be considered source depending on the preceding processing steps.	データ収集プロセスのすべての時点で、原資料及びそこに含まれる関連する原データがどこにあるのかを明確に特定できるようにすること。 下図はデータ収集で始まる一連のデータ処理ステージの概要を示す (figure 1) 。原データを正しく特定することは、原データの適切なデータベリフィケーション及びアーカイブのために重要である。ある処理ステージにあるデータは前段となる処理ステップによってはソースであると考えられる。



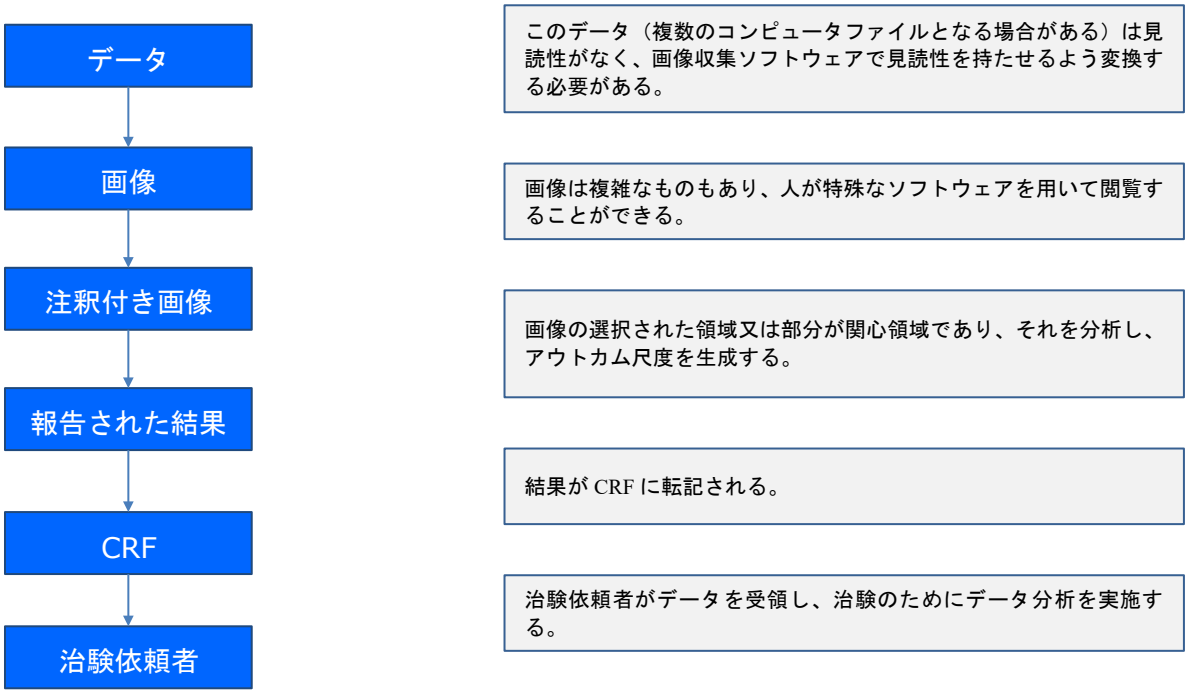


Figure. 1

Data capture sometimes requires some degree of processing prior to data recording. In this process, the data generated during an observation, measurement or data collection is checked, processed, and transferred into a new format and then recorded.	データ収集では、時折、データを記録する前に、ある程度の処理が必要になる場合がある。その処理では、観察で得られたデータ、計測値又は集められたデータをチェックし、処理を行い、新しいフォーマットに移し、記録する。
The retention of unprocessed data records is not always feasible. If the processing is an integral part of the solution used and is recognisable as such in the solution characteristics, there is no need to extract and retain the unprocessed data. It should be possible to validate the correct operation of the processing.	処理前のデータレコードを保持しておくことが常に可能であるとは限らない。その処理が用いるソリューションにとって不可欠であり、そのことがソリューションの特性として認められるのであれば、処理前のデータを抽出して保持しておく必要はない。処理の正しい操作をバリデートできるようにしておくこと。
As a general principle, the source data should be processed as little as possible and as much as necessary.	一般的な原則として、原データに対する処理は必要最小限にとどめるべきである。

From a practical point of view, the first obtainable permanent data from an electronic data generation/capture should be considered and defined as the electronic source data. This process should be validated to ensure that the source data generated/captured is representative of the original observation and should contain metadata, including audit trail, to ensure adherence to the ALCOA++ principles (see section 4.5.). The location where the source data is first obtained should be part of the metadata.	現実的に、電子データ生成/収集から最初に入手できる永続的データが電子原データと考えられ、またそのように定義すべきである。生成/収集された原データがオリジナルの観察結果を表わすものであり、かつ監査証跡などのメタデータを含み、確実に ALCOA++原則 (4.5 章参照) に準拠するものであることを確実にするために、そのプロセスをバリデートすべきである。メタデータには、原データが最初に取得された場所を含める必要がある。

4.5. ALCOA++ principles (ALCOA++原則)

A number of attributes are considered of universal importance to data. These include that the data are:	多くの属性がデータにとって共通的に重要であると考えられる。そういった属性とは、データが以下のようになることである。
Attributable Data should be attributable to the person and/or system generating the data. Based on the criticality of the data, it should also be traceable to the system/device, in which the data were generated/captured. The information about originator (e.g. system operator, data originator) and system (e.g. device, process) should be kept as part of the metadata.	**帰属性** データは、データを生成する人、及び (又は) システムに紐づけできること。データの重要性によっては、データが生成/収集されたシステム/デバイスまで辿れる必要がある。オリジネータ (例：システム操作者、データオリジネータ) 及びシステム (例：デバイス、プロセス) に関する情報は、メタデータの一部として保持すべきである。
Legible Data should be maintained in a readable form to allow review in its original context. Therefore, changes to data, such as compression, encryption and coding should be completely reversible.	**判読性** データは、〔人の〕読めるフォーマットで維持管理し、オリジナルのコンテキストでレビューできるようにすること。したがって、圧縮、暗号化、コーディングなどのデータへの変更は、完全に可逆的にすべきである。

Contemporaneous Data should be generated by a system or captured by a person at the time of the observation. The time point of the observation and the time point of the storage should be kept as part of the metadata, including the audit trail. Accurate date and time information should be automatically captured and should be linked and set by an external standard.	**同時性** データは、システムによって生成されるか、又は人によって取得されるが、それを観察時に行うこと。どの時点で観察したか、またどの時点で格納したかは、メタデータ (監査証跡を含む) の一部として保持する必要がある。自動的に正確な日付時刻情報を取得すべきであり、外部標準〔時刻〕に接続して設定すべきである。
Original Data should be the original first generation/capture of the observation. Certified copies can replace original data (see section 6.5. on certified copies). Information that is originally captured in a dynamic state should remain available in that state.	**原本性** データは、オリジナルの、最初に生成/収集された観察であること。オリジナルデータは保証付きコピーで置き換えることができる。(保証付きコピーについては、6.5 章参照) 。もともと動的な状態で収集された情報は、〔動的な〕状態のままで利用できるようにすべきである。
Accurate The use of computerised systems should ensure that the data are at least as accurate as those recorded on paper. The coding process, which consists in matching text or data collected on the data acquisition tools to terms in a standard dictionary, thesaurus, or tables (e.g. units, scales), should be controlled. The process of data transfer between systems should be validated to ensure the data remain accurate.	**正確性** コンピュータ化システムを使用することで、データが、少なくとも紙に記録されたものと同程度には、正確であることを確実にすること。データ収集ツールで収集されたテキスト又はデータを、標準辞書、シソーラス、又はテーブル (例：単位、尺度) に掲載されている用語と照合するコーディングプロセスは、コントロールする必要がある。システム間のデータ転送プロセスはバリデートして、データの正確性が確実に保たれるようにすること。

Data should be an accurate representation of the observations made. Metadata should contain information to describe the observations and, where appropriate, it could also contain information to confirm its accuracy.	データは、観察結果を正確に表したものとすべきである。メタデータには、観察結果を説明する情報を含めるべきであるが、必要に応じて、その正確性を確認するための情報も含めてもよい。
Complete To reconstruct and fully understand an event, data should be a complete representation of the observation made. This includes the associated metadata and audit trail and may require preserving the original context.	**完全性** データは、イベントを再構築して完全に理解できるように、観察結果を完全に表したものとすること。このためには、関連するメタデータと監査証跡を含む必要がある。また、オリジナルコンテキストを保持しておく必要があるかもしれない。
Consistent Processes should be in place to ensure consistency of the definition, generation/capturing and management (including migration) of data throughout the data life cycle. Processes should be implemented to detect and/or avoid contradictions, e.g. by the use of standardisation, data validation and appropriate training.	**一貫性** データライフサイクル全体を通じて、データの定義、生成/収集、及び管理 (移行を含む) に一貫性を持たせるためのプロセスを設けること。矛盾を検出、及び (又は) 回避するためのプロセス (例：標準化、データバリデーション、及び適切なトレーニングの使用) を設けること。
Enduring Data should be maintained appropriately such that they remain intact and durable through the entire data life cycle, as appropriate, according to regulatory retention requirements (see sections 6.8. and 6.10. on back-up and archiving).	**永続性** データは、必要に応じてデータライフサイクル全体を通じて、規制による保存要件に従って、損傷も劣化もない状態を保てるように適切に維持管理すること。 (バックアップとアーカイブについては、6.8 章 及び 6.10 章を参照) 。
Available when needed Data should be stored throughout the data life cycle and should be readily available for review when needed.	**必要時の可用性** データは、データライフサイクル全体を通じて保管され、必要時にすぐに利用できるようにすること。

Traceable Data should be traceable throughout the data life cycle. Any changes to the data, to the context/metadata should be traceable, should not obscure the original information and should be explained, if necessary. Changes should be documented as part of the metadata (e.g. audit trail).	**追跡可能性** データは、データライフサイクル全体を通じて追跡可能とすること。データやコンテキスト/メタデータへのすべての変更は追跡可能とし、オリジナル情報を隠さないようにし、必要に応じて〔変更を〕説明できるようにすること。変更はメタデータ (例：監査証跡) の一部として記録する必要がある。

4.6. Criticality and risks (重要度とリスク)

ICH E6 describes the need for a quality management system with a risk-based approach. Risks should be considered at both the system level e.g. standard operating procedures (SOPs), computerised systems and staff, and for the specific clinical trial e.g. trial specific data and data acquisition tools or trial specific configurations or customisations of systems.	ICH E6 は、リスクベースアプローチのある品質管理システムの必要性を説明している。リスクはシステムレベル (例：標準操作手順 (SOP)、コンピュータ化システム、及び職員) と特定の治験〔レベル〕 (例：治験固有のデータとデータ収集ツール、又は治験固有の構成設定やシステムのカスタマイズ) の両方を考慮する必要がある。
Risks in relation to the use of computerised systems and especially critical risks affecting the rights, safety and well-being of the trial participants or the reliability of the trial results would be those related to the assurance of data integrity. Those risks should be identified, analysed, and mitigated or accepted, where justified, throughout the life cycle of the system. Where applicable, mitigating actions include revised system design, configuration or customisation, increased system validation or revised SOPs (including appropriate training) for the use of systems and data governance culture.	コンピュータ化システムの使用に関連するリスク、とりわけ治験参加者の権利、安全及び健康又は治験結果の信頼性に影響を与えるような重大なリスクとなるのは、データインテグリティの保証に関連するリスクである。これらのリスクは、システムライフサイクル全体を通じて、特定し、分析したうえで、低減するか、又は (合理的な理由があれば) 受容する。該当する場合、リスク低減措置には、システム設計、構成設定又はカスタマイズの変更、システムバリデーションの強化、又はシステム利用やデータガバナンス文化に関する SOP の改訂 (適切なトレーニングを含む) が含まれる。

In general, risks should be determined based on the system used, its complexity, operator, use of system and data involved. Critical component parts of any system should always be addressed. For example, a component part of an IRT system that calculates IMP dose based on data input by the investigator would be high risk compared to other functionalities such as the generation of an IMP shipment report. The interface and interdependency between systems or system components should be taken into consideration.	一般的に、リスクは、使用するシステム、その複雑さ、操作者、システムの使用方法、及び関連するデータ、に基づいて決定する必要がある。いかなるシステムにおいても、重要な構成部分を、常に〔リスクの検討に〕取り上げる必要がある。例えば、IRT システムでは、治験責任医師が入力したデータに基づいて IMP 服用量を計算する構成部分は、IMP 出荷報告書作成などの他の機能と比べるとリスクが高い。システム間、又はシステム構成部分の間のインターフェースと相互依存性を考慮すること。
All data collected or generated in the context of a clinical trial should fulfil ALCOA++ principles. Consequently, the arrangements for data governance to ensure that data, irrespective of the format in which they are generated, recorded, processed (including analysis, alteration/imputation, transformation, or migration), used, retained (archived), retrieved and destroyed should be considered for data integrity risks and appropriate control processes implemented.	治験というコンテキストで収集又は生成されるすべてのデータは、ALCOA++ 原則を満たす必要がある。その結果、データインテグリティのリスクとして、データが確実に生成、記録、処理 (分析、変更/代入、変換、又は移行を含む) 、使用、保存 (アーカイブ) 、検索、及び破壊されるようにするためのデータガバナンスの計画を考慮に入れ、適切なコントロールプロセスが実装されるようにすること。なお、このことはデータのフォーマットに関係なく当てはまる。
The approach used to reduce risks to an acceptable level should be proportionate to the significance of the risk. Risk reduction activities may be incorporated in protocol design and implementation, system design, coding and validation, monitoring plans, agreements between parties that define roles and responsibilities, systematic safeguards to ensure adherence to SOPs, training in processes and procedures, etc.	リスクを許容レベルにまで低減するために使用されるアプローチは、リスクの重要性に応じたものとすべきである。リスク低減活動は、治験実施計画書の設計と実装、システムの設計、コーディングとバリデーション、モニタリング計画、役割と責任を定義する当事者間の合意、SOP を確実に順守させるための体系的な保護手段、プロセスと手順のトレーニングなどに組み込むとよい。

There are special risks to take into consideration when activities are transferred/delegated. These are further elaborated on in Annex 1 on agreements. The risk-assessment should take the relevance of the system use for the safety, rights, dignity and well- being of the participant and the importance and integrity of derived clinical trial data into account i.e. whether the system is used for standard care and safety measurements for participants or if systems are used to generate primary efficacy data that are relied on in e.g. a marketing authorisation application. Systems used for other purposes than what they were developed for, or which are used outside the supplier's specification/validation are inherently higher risk. In case of well-established computerised systems, which are used as intended in a routine setting for less critical trial data, the certification by a notified body may suffice as documentation whereas other more critical systems may require a more in- depth validation effort. This decision should be justified prior to use in the trial.	活動を移転/委任する際に考慮すべき特別なリスクがあるが、これらについては、合意に関する附属書 1 でさらに詳しく述べる。 リスクアセスメントでは、システムの使用と、参加者の安全／権利／尊厳／健康との関連、及び得られた治験データの重要性とインテグリティ (すなわちシステムが標準的なケアや安全性測定に使用されているのか、又はシステムが、例えば、販売承認申請の根拠となるような、一次有効性データの生成に使用するのか) を考慮に入れる必要がある。開発時とは異なる目的で使用されるシステム、又はサプライヤの仕様/バリデーション外で使用されるシステムは、本質的にリスクが高くなる。十分に確立されたコンピュータ化システムが、重要度の低い治験データのために、通常の設定で、意図した用途で使用されるのであれば、文書として公認機関【訳注】による認証があれば十分であろう。しかし、他のより重要なシステムでは、より詳細なバリデーション作業が必要になる。この決定は、治験で〔コンピュータ化システムを〕使用する前に正当化しておく必要がある。 【訳注】公認機関 (Notified body) は欧州連合における認証機関であり、特定の製品が EU 市場に投入される前に、該当する必須の技術要件への適合性を評価するために加盟国によって指定された組織である。(Wikipedia)

For systems deployed by the investigator/institution specifically for the purposes of clinical trials, the investigator should ensure that the requirements for computerised systems as described in this guideline are addressed and proportionately implemented. For systems deployed by the investigator/institution, the sponsor should determine during site selection whether such systems (e.g. electronic medical records and other record keeping systems for source data collection and the investigator site file) are fit for purpose.	治験責任医師/治験実施医療機関が特に治験の目的で配備するシステムの場合、治験責任医師は、本ガイドラインに記載されているコンピュータ化システムの要件が理解され、適切に実装されていることを確実にすべきである。治験責任医師/治験実施医療機関が配備するシステムについては、治験依頼者は治験実施施設選定時に、それらのシステム (例：電子医療記録や他の記録を管理システムで、原データ収集及び ISF に用いるもの) が目的に適合しているかどうかを判断する必要がある。
For computerised systems deployed by the sponsor, the sponsor should ensure that the requirements of this guideline are addressed and proportionately implemented.	治験依頼者が配備するコンピュータ化システムの場合、治験依頼者は、本ガイドラインの要件が理解され、適切に実装されていることを確実にすべきである。

4.7. Data capture (データ収集)

The clinical trial protocol should specify data to be collected and the processes to capture them, including by whom, when and by which tools.	治験実施計画書には収集するデータ、及びそれらを収集するプロセス (誰が、いつ、どのツールを使用して収集するかを含む) を記述する必要がある。
Data acquisition tools should be designed and/or configured or customised to capture all information required by the protocol and not more. Data fields should not be prepopulated or automatically filled in, unless these fields are not editable and are derived from already entered data (e.g. body surface area). The protocol should identify any data to be recorded directly in the data acquisition tools and identify them as source data.	データ収集ツールは、治験実施計画書で求められるすべての情報 (ただし、それ以上は不要) を収集するように設計し、及び (又は) 構成設定又はカスタマイズする必要がある。データフィールドにはデータを事前に埋めておかないこと。また、自動的に入力しないこと。ただし、フィールドが編集不可の場合や、すでに入力されたデータから得られる (例：体表面積) 場合はその限りではない。治験実施計画書では、データ収集ツールにより直接記録されるデータを特定し、それらを原データとして識別すべきである。

A detailed diagram and description of the transmission of electronic data (data flow) should be available in the protocol or a protocol-related document. The sponsor should describe which data will be transferred and in what format, the origin and destination of the data, the parties with access to the transferred data, the timing of the transfer and any actions that may be applied to the data, for example, data validation, reconciliation, verification, and review. The use of a data management plan (DMP) is encouraged. The sponsor should ensure the traceability of data transformations and derivations during data processing and analysis.	電子データの転送の詳細な図及び説明 (データフロー) は、治験実施計画書、又は治験実施計画書の関連文書で参照できるようにすること。治験依頼者は、どのデータがどのようなフォーマットで転送されるか、データの転送元と転送先、転送されたデータにアクセスできる当事者、転送のタイミング、及びデータに対するアクション (例えば、データバリデーション、修正、検証、及びレビュー) について説明すべきである。データマネジメント計画書 (DMP) を用いることを勧める。 治験依頼者は、データを処理／分析する際のデータ変換／導出についての追跡可能性を確保する必要がある。

4.8. Electronic signatures (電子署名)

Whenever ICH E6 requires a document to be signed and an electronic signature is used for that purpose, the electronic signature functionality should meet the expectations stated below regarding authentication, non-repudiation, unbreakable link, and timestamp of the signature. The system should thus include functionality to: • authenticate the signatory, i.e. establish a high degree of certainty that a record was signed by the claimed signatory; • ensure non-repudiation, i.e. that the signatory cannot later deny having signed the record;	ICH E6 において文書へ署名することが求められ、その目的で電子署名を使用する場合、電子署名機能は、認証、否認防止、壊れないリンク、及び署名のタイムスタンプに関して、以下に示す期待事項を満たすこと。 システムには次の機能を持たせること： • 署名者を認証する機能。すなわち、記録に署名したと言う者が確かに署名したことについて高度な確実性を確立する。 • 否認防止を確実にする機能。すなわち、署名者が、記録に署名したことを後で否定できないようにする。

• ensure an unbreakable link between the electronic record and its signature, i.e. that the contents of a signed (approved) version of a record cannot later be changed by anyone without the signature being rendered visibly invalid; • provide a timestamp, i.e. that the date, time, and time zone when the signature was applied is recorded.	• 電子記録とその署名の間の壊れないリンクを確実にする機能。すなわち、署名された (承認された) バージョンの記録の内容は後から誰も変更することができない。変更した時は、署名が無効になり、そのことが見て明らかとなる。 • タイムスタンプを提供する機能。すなわち、署名が適用された日付、時刻、タイムゾーンが記録される。
Electronic signatures can further be divided into two groups depending on whether the identity of the signatory is known in advance, i.e. signatures executed in '*closed*' and in '*open*' systems.	電子署名は、署名者の身元が事前にわかっているかどうかによって、さらに 2 つのグループに分けられる。すなわち「*クローズド*」システムで実行される署名と「*オープン*」システムで実行される署名である。
For '*closed*' systems, which constitute the majority of systems used in clinical trials and which are typically provided by the responsible party or by their respective service provider, the system owner knows the identity of all users and signatories and grants and controls their access rights to the system. Regulation (EU) No 910/2014 ('*eIDAS*') on electronic identification and trust services for electronic transactions is not applicable for '*closed*' systems ('*eIDAS*' article 2.2). The electronic signature functionality in these systems should be proven during system validation to meet the expectations mentioned above.	「*クローズド*」システムは、治験で使用されるシステムの大部分を占め、通常は責任のある当事者又はサービスプロバイダが提供する。システムオーナーはすべてのユーザーと署名者の身元を知っており、システムへのアクセス権を付与及びコントロールする。電子トランザクションの電子識別及びトラストサービスに関する Regulation (EU) No 910/2014 (「*eIDAS*」) は、「*クローズド*」システムには適用されない (「*eIDAS*」第 2.2 条)。これらのシステムの電子署名機能は、上記の期待事項を満たすことをシステムバリデーション実施時に証明する必要がある。

For '*open*' systems, the signatories (and users) are not known in advance. For sites located in the EU, electronic signatures should meet the requirements defined in the '*eIDAS*' regulation. Sites located in third countries should use electronic or digital signature solutions compliant with local regulations and proven to meet the expectations mentioned above. Irrespective of the media used, in case a signature is applied on a different document or only on part of a document (e.g. signature page), there should still be an unbreakable link between the electronic document to be signed and the document containing the signature.	「*オープン*」システムの場合、署名者 (及びユーザー) は事前にわからない。治験実施施設が EU にある場合、電子署名は「*eIDAS*」規制で定められている要件を満たす必要がある。第三国にあるサイトは、現地の規制に準拠し、かつ上記の期待事項を満たすことが証明された電子署名／デジタル署名ソリューションを使用すること。 使用する媒体に関係なく、署名が別文書又は文書の一部のみ (例：署名ページ) に適用される場合、署名対象となる電子文書と署名を含む文書の間に、壊れないリンクが必要である。

4.9. Data protection (データ保護)

The confidentiality of data that could identify trial participants should be protected, respecting privacy and confidentiality rules in accordance with the applicable regulatory requirement(s). The requirements of General Data Protection Regulation (EU) No 2016/679 (GDPR) on the protection of individuals with regard to the processing of personal data and on the free movement of such data should be followed except when specific requirements are implemented for clinical trials e.g. that a trial participant does not have the right to be forgotten (and for the data to be consequently deleted) as this would cause bias to e.g. safety data (Regulation (EU) No 536/2014 recital 76 and Article 28(3)). Trial participants should be informed accordingly.	治験参加者を特定することのできるデータは、適用される規制要件に沿った個人情報及び機密保持規則に従い、機密性を保護する必要がある。 個人データの処理に関する個人の保護、及びそのようなデータの自由な移動に関する規制である General Data Protection Regulation (EU) No 2016/679 (GDPR) の要件に従う必要があるが、治験で特定の要件が実施されている場合を除く。例えば、安全性データなどに偏りが生じないよう、治験参加者が忘れられる (つまりは結果的にデータが削除される) 権利を持たないような場合である。(Regulation (EU) No 536/2014 の recital76 及び第 28 (3) 条)。治験参加者には、その旨を通知する必要がある。

In accordance with EU data protection legislation, if personal data of trial participants from an EU Member State are processed (at rest or in transit) or transferred to a third country or international organisation, such data transfer must comply with applicable Union data protection. In summary, this means that the transfer must be either carried out on the basis of an adequacy decision (Article 45 of GDPR, Article 47 of Regulation (EU) No 2018/1727 - EUDPR), otherwise the transfer must be subject to appropriate safeguards (as listed in Article 46 of GDPR or Article 48 of EUDPR) or the transfer may take place only if a derogation for specific situations apply (under Article 49 of GDPR or Article 50 of EUDPR).	EU データ保護法によると、EU 加盟国の治験参加者の個人データが、 (保存時又は転送時に) 第三国又は国際機関で処理される、又は転送される場合、そのようなデータ転送は、適用される EU データ保護に準拠しなければならない。すなわち、転送は、適切な決定に基づいて実行する (GDPR の第 45 条、規則 (EU) No 2018/1727 - EUDPR の第 47 条)。さもなければ転送に際して (GDPR の第 46 条又は EUDPR の第 48 条に記載されるような) 適切な保護策を講じる、或いは (GDPR の第 49 条又は EUDPR の第 50 条に基づき) 特定の状況の特例が適用される場合にのみ転送を行う、のいずれかでなければならない。

4.10. Validation of systems (システムのバリデーション)

Computerised systems used within a clinical trial should be subject to processes that confirm that the specified requirements of a computerised system are consistently fulfilled, and that the system is fit for purpose. Validation should ensure accuracy, reliability, and consistent intended performance, from the design until the decommissioning of the system or transition to a new system.	治験で使用されるコンピュータ化システムは、コンピュータ化システムの仕様で定めた要件が一貫して満たされていること、及びシステムが目的に適合していることを確認するプロセスに従うこと。バリデーションは、設計からシステムの運転停止又は新システムへの移行までの間、正確性、信頼性、及び一貫した意図どおりのパフォーマンスを確実にするものである。
The processes used for the validation should be decided upon by the system owner (e.g. sponsors, investigators, technical facilities) and described, as applicable. System owners should ensure adequate oversight of validation activities (and associated records) performed by service providers to ensure suitable procedures are in place and that they are being adhered to.	バリデーションに使用されるプロセスは、システムオーナー (例：治験依頼者、治験責任医師、技術施設) が決定し、必要に応じて記述すること。システムオーナーは、サービスプロバイダによるバリデーション活動 (及び関連する記録) が適切に監督されるようにし、適切な手順が設けられ、それらが順守されることを確実にすべきである。

Documentation (including information within computerised systems used as process tools for validation activities) should be maintained to demonstrate that the system is maintained in the validated state. Such documentation should be available for both the validation of the computerised system and for the validation of the trial specific configuration or customisation.	システムがバリデートされた状態で維持されていることを示すために、文書一式 (バリデーション活動のプロセスツールとして使用されるコンピュータ化システム内の情報を含む) を維持管理する必要がある。このような文書は、コンピュータ化システムのバリデーションと、治験固有の構成設定又はカスタマイズのバリデーションの両方〔のレベル〕で用意する必要がある。
Validation of the trial specific configuration or customisation should ensure that the system is consistent with the requirements of the approved clinical trial protocol and that robust testing of functionality implementing such requirements is undertaken, for example, eligibility criteria questions in an eCRF, randomisation strata and dose calculations in an IRT system. See Annex 2 for further detail on validation.	治験固有の構成設定又はカスタマイズのバリデーションでは、承認された治験実施計画書の要件とシステムが一致していること、及びそのような要件を実装する機能 (例えば、eCRF の適格基準の質問、IRT システムでの無作為化階層と用量の計算) について堅牢なテストが行われることを確実にすること。 バリデーションの詳細については、付属書 2 を参照のこと。

4.11. Direct access (直接アクセス)

All relevant computerised systems should be readily available with full, direct and read-only access (this requires a unique identification method e.g. username and password) upon request by inspectors from regulatory authorities. If a computerised system is decommissioned, direct access (with a unique identification method) to the data in a timely manner should still be ensured (see section 6.12.).	規制当局の査察官からの要求に応じて、完全な、直接の読み取り専用アクセス (ユーザー名とパスワードのようなユニークな識別方法が必要) により、関連するすべてのコンピュータ化システムをすぐに利用できるようにすること。コンピュータ化システムを運転停止した場合であっても、タイムリーに (ユニークな識別方法を使用して) データへの直接アクセスが引き続きできるようにしておく必要がある (6.12 章参照) 。

5. Computerised systems (コンピュータ化システム)

Requirements for validation are described in section 4.10. and Annex 2, the requirements for user management are described in Annex 3, while the requirements for information technology (IT) security are detailed in Annex 4 of this guideline.	バリデーションの要件は、4.10 章及び付属書 2 で説明している。ユーザー管理の要件は付属書 3 に説明しており、情報技術 (IT) セキュリティの要件は本ガイドラインの付属書 4 に詳述している。

5.1. Description of systems (システムの説明)

The responsible party should maintain a list of physical and logical locations of the data e.g. servers, functionality and operational responsibility for computerised systems and databases used in a clinical trial together with an assessment of their fitness for purpose. Where multiple computerised systems/databases are used, a clear overview should be available so the extent of computerisation can be understood. System interfaces should be described, defining how the systems interact, including validation status, methods used, and security measures implemented.	責任のある当事者は、データの物理的及び論理的な場所 (例：サーバー)、コンピュータ化システムの機能及び運用の責任、及び治験で使用しているデータベースを、システム目的への適合性のアセスメント結果とともにリストにして維持管理すること。 〔1 つの業務に〕複数のコンピュータ化システム/データベースを使用している場合は、それぞれどの範囲をコンピュータ化しているのかを理解できるように、分かりやすい概要を用意すること。システム間でどのように相互作用するか (バリデーション状況、使用される方式、実装されているセキュリティ対策などを含む) を定義するシステムインターフェイスを記述すべきである。

5.2. Documented procedures (文書化された手順)

Documented procedures should be in place to ensure that computerised systems are used correctly. These procedures should be controlled and maintained by the responsible party.	文書化された手順を設け、コンピュータ化システムが正しく使用されるようにする必要がある。これらの手順は、責任のある当事者がコントロール及び維持管理する必要がある。

5.3. Training (トレーニング)

Each individual involved in conducting a clinical trial should be qualified by education, training, and experience to perform their respective task(s). This also applies to training on computerised systems. Systems and training should be designed to meet the specific needs of the system users (e.g. sponsor, investigator or service provider). Special consideration should be given to the training of trial participants when they are users.	治験の実施に関与する各個人は、それぞれのタスクを実行するための教育／トレーニング／経験に関して適格である必要がある。これは、コンピュータ化システムについてのトレーニングにも当てはまる。システム及びトレーニングは、システムユーザー (例: 治験依頼者、治験責任医師、又はサービスプロバイダ) の特定のニーズを満たすように設計すべきである。治験参加者がユーザーである場合のトレーニングには、特別な配慮が必要となる。
There should be training on the relevant aspects of the legislation and guidelines for those involved in developing, coding, building, and managing trial specific computerised systems, for example, those employed at a service provider supplying eCRF, IRT, ePRO, trial specific configuration, customisation, and management of the system during the conduct of the clinical trial.	治験固有のコンピュータ化システムの開発、コーディング、構築、及び管理に携わる者 (例えば、治験実施中に eCRF、IRT、ePRO、治験固有の構成設定、カスタマイズ、システム管理、を提供するサービスプロバイダの社員) に対して、法律及びガイドラインの関連部分についてトレーニングを提供する必要がある。
All training should be documented, and the records retained and available for monitoring, auditing, and inspections.	すべてのトレーニングは文書化し、記録を保管し、モニタリング／監査／査察時に提供できるようにしておくこと。

5.4. Security and access control (セキュリティとアクセスコントロール)

To maintain data integrity and the protection of the rights of trial participants, computerised systems used in clinical trials should have security processes and features to prevent unauthorised access and unwarranted data changes and should maintain blinding of the treatment allocation where applicable.	データインテグリティと治験参加者の権利の保護を維持し続けるために、治験で使用されるコンピュータ化システムには、許可のないアクセスと不当なデータ変更を防ぐためのセキュリティプロセスと機能を設けておくこと。また、該当する場合は治療割付の盲検性を維持する必要がある。

Checks should be used to ensure that only authorised individuals have access to the system and that they are granted appropriate permissions (e.g. ability to enter or make changes to data). Records of authorisation of access to the systems, with the respective levels of access clearly documented, should be maintained. The system should record changes to user roles and thereby access rights and permissions.	チェックを行って、許可された個人のみがシステムにアクセスできていること、及び適切な権限 (例：データを入力する権限又は変更する権限) が付与されていることを確実にすること。システムへのアクセス許可の記録を維持管理すべきであり、そこには〔許可した〕アクセスレベルを明確に記録する。システムでは、ユーザーロール (及びそれに伴うアクセス権とアクセス許可) の変更を記録するようにすること。
There should be documented training on the importance of security e.g. the need to protect passwords and to keep them confidential, enforcement of security systems and processes, identification and handling of security incidents, social engineering and the prevention of phishing.	セキュリティの重要性に関する文書化されたトレーニングが必要である。例えば、パスワードの保護とパスワードを秘密にしておくことの必要性、セキュリティシステム／プロセスの励行、セキュリティインシデントの特定と取扱い、ソーシャルエンジニアリング及びフィッシングの防止などである。
See Annexes 3 and 4 for further guidance on user management and IT security.	ユーザー管理と IT セキュリティに関する詳細なガイダンスについては、付属書 3 と 4 を参照のこと。

5.5. Timestamp (タイムスタンプ)

Accurate and unambiguous date and time information given in coordinated universal time (UTC) or time and time zone (set by an external standard) should be automatically captured.	正確かつ明瞭な日付と時刻の情報は、協定世界時 (UTC) で 、又は時刻と (外部標準で定められた) タイムゾーン〔の組み合わせ〕で、自動的に取得すべきである。
Users should not be able to modify the date, time and time zone on the device used for data entry, when this information is captured by the computerised system and used as a timestamp.	データ入力に用いるデバイスの日付／時刻／タイムゾーンは、それがコンピュータ化システムによって収集され、タイムスタンプとして使用される場合、ユーザーが変更できないようにすること。

6. Electronic data (電子記録)

For each trial, it should be identified what electronic data and records will be collected, modified, imported and exported, archived and how they will be retrieved and transmitted. Electronic source data, including the audit trail should be directly accessible by investigators, monitors, auditors, and inspectors without compromising the confidentiality of participants' identities.	治験ごとに、収集、変更、インポート／エクスポート、アーカイブされる電子データ及び電子記録と、それらの収集／転送方法を特定する必要がある。監査証跡を含む電子原データは、参加者の身元の機密性を損なうことなく、治験責任医師、モニター、監査者、及び査察官が直接アクセスできるようにすること。

6.1. Data capture and location (データ収集と場所)

The primary goal of data capture is to collect all data required by the protocol. All pertinent observations should be documented in a timely manner. The location of all source data should be specified prior to the start of the trial and updated during the conduct of the trial where applicable.	データ収集の主な目的は、治験実施計画書が求めるすべてのデータを集めることである。関連するすべての観察結果はタイムリーに記録に残す必要がある。すべての原データの場所は、治験開始前に指定し、治験実施中に必要に応じて更新する必要がある。

6.1.1. Transcription (転記)

Source data collected on paper (e.g. worksheets, paper CRFs or paper diaries or questionnaires) need to be transcribed either manually or by a validated entry tool into the electronic data collection (EDC) system or database(s). In case of manual transcription, risk-based methods should be implemented to ensure the quality of the transcribed data (e.g. double data entry and/or data monitoring).	紙で収集された原データ (例：ワークシート、紙の CRF、紙の日記やアンケート) は、手作業で、又はバリデート済みの入力ツールを使用して、電子データ収集 (EDC) システム又はデータベースに転記する必要がある。手作業で転記する場合、転記データの品質を確保するために、リスクに応じた方法 (例：二重データ入力、及び (又は) データモニタリング) で実施する必要がある。

6.1.2. Transfer (転送)

Trial data are transferred in and between systems on a regular basis. The process for file and data transfer needs to be validated and should ensure that data and file integrity are assured for all transfers.	治験データは日常的にシステム内及びシステム間で転送される。ファイルやデータを転送するプロセスはバリデートする必要があり、すべての転送においてデータとファイルのインテグリティが保証されるようにする必要がある。
Data that is collected from external sources and transferred in open networks should be protected from unwarranted changes and secured/encrypted in a way that precludes disclosure of confidential information.	外部ソースから集められ、オープンネットワークで転送されるデータは、不当な変更から保護し、機密情報を漏らさない方法で保護/暗号化する必要がある。
All transfers that are needed during the conduct of a clinical trial need to be pre-specified.	治験実施中に必要となるすべての転送は、事前に特定しておく必要がある。
Validation of transfer should include appropriate challenging test sets and ensure that the process is available and functioning at clinical trial start (e.g. to enable ongoing sponsor review of diary data, lab data or adverse events by safety committees). Data transcribed or extracted and transferred from electronic sources and their associated audit trails should be continuously accessible (according to delegated roles and corresponding access rights).	転送のバリデーションには適切な厳しいテストセットを含めるようにし、(例えば、治験依頼者が継続的に日誌データ、ラボデータ、又は安全委員会からの有害事象をレビューできるように) 治験開始時に〔デ―タ転送〕プロセスが利用可能で、機能することを確実にしておくこと。転記されたデータ、又は電子ソースから抽出／転送されたデータとそれに関連する監査証跡は、(委任された役割とそれに応じたアクセス権に従って) いつでもアクセスできるようにしておくこと。
Transfer of source data and records when the original data or file are not maintained is a critical process and appropriate considerations are expected in order to prevent loss of data and metadata.	オリジナルデータ／ファイルが維持管理されない状況では、原データや記録の転送は重要なプロセスであり、データ及びメタデータの損失を防ぐための適切な考慮が必要である。

6.1.3. Direct capture (直接収集)

Direct data capture can be done by using electronic data input devices and applications such as electronic diaries, electronic questionnaires and eCRFs for direct data entry. Where treatment-related pertinent information is captured first in a direct data capture tool such as a trial participant diary, a PRO form or a special questionnaire, a documented procedure should exist to transfer or transcribe information into the medical record, when relevant.	直接データ収集 (DDC) は、 (電子日記、電子アンケート、DDC 用 eCRF などの) 電子データ入力デバイスやアプリケーションを利用することで実現できる。治療関連の情報 (治験参加者の日記、PRO フォーム、又は特別なアンケートなど) が、最初に DDC ツールで収集される場合、必要時に情報を医療記録へ転送／転記するための文書化された手順を設けておく必要がある。
Direct data capture can also be done by automated devices such as wearables or laboratory or other technical equipment (e.g. medical imaging, electrocardiography equipment) that are directly linked to a data acquisition tool. Such data should be accompanied by metadata concerning the device used (e.g. device version, device identifiers, firmware version, last calibration, data originator, timestamp of events).	また DDC は自動化されたデバイスを利用することによっても実現できる。例えばウェアラブル、検査室や他の技術機器 (例：医療用画像、心電図機器) などの、データ収集ツールに直接リンクされたデバイスである。このようなデータとともに、使用するデバイスに関するメタデータ (例：デバイスのバージョン、デバイス識別子、ファームウェアバージョン、最後のキャリブレーション、データオリジネータ、イベントのタイムスタンプ) も一緒に集める必要がある。

6.1.4. Edit checks (エディットチェック)

Computerised systems should validate manual and automatic data inputs to ensure a predefined set of validation criteria is adhered to. Edit checks should be relevant to the protocol and developed and revised as needed. Edit checks should be validated and implementation of the individual edit checks should be controlled and documented. If edit checks are paused at any time during the trial, this should be documented and justified. Edit checks could either be run immediately at data entry or automatically during defined intervals (e.g. daily) or manually.	コンピュータ化システムにより、手作業及び自動で入力されたデータをバリデートして、予め定義された一連のバリデーション基準が順守されていることを確実にすること。エディットチェックは、治験実施計画書に沿ったものとし、必要に応じて開発及び改訂を行うこと。エディットチェックをバリデートし、個々のエディットチェックの実装をコントロールし文書化する必要がある。治験実施中にエディットチェックの使用を中断した場合は、これを記録し、正当化する必要がある。エディットチェックは、データ入力時に直ちに実行してもよいし、定義された間隔 (例：毎日) で自動的又は手作業で実行してもよい。
Such approaches should be guided by necessity, should not cause bias and should be traceable e.g. when data are changed as a result of an edit check notification.	〔エディットチェックを〕どのように行うかは必要性に鑑みて決めるべきである。〔エディットチェックは〕バイアスを引き起こすものであってはならない。また追跡可能性 (例：エディットチェック通知の結果としていつデータが変更されたか) を持たせること。
The sponsor should not make automatic or manual changes to data entered by the investigator or trial participants unless authorised by the investigator.	治験依頼者は、治験責任医師の許可がない限り、治験責任医師又は治験参加者が入力したデータを自動又は手作業で変更すべきではない。

6.2. Audit trail and audit trail review (監査証跡と監査証跡レビュー)

6.2.1. Audit trail (監査証跡)

An audit trail should be enabled for the original creation and subsequent modification of all electronic data. In computerised systems, the audit trail should be secure, computer generated and timestamped.	すべての電子データのオリジナルの生成とその後の変更を記録するために監査証跡を有効にしておくこと。コンピュータ化システム内にて、監査証跡はセキュアで、コンピュータで生成され、タイムスタンプが付けられていること。
An audit trail is essential to ensure that changes to the data are traceable. Audit trails should be robust, and it should not be possible for '*normal*' users to deactivate them. If possible, for an audit trail to be deactivated by '*admin users*', this should automatically create an entry into a log file (e.g. audit trail). Entries in the audit trail should be protected against change, deletion, and access modification (e.g. edit rights, visibility rights). The audit trail should be stored within the system itself. The responsible investigator, sponsor, and inspector should be able to review and comprehend the audit trail and therefore audit trails should be in a human-readable format.	データ変更の追跡可能性を確実にするために監査証跡は不可欠である。監査証跡は堅牢である必要があり、「*通常の*」ユーザーが非アクティブ化できないようにする必要がある。「*管理者ユーザー*」が監査証跡を非アクティブ化できたとしても、可能であれば〔そのことを〕自動的にログファイル (例：監査証跡) に記録すること。監査証跡記録は、変更、削除、及びアクセスの変更 (例：編集権限、表示権限) から保護すべきである。監査証跡は、システム本体に保存する必要がある。責任ある治験責任医師、治験依頼者、及び査察官が監査証跡を確認して理解できることが必要であり、そのために監査証跡は見読性のあるフォーマットにすべきである。

Audit trails should be visible at data-point level in the live system, and it should be possible to export the entire audit trail as a dynamic data file to allow for the identification of systematic patterns or concerns in data across trial participants, sites, etc. The audit trail should show the initial entry and the changes (value - previous and current) specifying what was changed (field, data identifiers) by whom (username, role, organisation), when (date/timestamp) and, where applicable, why (reason for change).	運用中のシステムにおいては、監査証跡をデータポイントレベルで確認できるようにすべきであり、監査証跡全体を動的データファイルとしてエクスポートし、治験参加者や治験実施施設などを横通ししたデータから体系的なパターンや懸念事項を特定できるようにすること。監査証跡では、最初のエントリと変更 (変更前後の値) を示すこと。変更については、何を (フィールド、データ識別子) 、誰が (ユーザー名、役割、組織) 、いつ (日付/タイムスタンプ) 、及び該当する場合、なぜ (変更の理由) を特定する。
A procedure should be in place to address the situation when a data originator (e.g. investigator or trial participant) realises that she/he has submitted incorrect data by mistake and wants to correct the recorded data.	データオリジネータ (例：治験責任医師や治験参加者) が正しくないデータを誤って提出したことに気づき、記録されたデータを修正したい場合に対応するための手順を設けること。
It is important that original electronic entries are visible or accessible (e.g. in the audit trail) to ensure the changes are traceable. The audit trail should record all changes made as a result of data queries or a clarification process. The clarification process for data entered should be described and documented. Changes to data should only be performed when justified. Justification should be documented. In case the data originator is the trial participant, special considerations to data clarifications might be warranted. See Annex 5 section A5.1.1.4 for further details.	変更の追跡可能性を保証するために、 (例えば監査証跡により) オリジナルの電子的な入力を表示又はアクセスできることが重要である。監査証跡には、データクエリ又はクラリフィケーションプロセスの結果として行われたすべての変更を記録する必要がある。入力データのクラリフィケーションプロセスを説明し、文書化しておく必要がある。データへの変更は、正当な理由がある場合に限定し、その正当性を文書化すべきである。データオリジネータが治験参加者である場合、データクラリフィケーションについて特別な配慮が必要になる場合がある。詳細については、付属書 5 A5.1.1.4 章を参照。

For certain types of systems (e.g. ePRO) the data entered may not be uploaded immediately but may be temporarily stored in local memory. Such data should not be edited or changed without the knowledge of the data originator prior to saving. Any changes or edits should be acknowledged by the data originator, should be documented in an audit trail and should be part of validation procedures. The timestamp of data entry in the capture tool (e.g. eCRF) and timestamp of data saved to a hard drive should be recorded as part of the metadata. The duration between initial capture in local memory and upload to a central server should be short and traceable (i.e. transaction time), especially in case of direct data entry.	ある種類のシステム (例：ePRO) では、入力されたデータがすぐにアップロードされず、一時的にローカルメモリに保存される場合がある。このようなデータは、保存される前に、データオリジネータの知らないところで編集又は変更できてはならない。すべての変更又は編集は、データオリジネータによって承認され、監査証跡に記録され、バリデーション手順に組み込まれている必要がある。収集ツール (例：eCRF) に入力されたデータのタイムスタンプと、ハードドライブに保存されたデータのタイムスタンプは、メタデータの一部として記録する必要がある。ローカルメモリに最初に保存された時刻と中央サーバーへアップロードされた時刻の間の時間は、特に直接データ入力の場合、短くすべきであり、かつ追跡可能 (すなわち、トランザクション時間) とすべきである。
Data extracts or database extracts for internal reporting and statistical analysis do not necessarily need to contain the audit trail information. However, the database audit trail should capture the generation of data extracts and exports.	内部報告や統計分析のためのデータ抽出やデータベース抽出には必ずしも監査証跡情報は必要ではない。ただし、データベースの監査証跡には、データ抽出とエクスポートの生成を記録すること。
Audit trails should capture any changes in data entry per field and not per page (e.g. eCRF page).	監査証跡は、ページ (例：eCRF ページ) 単位ではなくフィールド単位でデータ入力の変更を記録すること。
In addition to the audit trail, metadata could also include (among others) review of access logs, event logs, queries etc.	メタデータ〔のレビュー〕は、監査証跡だけでなく（いろいろあり）アクセスログ、イベントログ、クエリなどのレビューも含まれる。

Access logs, including username and user role, are in some cases considered to be important metadata and should consequently be available. This is considered necessary e.g. for systems that contain critical unblinded data. Care should be taken to ensure that information jeopardising the blinding does not appear in the audit trail accessible to blinded users.	(ユーザー名とユーザーロールを含む) アクセスログは、場合によっては重要なメタデータと見なされるため、利用できるようにしておく必要がある。これは、例えば重要な非盲検化データを含むシステムなどでは、必要であると考えられる。 盲検化対象となっているユーザーがアクセスできる監査証跡に、盲検化を危うくするような情報が含まれないよう注意する必要がある。

6.2.2. Audit trail review (監査証跡レビュー)

Procedures for risk-based trial specific audit trail reviews should be in place and performance of data review should be generally documented. Data review should focus on critical data. Data review should be proactive and ongoing review is expected unless justified. Manual review as well as review by the use of technologies to facilitate the review of larger datasets should be considered. Data review can be used to (among others) identify missing data, detect signs of data manipulation, identify abnormal data/outliers and data entered at unexpected or inconsistent hours and dates (individual data points, trial participants, sites), identify incorrect processing of data (e.g. non-automatic calculations), detect unauthorised accesses, detect device or system malfunction and to detect if additional training is needed for trial participants /site staff etc. Audit trail review can also be used to detect situations where direct data capture has been defined in the protocol but where this is not taking place as described.	治験の監査証跡をリスクベースでレビューするための手順を設けること。また、データレビューのパフォーマンスを一般的に記録すること。データレビューは、重要なデータに焦点を当てること。データレビューはプロアクティブに行う必要があり、正当な理由がない限り、継続的にレビューすることが期待される。手作業によるレビューでもよいし、大規模なデータセットのレビューを容易にする技術を使用したレビューでもよい。データレビューを行うことで、欠落データの特定、データ改ざんの兆候の検出、異常/基準外のデータ、及び予想外又は一貫性のない時刻や日付に入力されたデータ (例：個々のデータポイント、治験参加者、治験実施施設) の特定、不適切なデータの処理 (例：自動でない計算) の特定、許可のないアクセスの検出、デバイス又はシステムの誤動作の検出、及び治験参加者/治験実施施設の職員などへの追加トレーニングの必要性の検出 (など) ができるようになる。監査証跡をレビューすることにより、治験実施計画書では DDC を行うと記載しながら、実際には行われていないという状況を検出することもできる。
In addition to audit trail review, metadata review could also include (among others) review of access logs, event logs, queries, etc.	メタデータのレビューには、監査証跡のレビューの他に、アクセスログ、イベントログ、クエリなどのレビュー (など) も含まれる。
The investigator should receive an introduction on how to navigate the audit trail of their own data in order to be able to review changes.	治験責任医師は、自分たちのデータに対する監査証跡をナビゲートする方法について説明を受け、変更をレビューできるようにしておくこと。

6.3. Sign-off of data (データへの署名)

The investigators are responsible for data entered into eCRFs and other data acquisition tools under their supervision (electronic records).	治験責任医師は、自分の監督下にある eCRF やその他のデータ収集ツールに入力されたデータ (電子記録) に責任を負う。
The sponsor should seek investigator endorsement of their data at predetermined milestones. The signature of the investigator or authorised member of the investigator's staff is considered as the documented confirmation that the data entered by the investigator and submitted to the sponsor are attributable, legible, original, accurate, and complete and contemporaneous. Any member of the staff authorised for sign-off should be qualified to do so in order to fulfil the purpose of the review as described below. National law could require specific responsibilities, which should then be followed.	治験依頼者は、彼らのデータについて、あらかじめ決められたマイルストーンで治験責任医師の承認を求める必要がある。治験責任医師、又は治験責任医師スタッフの許可されたメンバーによる署名は、治験責任医師により入力され、治験依頼者に提出されたデータが、帰属性、判読性、原本性、正確性、完全性、同時性を満たしていることについての文書化された確認であると見なされる。署名の権限を与えられたスタッフは、以下に説明するレビューの目的を達成するために、署名者として適格である必要がある。国内法は特定の責任を要求する可能性があり、その場合はそれに従う必要がある。

The acceptable timing and frequency for the sign-off needs to be defined and justified for each trial by the sponsor and should be determined by the sponsor in a risk-based manner. The sponsor should consider trial specific risks and provide a rationale for the risk-based approach. Points of consideration are types of data entered, non-routine data, importance of data, data for analysis, length of the trial and the decision made by the sponsor based on the entered data, including the timing of such decisions. It is essential that data are confirmed prior to interim analysis and the final analysis, and that important data related to e.g. reporting of serious adverse events (SAEs), adjudication of important events and endpoint data, data and safety monitoring board (DSMB) review, are signed off in a timely manner. In addition, a timely review and sign-off of data that are entered directly into the eCRF as source is particularly important.	許容可能な署名のタイミングと頻度は、治験依頼者が治験ごとに定義及び正当化し、リスクベースで決定すること。治験依頼者は、治験固有のリスクを考慮し、リスクベースアプローチの根拠を提供する必要がある。考慮すべき点は、入力データの種類、非日常的なデータ、データの重要性、分析用データ、治験期間、入力されたデータに基づいて治験依頼者が行う決定 (決定を行うタイミングも含む)である。中間分析と最終分析の前にデータを確認することは必須である。また、例えば serious adverse events (SAEs)の報告、重要なイベントやエンドポイントデータの裁定、data and safety monitoring board (DSMB) のレビューなどに関連する重要なデータをタイムリーに承認することが不可欠である。さらに、ソースとして eCRF に直接入力されたデータをタイムリーにレビューし、署名することは特に重要である。
Therefore, it will rarely be sufficient to just provide one signature immediately prior to database lock. Signing of batches of workbooks is also not suited to ensure high data quality and undermines the purpose of timely and thorough data review.	以上から、データベースがロックされる直前に 1 つの署名を提供するだけでは十分とはいえない。ワークブックをまとめて署名することも、高いデータ品質を確実にするためには適しておらず、タイムリーで徹底的なデータレビューを行うという目的が台無しになる。
For planned interim analysis, e.g. when filing for a marketing authorisation application, all submitted data need to be signed off by the investigator or their designated and qualified representative before extracting data for analysis. The systems should be designed to support this functionality.	(例えば、販売承認申請書を提出する場合などに) 計画的な中間分析を行う場合、提出されるすべてのデータは、分析用にデータを抽出する前に、治験責任医師又は指定された適格な代表者によって署名される必要がある。システムは、この機能をサポートするように設計すること。

To facilitate timely data review and signing by the investigator or their designated representative, the design of the data acquisition tool should be laid out to support the signing of the data at the defined time points.	タイムリーなデータのレビューと治験責任医師又は指定された代表者による署名を容易にするために、データ収集ツールの設計を明らかにし、決められた時点でのデータへの署名をサポートすること。
Furthermore, it is important that the investigator review the data on an ongoing basis in order to detect shortcomings and deficiencies in the trial conduct at an early stage, which is the precondition to undertake appropriate corrective and preventive actions.	さらに、治験責任医師が継続的にデータをレビューし、早期段階で治験実施に関わる欠点や欠陥を検出することが重要である。このことは適切な是正・予防措置を講じるための前提条件である。
Adequate oversight by the investigator is a general requirement to ensure participant safety as well as data quality and integrity. Oversight can be demonstrated by various means, one of them being the review of reported data. Lack of investigator oversight may prevent incorrect data from being corrected in a timely manner and necessary corrective and preventive actions being implemented at the investigator site.	治験責任医師が適切に監督を行うことは、参加者の安全、及びデータ品質とデータインテグリティを確実にするための一般的な要件である。監督を行うやり方はさまざまであるが、その 1 つが報告されたデータのレビューである。治験責任医師が監督していないと、不正確なデータがタイムリーに修正されなかったり、治験実施施設で必要な是正・予防措置が実施されなかったりするかもしれない。

6.4. Copying data (データのコピー)

Data can be copied or transcribed for different purposes, either to replace source documents or essential documents or to be distributed amongst different stakeholders as working copies. If essential documents or source documents are irreversibly replaced by a copy, the copy should be certified (see section 6.5.).	データは、さまざまな目的でコピー又は転記することができる。コピーで原資料又は重要な文書を置き換える場合もあれば、作業用コピーとしてさまざまな利害関係者に配布される場合もある。必須文書又は原資料を不可逆的にコピーで置き換える場合、そのコピーを保証する必要がある (6.5 章を参照) 。

Copies should contain a faithful representation of the data and the contextual information. Source documents and data should allow accurate copies to be made. The method of copying should be practical and should ensure that the resulting copy is complete and accurate. It should include the relevant metadata and such metadata should be complete and accurate. See also section 5 of the 'Guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic)' (EMA/INS/GCP/856758/2018), for further details on definition.	コピーには、データとコンテキスト情報の忠実な表現が含まれている必要がある。原資料と原データは、正確なコピーが作成できること。コピーの方法は現実的かつコピー結果が完全かつ正確であることを確実にするものであること。〔コピーは〕関連するメタデータを含むべきであり、そのようなメタデータは完全かつ正確である必要がある。定義のさらなる詳細については、「Guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic」(EMA/INS/GCP/856758/2018) の 5 章も参照のこと。

6.5. Certified copies (保証付きコピー)

When creating a certified copy, the nature of the original document needs to be considered. For example, the content of the file is either static (e.g. a PDF document) or dynamic (e.g. a worksheet with automatic calculations) or the copy tries to capture the result of an interpreter (e.g. a web page, where a web- browser interprets written hypertext mark-up language (HTML), JavaScript (JS) among other programming languages). Either way, the result of the copy process should be verified either automatically by a validated process or manually to ensure that the same information is present — including data that describe the context, content, and structure — as in the original.	保証付きコピーを作成する場合、オリジナル文書の性質を考慮すること。例えば、ファイルのコンテンツが静的 (例：PDF ドキュメント) なのか動的 (例：自動計算を含むワークシート) なのか、またインタープリタ〔が処理した〕結果 (例えば、Web ページは Web ブラウザが HTML、JavaScript (JS) などのプログラミング言語を解釈するものである) なのか。いずれにせよ、コピープロセスの結果は、バリデート済みのプロセスによって自動的に検証するか、手作業で検証することにより、オリジナルと同じ情報が存在する—コンテキスト、コンテンツ、及び構造を説明するデータを含む—ことを確実にすること。

In case of dynamic files e.g. when a database is decommissioned and copies of data and metadata are provided to sponsors, the resulting file should also capture the dynamic aspects of the original file. In case of files, which are the result of an interpreter, special care needs to be taken to not only consider the informative content of such a file, but also to capture and preserve aspects that are the result of the interactions of the used interpreter(s) and system settings during the display. For example, window size, browser type, operating system employed and the availability of software dependencies (e.g. enabled active web content) can influence the structure and content displayed. Special considerations should be taken whenever copies are to replace original source documents.	動的ファイルの場合、例えばデータベースが運転停止となり、データとメタデータのコピーが治験依頼者に提供されるとき、コピーされたファイルにはオリジナルファイルの動的な側面も写し取られていること。インタープリタの処理結果であるファイルの場合、ファイルのコンテンツ情報の部分を考慮するだけでなく、使用されたインタープリタと表示した時のシステム設定の相互作用の結果であるという側面も踏まえて保存するよう特別な注意を払う必要がある。例えば、ウィンドウサイズ、ブラウザの種類、使用されているOS、及び依存するソフトウェアの可用性(例：有効となっていたアクティブな Web コンテンツ) は、構造と表示されるコンテンツに影響を与える可能性がある。オリジナルの原資料をコピーで置き換える場合は常に特別な配慮が必要である。

6.6. Control of data (データのコントロール)

Data generated at the clinical trial site relating to the trial participants should be available to the investigator at all times during and after the trial to enable investigators to make decisions related to eligibility, treatment, care for the participants, etc. and to ensure that the investigator can fulfil their legal responsibility to retain an independent copy of the data for the required retention period. This includes data from external sources, such as central laboratory data, centrally read imaging data and ePRO data. Exceptions should be justified in the protocol e.g. if sharing this information with the investigator would jeopardise the blinding of the trial.	治験実施施設において生成された治験参加者に関するデータは、治験中及び治験後いつでも治験責任医師が利用できるようにし、治験責任医師が参加者の適格性、治療、ケアなどに関連する決定を下せるようにするとともに、治験責任医師が、データコピーを、必要な保存期間を通じて〔治験依頼者とは〕独立して保持するという法的責任を果たすことができるようにする必要がある。これには外部ソースからのデータ (中央検査室のデータ、中央で読み取られた画像データ、ePRO データなど) が含まれる。 例外は、治験実施計画書で正当化 (例えば、情報を治験責任医師と共有すると治験の盲検性が脅かされる) する必要がある。

The sponsor should not have exclusive control of the data entered in a computerised system at any point in time. All data held by the sponsor that has been generated in a clinical trial should be verifiable to a copy of these data that is not held (or that has not been held) by the sponsor.	治験依頼者は、いつの時点であっても、コンピュータ化システムに入力されたデータを独占的にコントロールするべきではない。治験依頼者が保有する、治験で生成されたすべてのデータは、治験依頼者の保有していない (又は保有してこなかった) コピーと照合できること。
The requirements above are not met if data are captured in a computerised system and the data are stored on a central server under the sole control of the sponsor or under the control of a service provider that is not considered to be independent from the sponsor or if the sponsor (instead of the service provider) is distributing the data to the investigator. This is because the investigator does not hold an independent copy of the data and therefore the sponsor has exclusive control of the data. In order to meet the requirements, the investigator should be able to download a contemporaneous certified copy of the data. This is in addition to the record maintained at a service provider.	データがコンピュータ化システムで収集され、治験依頼者の単独のコントロール下にある中央サーバーに保存されている場合、又はデータが治験依頼者から独立しているとは見なされないサービスプロバイダのコントロール下にある場合、又は治験責任医師に (サービスプロバイダではなく) 治験依頼者がデータを配布するような場合、上記の要件が満たされているとはいえない。というのは、治験責任医師が独立したデータコピーを保持しておらず、そのため治験依頼者がデータを独占的に管理していることになるためである。要件を満たすためには、治験責任医師が、同時性のある、データの認証付きコピーを、ダウンロードできる必要がある。これは、サービスプロバイダにより維持管理されている記録とは別である。
Instead of a system maintained by an independent service provider, the sponsor may take other adequate technical measures that preclude sole control. E.g. the verifiability of data (transactions) by an independent (distributed) tamper-proof ledger may provide comparable security to a system maintained by an independent service provider. This should be justified and documented.	独立したサービスプロバイダによってシステムを維持させる代わりに、治験依頼者は独占的なコントロールを排除するための適切な技術的手段を講じてもよい。例えば、独立した、改ざんから保護された (分散された) 台帳によってデータ (トランザクション) を検証できるようにすれば、独立したサービスプロバイダによって維持されるシステムと同等のセキュリティを得られるであろう。このことは正当化し、文書化すべきである。

Data entered to data acquisition tools by the investigator should be available to the investigator throughout the whole legally mandated duration and for the full duration of local legal requirements. This can be ensured either by contemporaneous local copies at the trial site or e.g. by the use of a service provider. Access to the data may be amended to read-only as part of the database lock process. Prior to read-only access to the investigator being revoked, a copy including the audit trail should be made available to the investigator in a complete and comprehensive way. In the situation where a service provider is hosting the data, the copy should not be provided via the sponsor, as this would temporarily provide the sponsor with exclusive control over the data and thereby jeopardise the investigator's control. Copies should not be provided in a way that requires advanced technical skills from the investigators. The period between the provision of the copy to the investigator and the closure of the investigators' read-only access to the database(s) should allow sufficient time for the investigator to review the copy and access should not be revoked until such a review has been performed.	治験責任医師がデータ収集ツールに入力したデータは、法的に義務付けられている全期間、及びローカルの法的要件の全期間を通して、治験責任医師が利用できるようにすること。これは、治験実施施設で、又は例えばサービスプロバイダを使用して、同時的にローカルコピーを取ることで確実にすることができる。データベースロックプロセスの一環で、データへのアクセスが読み取り専用に変更されることがある。治験責任医師の読み取り専用アクセス権を取り消す前に、治験責任医師に、監査証跡を含むコピーを、完全かつ包括的な方法で提供すること。サービスプロバイダがデータをホストしているのであれば、コピーは治験依頼者経由で提供しないようにすること。そうしないと一時的にデータの独占的コントロールを治験依頼者に与えることになり、治験責任医師によるコントロールが危うくなるからである。コピーは、治験責任医師に高度な技術的スキルを求めるような方法で提供すべきではない。治験責任医師へコピーを提供してから、治験責任医師のデータベースへの読み取り専用アクセスを取り消すまでの期間は、治験責任医師がコピーをレビューするのに十分な期間とし、そのようなレビューが終わるまではアクセスを取り消すべきではない。
Any contractual agreements regarding hosting should ensure investigator control. If the sponsor is arranging hosting on behalf of the investigators through a service provider, agreements should ensure the level of investigator control mentioned above.	ホスティングに関する契約上の合意において、治験責任医師が確実にコントロールを持つようにすること。治験責任医師の代わりに治験依頼者がサービスプロバイダ経由でホスティングを準備する場合、上記の治験責任医師のコントロールレベルを契約で確実にする必要がある。

Investigators delegating hosting of such data to service providers themselves should ensure that the intended use is covered by local legal requirements and the in-house rules of the institution.	治験責任医師がそのようなデータのホスティングをサービスプロバイダに委任する場合、意図した用途がローカルの法的要件及び自組織の社内規則によってカバーされていることを確実にすること。
For investigator-initiated trials, where the data are hosted somewhere in the sponsor/institution organisation, the degree of independence should be justified and pre-specified in agreements e.g. that it is a central IT department, not otherwise involved in the operational aspects of the trial, hosting the data and providing copies to the participating investigators.	医師主導の治験で、データが治験依頼者/治験実施医療機関のどこかの組織によりホストされている場合、独立性の程度を正当化し、契約で事前に明確にしておくこと。例えば、当該組織が中央の IT 部門であり、治験の運用面には関与せず、データをホストし、参加する治験責任医師にコピーを提供する、など。

6.7. Cloud solutions (クラウドソリューション)

Irrespective whether a computerised system is installed at the premises of the sponsor, investigator, another party involved in the trial or whether it is made available by a service provider as a cloud solution, the requirements in this guideline are applicable. There are, however, specific points to be considered as described below.	コンピュータ化システムが治験依頼者、治験責任医師、その他の治験関係者の敷地内に設置されている場合であっても、又はサービスプロバイダがクラウドソリューションとして提供している場合であっても、本ガイドラインの要件は適用可能である。ただし、以下に説明するように、特別に配慮すべき点がある。
Cloud solutions cover a wide variety of services related to the computerised systems used in clinical trials. These can range from Infrastructure as a Service (IaaS) over Platform as a Service (PaaS) to Software as a Service (SaaS). It is common for these services that they provide the responsible party on-demand availability of computerised system resources over the internet, without having the need or even the possibility to directly manage these services.	クラウドソリューションは、治験で使用されるコンピュータ化システムに関連するさまざまなサービスをカバーしている。これらの範囲は Infrastructure as a Service (IaaS)、Platform as a Service (PaaS)、Software as a Service (SaaS) に及ぶ。これらのサービスは一般的に、コンピュータ化システムのリソースがオンデマンドでインターネットを介して責任のある当事者に提供されるものであり、サービスを直接管理する必要も、可能性もない。

If a cloud solution is used, the responsible party should ensure that the service provider providing the cloud is qualified.	クラウドソリューションを使用する場合、責任のある当事者は、クラウドを提供するサービスプロバイダが適格であることを確実にする必要がある。
When using cloud computing, the responsible parties are at a certain risk, because many services are managed less visibly by the cloud provider.	多くのサービスはクラウドプロバイダにより、可視化が不十分な形で管理されるため、クラウドコンピューティングを使用する場合、責任のある当事者は一定のリスクを負うことになる。
Contractual obligations with the cloud solution provider should be detailed and explicit and refer to all ICH E6 relevant topics and to all relevant legal requirements (see Annex 1).	クラウドソリューションプロバイダの契約上の義務は、詳細かつ明示的に定め、すべての ICH E6 関連トピックとすべての関連法的要件を参照すること (付属書 1 参照) 。
Data jurisdiction may be complex given the nature of cloud solutions and services being shared over several sites, countries, and continents; however, any uncertainties should be addressed and solved by contractual obligations prior to the use of a cloud solution.	複数の治験実施施設／国／大陸にまたがって共有されるというクラウドソリューションとサービスの性質を考えると、データの管轄は複雑となり得るが、不確かなことがあれば、クラウドソリューション使用前に、契約上の義務として取り上げ、解決しておくこと。
If the responsible party choses to perform their own validation of the computerised system, the cloud provider should make a test environment available that is identical to the production environment.	責任のある当事者がコンピュータ化システムを独自にバリデートすることを選択した場合、クラウドプロバイダは、運用環境と同一のテスト環境を利用できるようにすること。

6.8. Backup of data (データのバックアップ)

Data stored in a computerised system are susceptible to system malfunction, intended or unintended attempts to alter or destroy data and physical destruction of media and infrastructure and are therefore at risk of loss. Data and configurations should be regularly backed up. Please also refer to Annex 4 for further details on IT security.	コンピュータ化システムに保存されているデータは、システムの誤動作、故意又は事故によるデータ変更又は破壊の試み、及びメディアやインフラストラクチャの物理的破壊に対して脆弱であり、したがって損失するリスクがある。データと構成設定は定期的にバックアップすべきである。IT セキュリティの詳細については付属書 4 も参照のこと。

The use of replicated servers is strongly recommended. Backups should be stored in separate physical locations and logical networks and not behind the same firewall as the original data to avoid simultaneous destruction or alteration.	レプリケーションサーバーの使用を強く勧める。バックアップは、オリジナルデータと同じファイアウォール内ではなく、別の物理的な場所及び論理ネットワークに保存し〔オリジナルデータと〕一緒に破壊されたり、変更されたりしないようにすること。
Frequency of backups (e.g. hourly, daily, weekly) and their retention (e.g. a day, a week, a month) should be determined through a risk-based approach.	バックアップの頻度 (例：毎時、毎日、毎週) とその保存期間 (例：1 日、1 週間、1 か月) は、リスクベースアプローチで決定すること。
Checks of accessibility to data, irrespective of format, including relevant metadata, should be undertaken to confirm that the data are enduring, continue to be available, readable and understandable by a human being. There should be procedures in place for risk-based (e.g. in connection with major updates) restore tests from the backup of the complete database(s) and configurations and the performed restore tests should be documented.	フォーマットに関係なく、データ (関連するメタデータを含む) にアクセスできるかどうかのチェックを実施して、データが永続的で、引き続き利用可能で、人間が読んで理解できることを確認する必要がある。データベースと構成設定をバックアップから完全に復元できることのテストを定めるリスクベース (例：メジャーアップデートに合わせて実施するなど) の手順を用意するとともに、実施した復元テストを記録すること。
Disaster mitigation and recovery plans should be in place to deal with events that endanger data security. Such plans should be regularly reviewed. Disaster mitigation and recovery plans should be part of the contractual agreement, if applicable.	データセキュリティを脅かすイベントに対処するために、災害の被害軽減と回復の計画を策定すること。そのような計画は定期的に見直すべきである。該当する場合は、災害の被害軽減と回復の計画を、契約上の合意に含めること。

6.9. Contingency plans (緊急時対応計画)

Agreements and procedures should be in place to allow trial continuation and prevent loss of data critical to participant safety and trial results.	契約と手順を設け、治験が継続でき、参加者の安全と治験結果にとって重要なデータの損失を防ぐようにすること。

6.10. Migration of data (データ移行)

Migration as opposed to the transfer of data (as described in section 6.1.2.) is the process of permanently moving existing data (including metadata) from one system into another system e.g. the migration of individual safety reports from one safety database to another. It should be ensured that the migration does not adversely affect existing data and metadata.	データ移行は、データ転送 (6.1.2 章で説明) と異なり、既存のデータ (メタデータを含む) をあるシステムから別のシステムに永久に移すプロセスである。例えば、ある安全性データベースから別の安全性データベースへの個々の安全性報告書の移行など。データ移行により既存のデータ／メタデータが悪影響を受けないようにすること。
In the course of the design or purchase of a new system and of subsequent data migration from an old system, validation of the data migration process should have no less focus than the validation of the system itself.	新しいシステムを設計又は購入し、その後に古いシステムからデータ移行する過程で、データ移行プロセスのバリデーションは、システム自体のバリデーションと同様に重要である。
The validation of data migration should take into consideration the complexity of the task and any foreseen possibilities that may exist to verify the migrated data (e.g. checksum, case counts, quality control of records).	データ移行のバリデーションでは、タスクの複雑さと、あらゆる起こり得ることを考慮に入れたうえで、移行データを検証 (例：チェックサム、ケース数、記録の品質管理) すべきである。
Prior to migration, the process should be planned in detail. A risk analysis identifying the most probable risks should take place and should yield appropriate mitigation strategies. After the planning, the intended procedure should be validated with mock data and results should be considered for risk- assessment and mitigation. A data verification focused on key data should be performed post migration.	データ移行の前に、プロセスを詳細に計画すること。最も起こりそうなリスクを特定するためのリスク分析を実施し、適切な低減戦略を導き出すこと。計画後、想定している手順を模擬データでバリデートし、その結果をリスクアセスメントとリスク低減に反映させること。データ移行後に、重要なデータに焦点を当てたデータ検証を実施すること。

Verification of migrated data can be simple or complex, depending on the different platforms and systems involved. Regardless of the effort needed, the migration process should be documented in such detail that throughout all data operations/transformations data changes remain traceable. Mapping from the old system onto the new system should be retained.	移行されたデータの検証は、プラットフォームやシステムの種類によって、単純にも複雑にもなる。必要となる作業に関係なく、移行プロセスは詳細に文書化すべきであり、それはすべてのデータ操作/変換を通じてどのようにデータが変更されたかを追跡できる程度に詳細なものとすること。旧システムから新システムへのマッピングは保管すること。
Data, contextual information, and the audit trail should not be separated. In case migration of data into a new system results in a loss of relevant data, adequate mitigating actions should be taken to establish a robust method to join the audit trail and the data for continuous access by all stakeholders. A detailed explanation is expected, if no such method has been established to allow the migration of data and the audit trail. Arrangements should ensure that the link between data and metadata can be established. If several parties are involved, agreements should be in place to ensure this.	データ、コンテキスト情報、及び監査証跡は分離しないこと。データを新システムに移行したことで関連するデータが失われた場合は、適切な是正措置を行い、すべての利害関係者が継続的にアクセスできるように監査証跡とデータを結合させる堅牢な方法を確立すること。データと監査証跡を〔まとめて〕移行する方法が確立されていない場合は、詳細な説明を行うことが期待される。手はずを整え、データとメタデータ間のリンクを確実に確立できるようにすること。複数の当事者が関与する場合は、このことを確実にするために予め合意しておく必要がある。

6.11. Archiving (アーカイビング)

The investigator and sponsor should be aware of the required retention periods for clinical trial data and essential documents, including metadata. Retention periods should respect the data protection principle of storage limitation. An inventory of all essential data and documents and corresponding retention periods should be maintained. It should be clearly defined which data are related to each clinical trial activity and where this record is located and who has access/edit rights to the document. Security controls should be in place to ensure data confidentiality, integrity, and availability.	治験責任医師と治験依頼者は、治験データ及び必須文書 (メタデータを含む) について要求される保存期間を認識しておく必要がある。データの保存期間は、データ保護原則における保存期間の制限【訳注】を尊重すべきである。すべての必須データと必須文書、及びそれらに対応する保存期間を記載する台帳を維持管理すること。どのデータがどの治験活動に関連し、その記録がどこにあるか、誰が文書へのアクセス/編集権限を持っているかを明確に定義すること。セキュリティコントロールを設け、データの機密性、インテグリティ、及び可用性を確保すること。 【訳注】個人データは、データ主体が識別・特定できる形では、処理目的達成に必要な期間を超えて保存してはならない。GDPR Art. 5 1. (e)
It should be ensured that the file and any software required (depending on the media used for storage) remain accessible, throughout the retention period. This could imply e.g. migration of data (see section 6.9.).	ファイル、及び (格納に使われるメディア次第ではあるが) 必要となるソフトウェアは、保存期間全体を通じてアクセス可能な状態を維持すること。このために例えばデータ移行 (6.9 章参照) が必要となるかもしれない。
Suitable archiving systems should be in place to safeguard data integrity for the periods established by the regulatory requirements including those in any of the regions where the data may be used for regulatory submissions, and not just those of the country where the data are generated.	規制要件によって定められた期間 (データが生成された国だけでなく、データを規制目的で提出する可能性のある地域で定められた期間) でデータインテグリティを保護するために、適切なアーカイブシステムを導入する必要がある。
Source documents and data should always be available when needed to authorised individuals to meet their regulatory obligations. Please refer to section 4.11 direct access.	原資料と原データを、権限のある個人が必要なときにいつでも利用できるようにし、規制上の義務を果たせるようにしておく必要がある。4.11 章「直接アクセス」を参照のこと。

Data should be maintained in a secure manner and should only be transferred between different (physical) locations in a validated process. Data should be archived in a read-only state.	データは安全な方法で維持管理する必要があり、異なる (物理的) 場所間の転送はバリデート済みのプロセスによってのみ行うこと。データは読み取り専用状態でアーカイブすること。

6.12. Database decommissioning (*データベースの運転停止*)

After the finalisation of the trial, database(s) might be decommissioned. It is recommended that the time of decommissioning is decided taking into consideration e.g. whether the clinical trial will be used for a marketing authorisation application in the near future in which case it is recommended to keep the database(s) live. Please refer to figure 2 for a proposed approach. A dated and certified copy of the database(s) and data should be archived and available on request. In case of decommissioning, the sponsor should ensure (contractually if done by a service provider) that archived formats provide the possibility to restore the database(s). This includes the restoration of dynamic functionality and all relevant metadata (audit trail, event logs, implemented edit checks, queries, user logs, etc.). Where recommissioning is no longer possible, the sponsor should ensure that all the data including metadata files (e.g. audit trails) are available in dynamic data files. The sponsor should review the system to determine the audit trails and logs available in the system and how these would be retained as dynamic files. Where a service provider is involved, this should be addressed in the contractual arrangements. Static formats of dynamic data will not be considered adequate. See definitions section on static and dynamic formats.	治験終了後、データベースは運転停止するかもしれない。運転停止の時期は、例えば近い将来治験が販売承認申請に使用されるかどうかを考慮して決定することを勧める。その場合、データベースは活かしたままにしておく方がよい。提案されているアプローチについては figure 2 を参照のこと。データベースとデータの日付入りの保証付きコピーをアーカイブし、要求に応じて利用できるようにすること。運転停止する場合、治験依頼者は、アーカイブのフォーマットからデータベースが復元できることを (サービスプロバイダによって行われる場合は契約によって) 確実にすること。ここで復元とは、動的機能とすべての関連メタデータ (監査証跡、イベントログ、実装された編集チェック、クエリ、ユーザー ログなど) を含む。〔データベースの〕運転再開が不可能な場合、治験依頼者は、メタデータファイル (例：監査証跡) を含むすべてのデータが動的データファイルとして確実に利用できるようにすること。治験依頼者は、システムをレビューし、システムで入手できる監査証跡とログを特定し、これらを動的ファイルとして保存する方法を決定すること。サービスプロバイダが関与する場合、これは契約上の取り決めにより対応すべきである。動的データを、静的フォーマット〔で保存すること〕は適切とは見なされない。静的フォーマット及び動的フォーマットを定義した章を参照のこと。

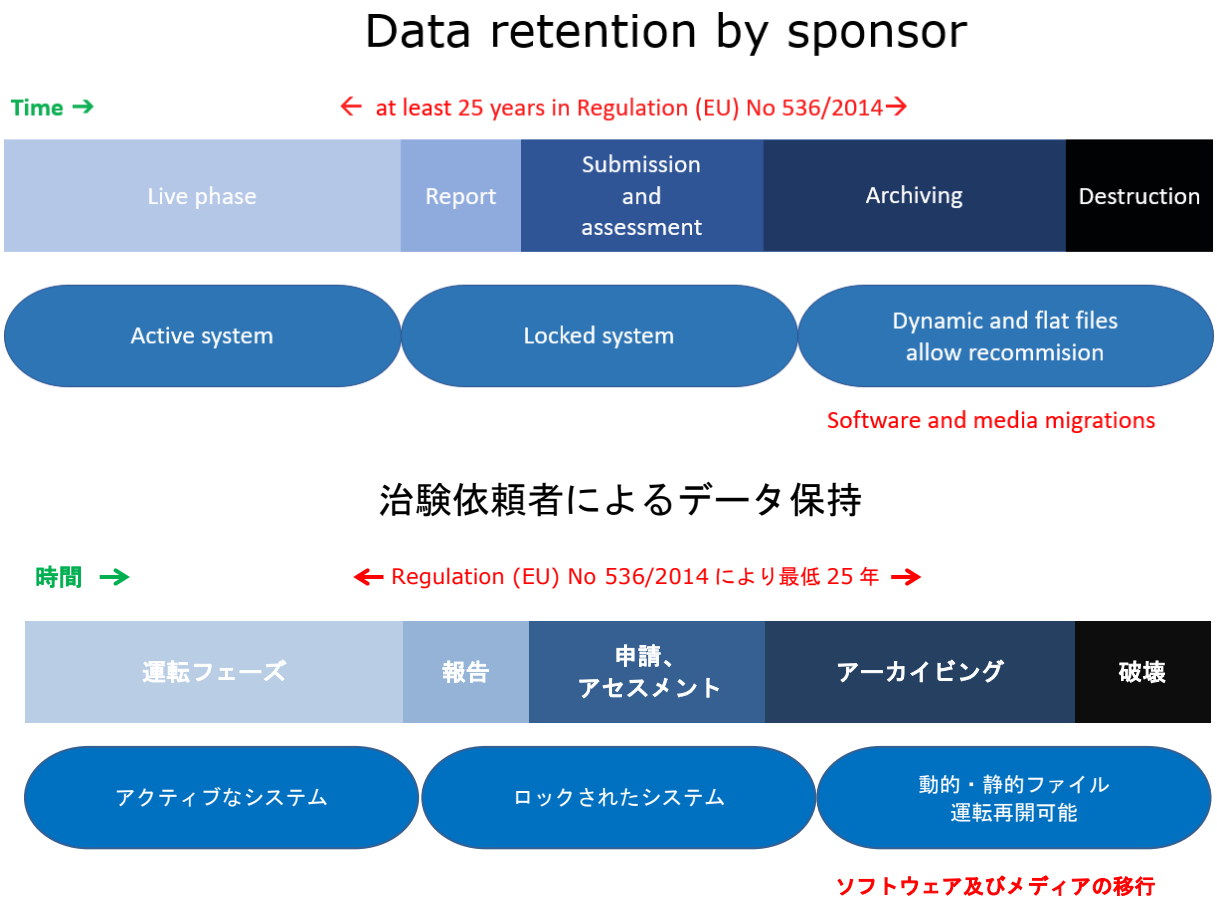

Data retention by sponsor
Time →
← at least 25 years in Regulation (EU) No 536/2014→
Live phase
Report
Submission and assessment
Archiving
Destruction
Active system
Locked system
Dynamic and flat files allow recommision
Software and media migrations
治験依頼者によるデータ保持
時間 →
← Regulation (EU) No 536/2014 により最低 25 年 →
運転フェーズ
報告
申請、アセスメント
アーカイビング
破壊
アクティブなシステム
ロックされたシステム
動的・静的ファイル 運転再開可能
ソフトウェア及びメディアの移行

Figure 2

Annex 1 Agreements (付属書 1 合意)

The legally responsible parties are the sponsors and investigators. They contract/delegate an increasing number of tasks in clinical trials, contracting is frequent in the area of computerised systems where the responsible party might lack internal knowledge or resources or they wish to purchase a product or a service that has been developed by others. The responsible parties can delegate tasks to a service provider, but nevertheless the full responsibility for the data integrity, security and confidentiality resides with them.	法的に責任のある当事者は、治験依頼者と治験責任医師である。彼らはますます多くの治験タスクを〔他者に〕契約/委任するようになっている。責任のある当時者の内部に知識やリソースが不足しているコンピュータ化システムの分野では〔他者と〕契約する頻度が高い。または他者によって開発された製品又はサービスを購入したいと考えている。責任のある当事者はサービスプロバイダにタスクを委任することはできるが、データのインテグリティ、セキュリティ、及び機密性に対する全責任は彼らにある。
Agreements can cover a variety of tasks such as system and trial specific configuration and customisation, provision of a license to an application, full clinical trial service including data management tasks e.g. site contact, training, data clarification processes, etc., but could also be restricted to hosting services. A risk-based approach can be used in relation to agreements as well as for computerised systems in general. It is recognised that a trial specific agreement is not required, if a product is purchased and used as intended without the involvement of the manufacturer of the system; however, such use will require a risk assessment by the responsible party to assess whether such a non-trial specific system is fit for its intended use.	契約ではさまざまなタスク、例えばシステム及び治験固有の構成設定とカスタマイズ、アプリケーションのライセンスの提供、データ管理タスクを含む治験全般にわたるサービス(例：治験実施施設との連絡窓口、トレーニング、データクラリフィケーションプロセス)をカバーすることができるが、契約をホスティングサービスに限定することもできる。リスクベースアプローチは、一般的にコンピュータ化システムだけでなく、契約にも用いることができる。製造元の関与なしに、製品を購入し、意図通りに使用するのであれば、治験独自の契約は必要ないと考えられる。しかし、そのような場合、責任のある当事者は、そういった、治験に特化していないシステムが、意図した用途に適しているかリスクアセスメントする必要がある。

The responsible party should ensure that the distribution of tasks in a trial is clearly documented and agreed on. It should be ensured that each party has the control of and access to data and information that their legal responsibilities require and that the ethics committees and regulatory authorities approving trials have been properly informed of distribution of activities as part of the clinical trial application process, where applicable. This should be carefully documented in the protocol and related documents, procedures, agreements, and other documents as relevant. It is important to consider who is providing and controlling the computerised system being used.	責任のある当事者は、治験のタスクの分担が明確に文書化され、合意されていることを確実にする必要がある。各当事者が、それぞれの法的責任で要求されるデータと情報をコントロールでき、かつアクセスできることを確実にする必要がある。また該当する場合、治験申請プロセスの一環として、治験を承認する倫理委員会と規制当局に対して、タスクの分担について適切に通知されるようにすべきである。このことは、治験実施計画書及び関連文書、手順書、契約書、及び関連するその他の文書に注意深く文書化する必要がある。重要なことは、使用しているコンピュータ化システムを誰が提供し、コントロールしているのかを考慮することである。
Clear written agreements should be in place and appropriately signed by all involved parties prior to the provision of services or systems. Agreements should be maintained/updated as appropriate. Sub-contracting and conditions for sub-contracting and the responsible party's oversight of sub-contracted activities should be specified.	サービス又はシステムの提供を受ける前に、明確な書面による契約を作成し、すべての関係者に適切に署名させること。契約は適切に維持/更新すべきである。下請けの有無、下請け〔を使う場合〕の条件、及び下請けの活動への責任のある当事者による監督を〔契約書に〕明記する必要がある。
The responsible parties should ensure oversight of these trial-related duties e.g. by reviewing defined key performance indicators (KPIs) or reconciliations.	責任のある当事者は、こういった治験関連の義務が確実に監督 (例えば、定義された key performance indicators (KPI) や〔問題を〕どう修復したかのレビュー) されるようにすべきである。

If appropriate agreements cannot be put in place due to the inability or reluctance of a service provider to allow access to important documentation (e.g. system requirements specifications) or the service provider is unwilling to support pre-qualification audits or regulatory inspections, systems from such a service provider should not be used in clinical trials.	サービスプロバイダが重要な文書 (例：システム要求仕様) へのアクセスを提供できない、又は提供を渋るために適切な契約を締結できない場合、又はサービスプロバイダが事前監査や規制査察を支援することに前向きでない場合、そのようなサービスプロバイダのシステムは治験に使用すべきではない。
The responsible party should ensure that service providers (including vendors of computerised systems) have the knowledge and the processes to ensure that they can perform their tasks in accordance with ICH E6, as appropriate to their tasks. Standards to be followed, e.g. clinical trial legislation and guidance should be specified in the agreement, where relevant. A number of tasks involve accessing, reviewing, collecting and/or analysing data, much of which is personal/pseudonymised data. In addition, in specific cases involving contact with (potential) trial participants, data protection legislation needs to be followed, in addition to the clinical trial legislation and guidance.	責任のある当事者は、サービスプロバイダ (コンピュータ化システムのベンダーを含む) が、各自のタスクに応じて、ICH E6 に従ってタスクを遂行するための知識とプロセスを持つことを確実にすべきである。必要に応じて、従うべき基準 (例：治験に関する法律やガイダンス) を契約書に明記する。多くのタスクには、データへのアクセス、データレビュー、データ収集、及び (又は) データ分析が含まれるが、そういったデータの多くは個人/匿名化されたデータである。さらに、(潜在的な) 治験参加者と接触するような特定のケースでは、治験の法律やガイダンスに加えて、データ保護法に従う必要がある。
The approved protocol, implicitly, defines part of the specification for system configuration or customisation (e.g. for interactive response technologies (IRT) systems and data acquisition tools) and there should be consistency between the protocol and the wording of the agreement. In addition, it should be clear how subsequent changes to the protocol are handled so that the vendor can implement changes to the computerised system, where relevant.	システム (例：IRT システム及びデータ収集ツール) の構成設定又はカスタマイズについての仕様の一部は、承認された治験実施計画書によって暗黙的に決定される。治験実施計画書と契約の文言には一貫性が必要である。さらに、後で治験実施計画書が変更されたときにどのように処理するかを明確にしておき、必要時にベンダーがコンピュータ化システムに変更を実装できるようにしておく必要がある。

It should be clear from agreements which tasks are delegated also in relation to retaining essential documentation for performed activities. In the context of clinical trials, system-documentation (including e.g. software/system validation documentation, vendor standard operating procedures (SOPs), training records, issues log/resolutions) as well as trial master file (TMF) documentation (e.g. emails on important decisions and meeting minutes) related to the individual clinical trial (including e.g. relevant helpdesk tickets or meeting minutes) should be retained for the full retention period. It should be clear from the agreement which party is retaining and maintaining which documentation and how and in what format that documentation is made available when needed e.g. for an audit or an inspection. There should be no difference in the availability of documentation irrespective of whether the documentation is held by the sponsor/investigator or a service provider or sub-contracted party.	実施した活動に関する必須文書の保存に関連して、どのタスクが委任されているのかについても契約で明確にしておく必要がある。治験のコンテキストでは、システム文書 (例えば、ソフトウェア/システムバリデーション文書、ベンダーの標準操作手順書 (SOP)、トレーニング記録、イシューログ/処置などを含む) 及び治験マスターファイル (TMF) 文書 (例：重要な決定に関する電子メールや議事録) で個々の治験に関連するもの (関連するヘルプデスクチケット又は会議議事録などを含む) は、保存期間全体にわたって保持する必要がある。どの当事者が、どの文書を保持し、維持管理するか、また必要なとき (例えば監査又は査察時) にその文書をどのように、どのようなフォーマットで利用できるようにするかを、契約で明確にしておく必要がある。文書を保持するのが、治験依頼者/治験責任医師、サービスプロバイダ、下請け業者のいずれであっても、文書の可用性に差異があってはならない。
The responsible party is ultimately responsible for e.g. the validation and operation of the computerised system and for providing adequate documented evidence of applicable processes.	責任のある当事者は、例えばコンピュータ化システムのバリデーションと運用を行うこと、及び関連するプロセスについての適切な文書化された証拠を提供することに最終的な責任を負う。
The responsible party should be able to provide the GCP inspectors of the EU/EEA authorities with access to the requested documentation regarding the validation and operation of computerised systems irrespective of who performed these activities.	これらの活動を誰が行ったかに関係なく、責任のある当事者は、EU/EEA 当局の GCP 査察官の要求するコンピュータ化システムのバリデーションや運用に関する文書一式へのアクセスを〔査察官〕に提供できるようにすること。

It should be specified in agreements that the sponsor or the institution, as applicable, should have the right to conduct audits at the vendor site and that the vendor site could be subject to inspections (by national and/or international authorities) and that the vendor site shall accept these. The responsible party should also ensure that their service providers act on/respond appropriately to findings from audits and inspections.	治験依頼者又は実施医療機関のどちらか該当する方が、ベンダーサイトに監査を行う権利を持つことを契約に明記すること。さらにベンダーサイトが (国内、及び (又は) 国際当局による) 査察の対象となる可能性があること、及びベンダーサイトはこれらを受け入れることを契約に盛り込むべきである。また、責任のある当事者は、サービスプロバイダが監査や査察の結果に適切に対処/応答することを確実にすること。
The sponsor has a legal responsibility under Regulation (EU) No 536/2014 to report serious breaches, including important data and security breaches, to authorities within seven days. To avoid undue delay in sponsor reporting from the time of discovery e.g. by a vendor, agreements and related documents should specify which information should be escalated immediately to ensure regulatory compliance.	治験依頼者は、Regulation (EU) No 536/2014 に基づき (データやセキュリティの重要な違反を含む) 深刻な違反を 7 日以内に当局に報告する法的責任を負う。例えばベンダー発見後に、治験依頼者の報告が過度に遅れることのないように、どういった情報を直ちにエスカレーションする必要があるのかを契約及び関連文書で定めておき、確実に規制遵守する必要がある。

As set out in ICH E6, to ensure that the investigator, rather than the sponsor, maintains control over their data, it should be specified in agreements how investigators' access to and control over data are ensured during and after the trial, and the revocation of investigator access to data in case of decommissioning should be described. It should also be specified which outputs the involved parties (e.g. sponsor and investigators) will receive during and after the clinical trial and in what formats. Types of output could include e.g. data collected via data acquisition tools including metadata, queries, history and status of changes to users and their access rights, and the description of format for delivery of the complete database to sponsors.	ICH E6 に規定されているとおりに、治験依頼者ではなく治験責任医師がデータのコントロールを維持することを確実にするために、治験中及び治験後に治験責任医師がデータを確実にアクセス及びコントロールさせるための方法、及び運転停止の場合の治験責任医師のデータアクセス〔権限〕の取り消しについて契約に記載する必要がある。また治験中及び治験後に関係者 (例：治験依頼者や治験責任医師) が受け取るアウトプットとそのフォーマットも明記すべきである。アウトプットの種類には、例えばデータ収集ツールを介して収集したデータ (メタデータを含む)、クエリ、ユーザーとユーザーのアクセス権の変更履歴／状態、完全なデータベースを治験依頼者に提供する際のフォーマットの説明などが含まれる。
Arrangements on the decommissioning of the database(s) should be clear, including the possibility to restore the database(s), for instance, for inspection purposes.	データベースの運転停止に関する取り決め 、例えば査察対応のためにデータベースを復元する可能性、を明確にする必要がある。
The agreements should address expectations regarding potential system 'down-time' and the preparation of contingency plans.	契約には、潜在的なシステム「ダウンタイム」と緊急時対応計画の準備に関する期待事項についても盛り込む必要がある。
Tasks transferred/delegated could include hosting of data. If data are hosted by a vendor, location of data storage and control (e.g. use of cloud services) should be described.	移転/委任されるタスクに、データのホスティングが含まれる場合がある。データがベンダーによってホストされる場合、データの保管場所とコントロール (例：クラウドサービスの使用) を記載する必要がある。

Agreements should ensure reliable, continued and timely access to the data in case of bankruptcy, shutdown, disaster of the vendor, discontinuation of service by the vendor or for reasons chosen by the sponsor/investigator (e.g. change of vendor).	ベンダーの破産／閉鎖／災害、ベンダーによるサービス停止、又は治験依頼者/治験責任医師側の都合 (例：ベンダーの変更) によるサービス停止などの事態にあっても、契約により、信頼でき、継続的かつタイムリーなデータへのアクセスを確実にすること。
Special consideration should be given on training and quality systems. Vendors accepting tasks on computerised systems should not only be knowledgeable about computerised systems and data protection legislation, but also on GCP requirements, quality systems, etc. as appropriate to the tasks they perform.	トレーニング及び品質システムに特別に配慮すること。コンピュータ化システムに関するタスクを受託するベンダーは、コンピュータ化システムとデータ保護法はもちろんであるが、実行するタスクに応じて GCP 要件、品質システムなどについても精通している必要がある。
This guideline should be read together with the notice to sponsors regarding computerised systems (EMA/INS/GCP/467532/2019) published on the EMA website.	本ガイドラインは、EMA Web サイトで公開されているコンピュータ化システムに関する治験依頼者への通知 (EMA/INS/GCP/467532/2019) と合わせて読むこと。

Annex 2 Computerised systems validation (付属書 2 コンピュータ化システムバリデーション)

A2.1 General principles (一般原則)

The responsible party should ensure that systems used in clinical trials have been appropriately validated and demonstrated to meet the requirements defined in ICH E6 and in this guideline.	責任のある当事者は、治験で使用されるシステムが適切にバリデートされ、ICH E6 及び本ガイドラインで定義された要件を確実に満たすようにすること。
Systems should be validated independently of whether they are developed on request by the responsible party, are commercially or freely available, or are provided as a service.	責任のある当事者の要求に応じて開発されたかどうか、有料なのか無償なのか、又はサービスとして提供されているかどうか、に関係なく、システムはバリデートする必要がある。

The responsible party may rely on validation documentation provided by the vendor of a system if they have assessed the validation activities performed by the vendor and the associated documentation as adequate; however, they may also have to perform additional validation activities based on a documented assessment. In any case, the responsible party remains ultimately responsible for the validation of the computerised systems used in clinical trials.	責任のある当事者は、ベンダーが実行したバリデーション活動と関連文書をアセスメントし、適切であると判断した場合、システムベンダーの提供するバリデーション文書を活用できる。ただし、文書化されたアセスメント結果によっては追加のバリデーション活動を実行しなければならない場合もある。いずれにせよ、責任のある当事者は、治験で使用されるコンピュータ化システムのバリデーションに対して最終的な責任を負う。
If the responsible party wants to use the vendor's validation documentation, the responsible party should ensure that it covers the responsible party's intended use as well as its defined needs and requirements. The responsible party should be thoroughly familiar with the vendor's quality system and validation activities, which can usually be obtained through an in-depth systematic examination (e.g. an audit). This examination should be performed by qualified staff with sufficient time spent on the activities and with cooperation from the vendor. It should go sufficiently deep into the actual activities, and a suitable number of relevant key requirements and corresponding test cases should be reviewed, and this review should be documented. The examination report should document that the vendor's validation process and documentation is satisfactory. Any shortcomings should be mitigated by the responsible party, e.g. by requesting or performing additional validation activities.	責任のある当事者がベンダーのバリデーション文書を利用することを希望する場合、責任のある当事者は、〔ベンダーのバリデーション文書が〕責任のある当事者の意図した用途だけでなく、〔ベンダーにより〕定義されたニーズ及び要件をカバーしていることを確実にすること。責任のある当事者は、ベンダーの品質システムとバリデーション活動に精通している必要がある。これは通常、綿密かつ体系的な調査 (例：監査) を通じて実現できる。この調査は、十分な時間をかけて、ベンダーの協力を得たうえで、適格なスタッフが実施すること。〔ベンダーの〕実際の活動を十分深く掘り下げ、適切な数の重要な要件を取り上げ、それらの要件に対応するテストケースをレビューし、そのレビュー結果を記録する必要がある。調査報告書では、ベンダーのバリデーションプロセスと文書化が満足できる旨を記載すること。あらゆる〔発見された〕欠点は、例えば追加のバリデーション活動を要求するか、又は〔自ら〕実施するなどにより、責任のある当事者が低減する。

Some service providers may release new or updated versions of a system at short notice, leaving insufficient time for the responsible party to validate it or to review any validation documentation supplied by the service provider. In such a situation, it is particularly important for the responsible party to evaluate the vendor's process for validation prior to release for production, and to strengthen their own periodic review and change control processes. New functionalities should not be used by the responsible party until they have validated them or reviewed and assessed the vendor's documentation.	一部のサービスプロバイダは、システムの新しいバージョン又はアップデートバージョンを、通知をしてすぐにリリースする。その場合、責任のある当事者は、バリデートしたり、サービスプロバイダの提供するバリデーション文書を確認したりする時間を十分に取ることができない。このような状況では、運用へリリースする前に、ベンダーのバリデーションプロセスを評価するとともに、責任のある当事者の定期レビューや変更管理プロセスを強化することが特に重要である。新しい機能をバリデートするか、ベンダーの文書をレビューしてアセスメントするまでは、責任のある当事者は新しい機能を使用すべきではない。
If the responsible party relies on the vendor's validation documentation, inspectors should be given access to the full documentation and reporting of the responsible party's examination of the vendor. If this examination is documented in an audit report, this may require providing access to the report. The responsible party, or where applicable, the service provider performing the examination activities on their behalf, should have a detailed understanding of the validation documentation.	責任のある当事者がベンダーのバリデーション文書を頼りにするのであれば、査察官に、完全な文書一式、及び責任のある当事者によるベンダー精査の報告にアクセスできるようにすること。この〔ベンダー〕精査結果が監査報告書に記載されている場合、報告書へアクセスさせる必要があるかもしれない。責任のある当事者、又は該当する場合は、代わりに精査を実施したサービスプロバイダは、バリデーション文書を詳細に理解している必要がある。

As described in Annex 1 on agreements, the validation documentation should be made available to the inspectors in a timely manner, irrespective of whether it is provided by the responsible party or the vendor of the system. Contractual arrangements should be made to ensure continued access to this documentation for the legally defined retention period even if the sponsor discontinues the use of the system or if the vendor discontinues to support the system or ceases its activities.	契約についての付属書 1 に記載されているように、責任のある当事者、又はシステムベンダーのどちらでもよいが、バリデーション文書をタイムリーに査察官に提供する必要がある。たとえ治験依頼者がシステムの使用を中止したり、ベンダーがシステムのサポートを中止したり事業活動を終えたとしても、法的に定義された保存期間中はバリデーション文書に継続してアクセスできるよう契約で取り決めておく必要がある。
In case the vendor's validation activities and documentation are insufficient, or if the responsible party cannot rely on the vendor to provide documentation, the responsible party should validate the system.	ベンダーのバリデーション活動とバリデーション文書が不十分な場合、又は責任のある当事者がベンダーからの文書一式の提供を期待できない場合、責任のある当事者がシステムをバリデートすべきである。
Any difference between the test and the production configuration and environment should be documented and its significance assessed and justified.	テスト時と本番で構成設定及び環境に違いがあればそれを文書化し、その〔違いの〕重要性をアセスメントし、正当化すること。
Interfaces between systems should be clearly defined and validated e.g. transfer of data from one system to another.	(例えば、あるシステムから別のシステムへのデータ転送のような) システム間のインターフェースを明確に定義し、バリデートすること。

A2.2 User requirements (ユーザー要件)

Critical system functionality implemented and used in a clinical trial should be described in a set of user requirements or use cases, e.g. in a user requirements specification (URS). This includes all functionalities, which ensure trial conduct in compliance with ICH E6 and which include capturing, analysing, reporting and archiving clinical trial data in a manner that ensures data integrity. User requirements should include, but may not be limited to operational, functional, data integrity, technical, interface, performance, availability, security, and regulatory requirements. The above applies independently of the sourcing strategy of the responsible party or the process used to develop the system.	治験で実装され、使用される重要なシステム機能は、一連のユーザー要件又はユースケースとして (例えば、ユーザー要件仕様 (URS) に) 記述する必要がある。これらには ICH E6 に準拠した治験の実施を確実にし、データインテグリティを確実に確保するような方法で治験データを収集、分析、報告、アーカイブするすべての機能を含める。ユーザー要件には、運用要件、機能要件、データインテグリティ要件、技術要件、インターフェース要件、性能要件、可用性要件、セキュリティ要件、及び規制要件を含むべきであるが、これらに限定されるものではない。上記は、責任のある当事者の調達戦略やシステム開発に用いられるプロセスに関係なく適用される。
Where relevant, user requirements should form the basis for system design, purchase, configuration, and customisation; but in any case, they should constitute the basis for system validation.	ユーザー要件は、それが当てはまる場合は、システムを設計、購入、構成設定、及びカスタマイズする際のベースとなり、またどのような場合であれシステムバリデーションのベースとなる。
The responsible party should adopt and take full ownership of the user requirements, whether they are documented by the responsible party, by a vendor or by a service provider. The responsible party should review and approve the user requirements in order to verify that they describe the functionalities needed by users in their particular clinical trials.	責任のある当事者、ベンダー、サービスプロバイダのいずれがユーザー要件を文書化したにせよ、責任のある当事者は、ユーザー要件を採用し、その完全なオーナーシップを持つべきである。責任のある当事者は、特定の治験でユーザーの必要とする機能が記述されていることを検証するために、ユーザー要件をレビューして承認する必要がある。
User requirements should be maintained and updated as applicable throughout a system's lifecycle when system functionalities are changed.	システムのライフサイクル全体にわたって、システムの機能が変更されたときは、ユーザー要件を適切に維持／更新する必要がある。

A2.3 Trial specific configuration and customization (治験固有の構成設定及びカスタマイズ)

The configuration and customisation of a system for use in a specific trial should be pre-specified, documented in detail and verified as consistent with the protocol, with the data management plan and other related documents. Trial specific configuration and customisation should be quality controlled and tested as applicable before release for production. It is recommended to involve users in the testing activities. The same process applies to modifications required by protocol amendments.	特定の治験で使用するためのシステムの構成設定及びカスタマイズは、事前に仕様を決め、詳細に文書化し、治験実施計画書、データ管理計画、その他の関連文書との一貫性を検証する必要がある。治験固有の構成設定及びカスタマイズは、運用へリリースする前に、品質管理を行い、必要に応じてテストすること。ユーザーをテスト活動に参加させることを勧める。治験実施計画書の修正によって必要となる〔システム〕変更にも同じプロセスが適用される。
If modifications to a system are introduced due to a protocol amendment, e.g. to collect additional information, it should be determined whether they should be applied to all trial participants or only to those concerned by the amendment.	治験実施計画書の修正 (例えば追加情報の収集など) によりシステムを変更する場合、変更を治験参加者全員に適用するか、〔治験実施計画書の〕修正部分に関係する参加者のみに適用するか決定すること。
If new functionalities or interfaces need to be developed, or new code added, they should be validated before use.	新しい機能やインターフェースの開発、又は新しいコードの追加が必要な場合は、それらを使用する前にバリデートすること。

A2.4 Traceability of requirements (要件のトレーサビリティ)

Traceability should be established and maintained between each user requirement and test cases or other documents or activities, such as standard operating procedures, as applicable. This traceability may have many forms and the process may be automated by software. It should be continuously updated as requirements are changed to ensure that where applicable, for every requirement, there is a corresponding test case or action, in line with the risk evaluation.	トレーサビリティは、各ユーザー要件と、テストケースや他の文書／活動 (標準操作手順など) との間で確立し、維持する必要がある。このトレーサビリティには多くの形式があり、〔トレーサビリティの〕プロセスがソフトウェアにより自動化されている場合がある。要件が変更されたら〔トレーサビリティを〕継続的に更新し、該当する場合は、すべての要件について、リスク評価に沿って、テストケースやアクションが対応していることを確実にする必要がある。

A2.5 Validation and test plans (バリデーションとテスト計画)

Validation activities should be planned, documented, and approved. The validation plan should include information on the validation methodology, the risk-based approach taken and if applicable, the division of tasks between the responsible party and a service provider. Prior to testing, the risk assessment should define which requirements and tests are related to critical system functionality.	バリデーション活動は、計画し、文書化し、承認すべきである。バリデーション計画には、バリデーション方法、採用したリスクベースアプローチ、及び該当する場合は責任のある当事者とサービスプロバイダ間のタスクの分担に関する情報を含めること。テストの前に、リスクアセスメントにより、重要なシステム機能に関連する要件とテストはどれなのかを特定する必要がある。
Test cases should be pre-approved. They may have many formats and while historically consisting of textual documents including tables with multiple columns corresponding to the elements below, they may also be designed and contained in dedicated test management systems, which may even allow automatic execution of test cases (e.g. regression testing). However, expectations to key elements are the same.	テストケースは事前に承認すること。テストケースにはいろいろなフォーマットがある。従来は、以下に示す要素に対応する複数の列を持つテーブルを含むテキスト文書で構成されていた。〔これらの要素が〕専用のテスト管理システムで設計され、含まれている場合もあり、テストケースの自動実行 (例：機能退行テスト) さえ可能な場合がある。ただし、〔テストケースの〕主要な要素への期待は同じである。
Test cases should include: • the version of the software being tested; • any pre-requisites or conditions prior to conducting the test; • a description of the steps taken to test the functionality (input); • the expected result (acceptance criteria).	テストケースには以下を含めること。 • テスト対象のソフトウェアのバージョン。 • テスト実施前に満たすべき前提や条件。 • 機能をテストするための手順の説明 (入力) 。 • 期待される結果 (受け入れ基準) 。

Test cases should require the tester to document the actual result as seen in the test step, the evidence if relevant and, if applicable, the conclusion of the test step (pass/fail). Where possible, the tester should not be the author of the test case. In case of test failure, the potential impact should be assessed and subsequent decisions regarding the deviations should be documented.	テストケースでは、テスト担当者に、テストステップで見た実際の結果、該当する場合は証拠、必要に応じてテストステップの結論 (合格/不合格) を記録することを求める。可能であれば、テスト担当者はテストケースの作成者とは別の者とすること。テストが不合格となった場合、潜在的影響をアセスメントし、逸脱に関する決定を記録すること。

A2.6 Test execution and reporting (テスト実行と報告)

Test execution should follow approved protocols and test cases (see section A2.5), the version of the software being tested should be documented, and where applicable and required by test cases and test procedures, evidence (e.g. screen shots) should be captured to document test steps and results. Where relevant, the access rights (role) and the identification of the person or automatic testing tool performing tests should be documented. Where previously passed scripts are not retested along with the testing of fixes for previous failing tests, this should be risk assessed and the rationale should be documented.	テストの実行は、承認された計画書とテストケース (A2.5 章を参照) に従うこと。テスト対象となるソフトウェアのバージョンを記録する。また該当する場合で、かつテストケースやテストスクリプトで要求されている場合、テストステップと実行結果を文書化するために、証拠 (例：スクリーンショット) を収集する。必要に応じて、アクセス権 (役割) と、テスト実施者又は自動テストツールの ID を記録すること。 不合格に対する修正をテストする際に、もともと合格していたスクリプトの再テストを省略する場合は、リスクアセスメントを行い、その根拠を文書化すること。

Deviations encountered during system validation should be recorded and brought to closure. Any failure to meet requirements pre-defined to be critical should be solved or mitigating actions should be implemented prior to deployment. All open deviations and any known issues with the system at the time of release should be assessed and subsequent decisions should be documented in the validation report and, if applicable, in the release notes. The validation report should be approved by the responsible party before release for production.	システムバリデーション中に発生した逸脱は、記録し、クローズすること。予め重要と定義していた要件を満たさない場合、デプロイメント前に解決するか、〔逸脱の影響を〕低減するためのアクションを実施する必要がある。未解決の逸脱、及びリリース時のシステムの既知のイシューをすべてアセスメントし、決定事項をバリデーション報告書、及び該当する場合はリリースノートに記録する。バリデーション報告書は、運用へリリースする前に、責任のある当事者が承認すること。

A2.7 Release for production (運用へのリリース)

The responsible party should sign off the release prior to initial use. Training materials, user guides and any other resources required for users should be available at the time of release.	責任のある当事者は、使用開始前にリリースを承認すること。 トレーニング資料、ユーザーガイド、及びユーザーに必要なその他のリソースは、リリース時に利用できるようにすること。

A2.8 User helpdesk (ユーザーヘルプデスク)

There should be a mechanism to report, record, and solve defects and issues raised by the users e.g. via a helpdesk. Defects and issues should be fixed in a timely manner.	ユーザーから寄せられる欠陥やイシューを報告、記録、及び解決するための仕組み (例えばヘルプデスク経由) を設けること。欠陥やイシューはタイムリーに解決すること。

A2.9 Periodic review (定期レビュー)

Validation of a system should be maintained throughout the full system life cycle. Periodic system reviews should be conducted to assess and document whether the system can still be considered to be in a validated state, or whether individual parts or the whole system needs re-validation.	システムのバリデーション〔状態〕は、システムのライフサイクル全体を通じて維持する必要がある。定期的なシステムレビューを実施して、システムが依然としてバリデートされた状態にあると見なすことができるかどうか、又はシステムを部分的又は全体を再バリデートする必要があるかどうかをアセスメントし、文書化すること。

Depending on the system type and application, the following elements (non-exhaustive list) should be evaluated and concluded, both individually and in combination: • changes to hardware/infrastructure; • changes to operating system/platform; • changes to the application; • changes to security procedures; • changes to backup and restore tools and procedures; • configurations or customisations; • deviations (or recurrence thereof); • performance incidents; • security incidents; • open and newly identified risks; • new regulation; • review of system accesses; • updates of agreements with the service provider. These elements should be reviewed whether the system is hosted by the responsible party or by a service provider.	システムの種類とアプリケーションに応じて、次の要素 (網羅的ではない) を個別に、又は組み合わせて評価し、結論を出すこと。 • ハードウェア/インフラストラクチャの変更。 • OS/プラットフォームの変更。 • アプリケーションの変更。 • セキュリティ手順の変更。 • バックアップと復元のツールと手順の変更。 • 構成設定又はカスタマイズ。 • 逸脱 (又はその再発) 。 • パフォーマンスインシデント。 • セキュリティインシデント。 • 未解決のリスク又は新たに特定されたリスク。 • 新しい規制。 • システムアクセスのレビュー。 • サービスプロバイダとの契約の更新。 責任のある当事者又はサービスプロバイダのどちらがシステムをホストしていたとしても、上記要素をレビューする必要がある。

A2.10 Change control (変更コントロール)

There should be a formal change control process. Requests for change should be documented and authorised and should include details of the change, risk-assessment (e.g. for data integrity, current functionalities and regulatory compliance), impact on the validated state and testing requirements. For trial specific configurations and customisations, the change request should include the details of the protocol amendment if applicable.	正式な変更コントロールプロセスを設けること。変更依頼は文書化し、承認すること。また、変更依頼には変更の詳細、 (例えばデータインテグリティ、現在の機能、規制適合についての) リスクアセスメント、バリデートされた状態への影響、及びテスト要件、を含めること。治験固有の構成設定及びカスタマイズについての変更依頼には、該当する場合、治験実施計画書への修正の詳細を含めること。

As part of the change control process, all documentation should be updated as appropriate (e.g. requirements, test scripts, training materials, user guide) and a report of the validation activities prepared and approved prior to release for production. The system should be version controlled. The responsible party should ensure that any changes to the system do not result in data integrity or safety issues or interfere with the conduct of an ongoing trial. The investigator should be clearly informed of any change to a form (e.g. electronic case report form [eCRF] or electronic clinical outcome assessment [eCOA] page) and it should be clear when such changes were implemented. The documentation relating to the validation of previous or discontinued system versions used in a clinical trial should be retained (see '*Guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic)*' [EMA/INS/GCP/856758/2018], section 6.3).	変更コントロールプロセスの一環として、すべての文書 (例：要件、テストスクリプト、トレーニング資料、ユーザーガイド) を必要に応じて更新し、バリデーション活動の報告書を準備し、運用へリリースする前に承認すること。システムはバージョンコントロールすること。 責任のある当事者は、システムへの変更が、データインテグリティや安全性のイシューを引き起こしたり、進行中の治験の実施に干渉しないことを確実にすること。書式 (例：eCRF 又は eCOA ページ) への変更は治験責任医師に明確に通知する必要があり、いつそのような変更が実施されたのかを明確にすること。 治験で使用されたシステムバージョンのバリデーション関連文書は、過去のものも、利用中止したものも保持すること (「'*Guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic)*」」[EMA/INS/ GCP/856758/2018]、6.3 章参照のこと) 。

Annex 3 User management (付属書 3 ユーザー管理)

A3.1 User management (ユーザー管理)

Organisations should have a documented process in place to grant, change and revoke system accesses in a timely manner as people start, change, and end their involvement/responsibility in the management and/or conduct of the clinical trial projects.	各人が治験プロジェクトの管理、及び (又は) 実施への関与/責任を開始、変更、終了するときに、システムアクセスをタイムリーに許可、変更、及び取り消すための文書化されたプロセスを組織として設けておくこと。

Access to the system should only be granted to trained site users when all the necessary approvals for the clinical trial have been received and all documentation is in place (e.g. signed protocol and signed agreement with the investigator). This also applies to any updates to the system, e.g. changes resulting from a protocol amendment should only be made available to users once it is confirmed that the necessary approvals have been obtained, except where necessary to eliminate an immediate hazard to trial participants.	システムへのアクセスは、治験に必要なすべての承認が得られ、すべての文書 (例：署名された治験実施計画書及び治験責任医師との署名された同意書) が整った後に、トレーニング受講済みのサイトユーザーに対してのみ許可すべきである。このことはシステム更新時にも適用される。例えば、治験実施計画書の修正に起因する〔システム〕変更は、必要な承認が得られたことを確認してからユーザーに〔アクセスを〕提供すべきである。ただし治験参加者への緊急の危害を取り除くためにやむを得ない場合はその限りではない。

A3.2 User reviews (ユーザーレビュー)

At any given time, an overview of current and previous access, roles and permissions should be available from the system. This information concerning actual users and their privileges to systems should be verified at suitable intervals to ensure that only necessary and approved users have access and that their roles and permissions are appropriate. There should be timely removal of access no longer required, or no longer permitted.	いつでも、最新及び過去の〔ユーザーの〕アクセス、役割、及び権限の全容を、システム上で入手できるようにすること。実際のユーザーと〔そのユーザーの〕システムへの権限に関するこういった情報は、適切な間隔で検証し、必要かつ承認されたユーザーのみが〔システムに〕アクセスでき、その役割と権限が適切であることを確実にすること。不要になった、又は許可のなくなったアクセスはタイムリーに削除すること。

A3.3 Segregation of duties (職務の分離)

System access should be granted based on a segregation of duties and also the responsibilities of the investigator and the sponsor, as outlined in ICH E6.	ICH E6 で概説されているように、システムへのアクセスへの許可は、職務の分離を踏まえ、かつ治験責任医師と治験依頼者の責任に基づいて許可すること。

Users with privileged or '*admin access*' have extensive rights in the system (operating system or application), including but not limited to changing any system setting (e.g. system time), defining or deactivating users (incl. '*admin users*'), activate or deactivate audit trail functionality (and sometimes even edit audit trail information) and making changes to data that are not captured in the audit trail [e.g. backend table changes in the database(s)]). There is a risk that these privileges can be misused. Consequently, users with privileged access should be sufficiently independent from and not be involved in the management and conduct of the clinical trial and in the generation, modification, and review of data.	特権又は「*管理者アクセス*」を持つユーザーは、システム (OS 又はアプリケーション) で広範な権限を持つ。これには、システム設定 (例：システム時間) の変更、ユーザー (「*管理者ユーザー*」を含む) の登録又は無効化、監査証跡機能の有効化／無効化 (場合によっては監査証跡情報の編集も) 、監査証跡に記録されないデータ変更 (例えばデータベース内のバックエンド テーブルの変更) が含まれるが、これらに限定されるものではない。こういった特権が悪用されるリスクがあるため、特権アクセスを持つユーザーは、治験の管理及び実施、並びにデータの生成、変更、レビュー〔といった業務〕から十分に独立し、関わらせないようにすること。
Users of computer clients [e.g. personal computer (PC)] which record or contain critical clinical trial data, should generally not have 'admin access' to the relevant equipment and when this is not the case, it needs to be justified.	重要な治験データを記録又は保持するコンピュータクライアント (例：PC) のユーザーは、一般的に、その機器への「管理者アクセス」を持つべきではなく、そうでない場合は正当化する必要がある。
Unblinded information should only be accessible to pre-identified user roles.	非盲検化情報へのアクセスは、予め定められたユーザーロールのみに許可すること。

A3.4 Least-privilege rule (最小特権ルール)

System access should be assigned according to the least-privilege rule, i.e. users should have the fewest privileges and access rights for them to undertake their required duties for as short a time as necessary.	システムアクセスは、最小特権ルールに従って割り当てること。つまり、ユーザーが、要求される職務を、なるべく短時間で遂行するために必要な最小限の特権とアクセス権を付与すること。

A3.5 Individual accounts (個人のアカウント)

All system users should have individual accounts. Sharing of accounts (group accounts) is considered unacceptable and a violation of data integrity and ICH E6 principles as data should be attributable.	すべてのシステムユーザーには、個人用のアカウントを持たせること。アカウントの共有 (グループアカウント) は、容認できるものではなく、データインテグリティ及び ICH E6 の帰属性の原則への違反と考えられる。

A3.6 Unique usernames (ユニークなユーザー名)

User access should be unique within the system and across the full life cycle of the system. User account names should be traceable to a named owner and accounts intended for interactive use and those assigned to human users should be readily distinguishable from machine accounts.	ユーザーアクセスは、システムの中で、及びシステムのライフサイクルを通じてユニークとすること。ユーザーアカウント名から、所有者の名前及び (インタラクティブな使用を目的とする) アカウントに辿れるようにすべきであり、人間のユーザーに割り当てられたアカウントは、機器のアカウントと容易に区別できるようにすること。

Annex 4 Security (付属書 4 セキュリティ)

A4.1 Ongoing security measures (継続的なセキュリティ方策)

The responsible party should maintain a security system that prevents unauthorised access to the data. Threats and attacks on systems containing clinical trial data and corresponding measures to ensure security of such systems are constantly evolving, especially for systems and services being provided over or interfacing the internet.	責任のある当事者は、許可のないデータアクセスを防止するセキュリティシステムを維持すること。治験データを格納するシステムに対する脅威と攻撃は常に進化しており、システムセキュリティを確実にするための対応策も (特にインターネット経由で提供される、又はインターネットに接続するサービスやシステムでは) 常に進化している。

A4.2 Physical security (物理的セキュリティ)

Computerised systems, servers, communication infrastructure and media containing clinical trial data should be protected against physical damage, unauthorised physical access, and unavailability.	治験データを格納するコンピュータ化システム、サーバー、通信インフラストラクチャ、及びメディアは、物理的な損傷、許可のない物理的なアクセス、及び利用不可となる事態から保護すること。

The extent of security measures depends on the criticality of the data.	どこまでセキュリティ方策を講じるかは、データの重要度による。
The responsible party should ensure an adequate level of security for data centres as well as for local hardware such as universal serial bus (USB) drives, hard disks, tablets, or laptops.	責任のある当事者は、データセンターだけでなく、USB ドライブ、ハードディスク、タブレット、ラップトップなどのローカルハードウェアに対しても、適切なレベルでセキュリティを確実にすること。
At a data centre hosting clinical trial data, physical access should be limited to the necessary minimum and should generally be controlled by means of two-factor authentication. The data centre should be constructed to minimise the risk of flooding, there should be pest control and effective measures against fire, i.e. cooling, and fire detection and suppression. There should be emergency generators and uninterruptable power supplies (UPS) together with redundant Internet protocol providers. In case of co-location (see section 6.7 Cloud solutions), the servers should be locked up and physically protected (e.g. in cages) to prevent access from other clients. Media (e.g. hard disks) should be securely erased or destroyed before disposal.	治験データをホストするデータセンターへの物理的アクセスは必要最小限に制限し、一般的に二要素認証によってコントロールする必要がある。データセンターは、洪水のリスクを最小限に抑えるように建設し、害虫対策と効果的な火災対策 (冷却、火災検出・消火など) を講じること。非常用発電機と無停電電源装置 (UPS) に加え、予備のインターネットプロトコルプロバイダを確保しておくこと。コロケーション (6.7 章クラウドソリューションを参照)〔施設〕は、他の施設利用者からのアクセスを防ぐために、サーバーを (例えばケージに) 収納し、物理的に保護すること。メディア (例：ハードディスク) は、処分する前に確実に消去又は破壊すること。
Data should be replicated at an appropriate frequency from the primary data centre to a secondary failover site at an adequate physical distance to minimise the risk that the same fire or disaster destroys both data centres. A disaster recovery plan should be in place and tested.	データは、プライマリデータセンターから適切な物理的距離のあるセカンダリフェイルオーバーサイトに適切な頻度でレプリケートし、同じ火災や災害によって両方のデータセンターが破壊されるリスクを最小限に抑えること。災害復旧計画を策定し、テストすること。

A4.3 Firewalls (ファイアウォール)

In order to provide a barrier between a trusted internal network and an untrusted external network and to control incoming and outgoing network traffic (from certain IP addresses, destinations, protocols, applications, or ports etc.), firewall rules should be defined. These should be defined as strict as practically feasible, only allowing necessary and permissible traffic. As firewall settings tend to change over time (e.g. as software vendors and technicians need certain ports to be opened due to installation or maintenance of applications), firewall rules and settings should be periodically reviewed. This should ensure that firewall settings match approved firewall rules and the continued effectiveness of a firewall.	信頼できる内部ネットワークと信頼できない外部ネットワークの間にバリアを設け、 (特定の IP アドレス、宛先、プロトコル、アプリケーション、又はポートなどから) 受信／発信するネットワークトラフィックをコントロールするために、ファイアウォールルールを定義すること。ルールは実現可能な範囲でできるだけ厳密に定義し、必要かつ許可されたトラフィックのみを通過させるようにする。 ファイアウォールの設定は時間の経過とともに変化する (例えば、ソフトウェアベンダーや技術者はアプリケーションをインストール又は保守するために特定のポートを開く必要がある) 傾向があるため、ファイアウォールルールと設定を定期的に見直し、ファイアウォールの設定が承認されたファイアウォールルールと一致し、ファイアウォールが継続的に有効であることを確実にすること。

A4.4 Vulnerability management (脆弱性の管理)

Vulnerabilities in computer systems can be exploited to perform unauthorised actions, such as modifying data or making data inaccessible to legitimate users. Such exploitations could occur in operating systems for servers, computer clients, tablets and mobile phones, routers and platforms (e.g. databases). Consequently, relevant security patches for platforms and operating systems should be applied in a timely manner, according to vendor recommendations.	コンピュータシステムの脆弱性が悪用されると、許可のないアクションが実行され、例えばデータが変更されたり、正当なユーザーのデータアクセスが妨害されたりする。このような〔脆弱性の〕悪用は、サーバーOS、コンピュータクライアント、タブレット、携帯電話、ルーター、プラットフォーム (例：データベース) で発生する可能性がある。したがって、ベンダーの推奨に従って、プラットフォーム／OS に関連するセキュリティパッチをタイムリーに適用すること。

Systems, which are not security patched in a timely manner according to vendor recommendations, should be effectively isolated from computer networks and the internet, where relevant.	ベンダーの推奨に従ったタイムリーなセキュリティパッチを適用していないシステムは、必要に応じて、コンピュータネットワークやインターネットから効果的に切り離すこと。

A4.5 Platform management (プラットフォームの管理)

Platforms and operating systems for critical applications and components should be updated in a timely manner according to vendor recommendations, in order to prevent their use in an unsupported state.	重要なアプリケーションとコンポーネントを支えるプラットフォーム／OS は、ベンダーの推奨に従ってタイムリーに更新し、サポート期限が切れた状態で使用されることのないようにすること。
Unsupported platforms and operating systems, for which no security patches are available, are exposed to a higher risk of vulnerability. Validation of applications on the new platforms and operating systems and of the migration of data should be planned ahead and completed in due time prior to the expiry of the supported state.	サポートが終了したプラットフォーム／OS はセキュリティパッチが利用できなくなり、高い脆弱性リスクにさらされる。サポートが終了する前に、新しいプラットフォーム／OS で動作するアプリケーションのバリデーション、及びデータ移行のバリデーションを事前に計画し、完了しておくこと。
Unsupported platforms and operating systems should be effectively isolated from computer networks and the internet.	サポートが終了したプラットフォーム／OS は、コンピュータネットワーク及びインターネットから効果的に切り離すこと。
It should be ensured that software used in clinical trials remains compatible with any changes to platforms/operating systems in order to avoid unintended impact on the conduct/management of the clinical trial due to interruption of functionality or requirements for alternative software and data migration.	プラットフォーム／OS がどのように変更されたとしても、治験で使用されるソフトウェアの互換性を保つようにし、(機能が使えなくなる、又は代替ソフトウェアやデータ移行が必要になることによる) 治験の実施/管理への意図しない影響が生じないようにすること。

A4.6 Bi-directional devices (双方向デバイス)

The use of bi-directional devices (e.g. USB devices), which come from or have been used outside the organisation, should be strictly controlled as they may intentionally or unintentionally introduce malware and impact data integrity, data availability, and rights of trial participants.	組織の外から持ち込まれた、又は組織外で使用されてきた双方向デバイス (例：USB デバイス) の使用は厳密にコントロールすること。これは、意図の有無にかかわらずマルウェアを持ち込むことであり、データインテグリティ、データの可用性、及び治験参加者の権利に影響を与える可能性があるためである。

A4.7 Anti-virus software (ウイルス対策ソフトウェア)

Anti-virus software should be installed and activated on systems used in clinical trials. The anti-virus software should be continuously updated with the most recent virus definitions in order to identify, quarantine, and remove known computer viruses. This should be monitored.	治験で使用されるシステムには、ウイルス対策ソフトウェアをインストールし、有効化すること。既知のコンピュータウイルスを特定、隔離、及び削除するために、ウイルス対策ソフトウェアにおいて最新のウイルス定義を継続的に更新する必要があり、そのことをモニターすること。

A4.8 Penetration testing (侵入テスト)

For systems facing the internet, penetration testing should be conducted at regular intervals in order to evaluate the adequacy of security measures and identify vulnerabilities in system security (e.g. code injection), including the potential for unauthorised parties to gain access to and control of the system and its data. Vulnerabilities identified, especially those related to a potential loss of data integrity, should be addressed and mitigated in a timely manner.	インターネットに接続されているシステムでは、侵入テストを定期的に実施し、セキュリティ対策の妥当性を評価し、例えば許可のない者がシステムやデータにアクセスし、コントロールする可能性などの、システムセキュリティの脆弱性 (例：コードインジェクション) を明らかにする必要がある。特定された脆弱性、特にデータインテグリティが失われる可能性のある脆弱性は、タイムリーに対処し、低減する必要がある。

A4.9 Intrusion detection and prevention (侵入検出及び防止)

An effective intrusion detection and prevention system should be implemented on systems facing the internet in order to monitor the network for successful or unsuccessful intrusion attempts from external parties and for the design and maintenance of adequate information technology (IT) security procedures.	インターネットと接続されたシステムに効果的な侵入検出及び防止システムを実装し、外部からの侵入の試みが成功したのか失敗したのかを監視し、適切な情報技術 (IT) セキュリティ手順を設計／維持管理できるようにすること。

A4.10 Internal activity monitoring (内部の活動の監視)

An effective system for detecting unusual or risky user activities (e.g. shift in activity pattern) should be in place.	普段と異なる、又は危険なユーザー活動 (例：活動パターンの変化) を検出するための効果的なシステムを設けること。

A4.11 Security incident management (セキュリティインシデント管理)

Organisations managing clinical trial data should have and work according to a procedure that defines and documents security incidents, rates the criticality of incidents, and where applicable, implements effective corrective and preventive actions to prevent recurrence. In cases where data have been, or may have been, compromised, the procedures should include ways to report incidents to relevant parties where applicable. When using a service provider, the agreement should ensure that incidents are escalated to the sponsor in a timely manner for the sponsor to be able to report serious breaches as applicable, in accordance with Regulation (EU) No 536/2014.	治験データを管理する組織は、セキュリティインシデントを定義し、記録し、インシデントの重要度を評価し、必要に応じて再発を防ぐための効果的な是正・予防措置を実施するような手順を設け、それに従って作業すること。手順には、データが侵害された場合、又は侵害された疑いがある場合、必要に応じて関係者にインシデントを報告する方法を含める必要がある。サービスプロバイダを使用する場合、インシデントがタイムリーに治験依頼者にエスカレートされることを契約で確実にすること。これにより治験依頼者は Regulation (EU) No 536/2014 に従って、重大な〔セキュリティ〕違反をタイムリーに報告できるようになる。

A4.12 Authentication method (認証方法)

The method of authentication in a system should positively identify users with a high degree of certainty. Methods should be determined based on the type of information in the system. A minimum acceptable method would be user identification and a password. The need for more stringent authentication methods should be determined based on a risk assessment of the criticality of the data and applicable legislation (including data protection legislation), and generally should include two-factor authentication.	システムの認証方法は、高い確度でユーザーを確実に識別できるものとすること。〔認証〕方法は、システム内の情報の種類に基づいて決定すること。最低限許容される方法は、ユーザーID とパスワードである。データの重要度と適用される法律 (データ保護法を含む) についてのリスクアセスメント〔結果〕に基づいて、より厳格な認証方法が必要かどうかを決定する必要がある。〔より厳格な認証方法には〕一般的に二要素認証が含まれる。
User accounts should be automatically locked after a pre-defined number of successive failed authentication attempts, either for a defined period of time, or until they are re-activated by a system administrator after appropriate security checks.	認証の試みが、連続して予め定義された回数失敗した場合は、一定時間後か、又は適切なセキュリティチェックの後にシステム管理者が再度有効化するまで、ユーザーアカウントを自動的にロックしておくこと。
Biometric approaches are currently not specifically addressed by ICH E6. If using biometrics to authenticate the creation of a signature, the investigator and sponsor should ensure that these fulfil the above-mentioned requirements and local legal requirements.	バイオメトリクスのアプローチは、現時点で ICH E6 で具体的に触れられていない。治験責任医師や治験依頼者が、バイオメトリクスを使用して署名の真正性を証明するのであれば、上記の要件と現地の法的要件を満たしていることを確実にすること。

A4.13 Remote authentication (リモート認証)

Remote access to clinical trial data, e.g. to cloud-based systems, raises specific challenges. The level of security should be proportionate to the sensitivity and confidentiality of the data (e.g. nominative data in electronic medical records are highly sensitive) and to the access rights to be granted (read-only, write or even 'admin' rights). A risk-based approach should be used to define the type of access control required. Depending on the level of risk, two-factor authentication may be appropriate or necessary. Two-factor authentication implies that two of the following three factors be used: • something you know, e.g. a user identification and password • something you have, e.g. a security token, a certificate or a mobile phone and an SMS pass code • something you are, e.g. a fingerprint or an iris scan (biometrics)	治験データにリモートで (例えば、クラウドベースのシステムに) アクセスする場合は特別な懸念が生じる。セキュリティレベルは、データの機微性や機密性 (例えば、電子医療記録に含まれる個人が特定できるデータは非常に機微性が高い) と、付与するアクセス権 (読み取り専用、書き込み、さらには「管理者」権限も) に応じたものとすること。リスクベースアプローチを用いて、必要なアクセスコントロールのタイプを定義すること。リスクレベルによっては、二要素認証が適切又は必須かもしれない。 二要素認証とは、次の 3 つの要素のうち 2 つを用いることを意味する。 • 知っていること。例：ユーザーID とパスワード • 持っているもの。例：セキュリティトークン、証明書、又は携帯電話、SMS パスコード • 自分。例：指紋又は虹彩スキャン (バイオメトリクス)

A4.14 Password managers (パスワードマネージャ)

A secure and validated password manager, with a unique, robust user authentication each time it is used to log into a web site or system, can help to create and use different, complex passwords for each site or system. However, attention should be paid to insufficiently secured password managers.	安全でバリデート済みのパスワードマネージャは、Web サイト／システムへのログインに使用されるたびにユニークかつ堅牢なユーザー認証を行い、各サイト／システムで異なる複雑なパスワードを生成し、利用できるようにする。ただし、安全性が不十分なパスワードマネージャには注意が必要である。

Password managers built into web browsers may save and automatically fill in user identification and passwords, regardless of whether an independent secure password manager is used or not. This poses a risk if uncontrolled equipment is used (e.g. personal equipment, shared equipment or user accounts), as user access control cannot be enforced; a risk that needs to be effectively mitigated. A policy or contractual arrangement would not be considered adequate to provide a sufficient level of security in such situations.	独立した安全なパスワードマネージャを利用しているかどうかにかかわらず、Web ブラウザに組み込まれたパスワードマネージャがユーザーID とパスワードを保存し、〔ログイン時に〕自動的に入力する場合がある。これは、コントロールされていない機器 (例：個人の機器、共有された機器／ユーザーアカウント) を使用する場合、ユーザーアクセスをコントロールできないため、リスクをもたらすことになる。このリスクは効果的に低減する必要がある。このような状況で十分なレベルのセキュリティを得るためには、ポリシー又は契約上の取り決め〔だけで〕は適切と考えることはできない。
The risk linked to the potential hacking of user equipment or to key loggers should also be considered.	ユーザー機器への潜在的なハッキングやキーロガーに関連するリスクも考慮すること。

A4.15 Password policies (パスワードポリシー)

Formal procedures for password policies should be implemented. The policies should include but not necessarily be limited to length, complexity, expiry, login attempts, and logout reset. The policies should be enforced by systems and verified during system validation.	パスワードポリシーを実現するための正式な手順を設けること。ポリシーには、長さ、複雑さ、有効期限、ログイン試行回数、及びログアウトのリセットを含める必要があるが、必ずしもこれらに限定されるものではない。ポリシーはシステムによって強制すべきであり、システムバリデーションの中で検証すること。

A4.16 Password confidentiality (パスワードの機密性)

Passwords should be kept confidential, sharing of passwords is unacceptable and a violation of data integrity. Passwords initially received from the system or from a manager or system administrator should be changed by the user on their first connection to the system. This should be mandated by the system.	パスワードは秘密にしておく必要がある。パスワードの共有は容認できるものではなく、データインテグリティ違反である。システムから、又はマネージャかシステム管理者から最初に受け取ったパスワードは、ユーザーがシステムへの最初の接続時に変更する必要がある。このことは、システムが強制すべきである。

A4.17 Inactivity logout (無操作時のログアウト)

Systems should include an automatic inactivity logout, which logs out a user after a defined period of inactivity. The user should not be able to set the inactivity logout time (outside defined and acceptable limits) or deactivate the functionality. Upon inactivity logout, a re-authentication should be required (e.g. password entry).	無操作状態が一定時間経過後にユーザーをログアウトさせる自動無操作ログアウト機能をシステムに設けること。ユーザーが、無操作ログアウト時間を (定義された許容範囲外の値に) 設定したり、機能を無効化できないようにすること。無操作時でログアウトした後は、再認証 (例：パスワードの入力) を要求すること。

A4.18 Remote connection (リモート接続)

When remotely connecting to systems over the internet, a secure and encrypted protocol (virtual private network (VPN) and/or hypertext transfer protocol secure (HTTPS)) should be used.	インターネット経由でシステムにリモート接続する場合は、安全で暗号化されたプロトコル (仮想プライベート ネットワーク (VPN) 、及び (又は) 安全な HTTPS) を使用すること。

A4.19 Protection against unauthorised back-end changes
(許可のないバックエンド変更からの保護)

The integrity of data should be protected against unauthorised back-end changes made directly on a database by a database administrator. A method to prevent such changes could be by setting the application up to encrypt its data on the database or by storing data un-encrypted with an encrypted copy. In either case, the database administrator should not be identical to the administrator of the application.	データベース管理者がデータベースに直接行う、許可のないバックエンドの変更に対して、データのインテグリティを保護する必要がある。このような変更を防ぐ方法は、データベース上のデータを暗号化するようにアプリケーションを設定するか、暗号化済みのコピーを暗号化せずに保存することである。いずれの場合であっても、データベース管理者はアプリケーションの管理者と同一であってはならない。

Annex 5 Additional consideration to specific systems
(付属書 5 特定のシステムに対する追加的配慮)

All computerised systems used in clinical trials should fulfil the requirements and general principles described in the previous sections. The following sub-sections define more specific wording for selected types of systems where the GCP inspectors' working group (GCP IWG) has found that supplemental guidance is needed. For electronic trial master files (eTMFs), please refer to the respective guideline[1].	治験で使用されるすべてのコンピュータ化システムは、これまでに説明した要件及び一般原則を満たす必要がある。以下の章では、いくつかの種類のシステムについてさらに具体的に規定するが、これらは GCP inspectors' working group (GCP IWG) が補足的なガイダンスが必要と判断したものである。eTMF については、関連ガイドライン[1]を参照のこと。 【訳注】Guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic) (EMA/INS/GCP/856758/2018) の和訳については、https://bunzen.co.jp/ 参照。

[1] Guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic) (EMA/INS/GCP/856758/2018).

A5.1 Electronic clinical outcome assessment (eCOA)

Electronic clinical outcome assessment (eCOA) employs technology in addition to other data acquisition tools for the reporting of outcomes by investigators, trial participants, care givers and observers. This guideline does not address the clinical validation or appropriateness of particular eCOA systems. The guideline aims at addressing the topics specifically related to these eCOA systems and also to those related to the situation where bring-your-own-device (BYOD) solutions are used.	eCOA は、治験責任医師、治験参加者、介護者、及び観察者が転帰の報告を行うために、他のデータ収集ツールにはないテクノロジーを採用している。本ガイドラインでは、治験のバリデーションや特定の eCOA システムの妥当性について述べるつもりはしない。本ガイドラインは、これらの eCOA システムに特に関連するトピックと、Bring Your Own Device (BYOD) ソリューションが使用される状況に関するトピックについて触れることとする。
Data can be collected by any of several technologies and will be transferred to a server. Data should be made available to involved/responsible parties such as the investigator e.g. via portals, display of source data on the server, generation of alerts and reports. These processes should be controlled and clearly described in the protocol (high-level) and protocol-related documents, and all parts of the processes should be validated.	データは、いくつかあるテクノロジーを用いて収集された後に、サーバーに転送される。データは、治験責任医師などの関係者/責任のある当事者が利用できるようにする必要があるが、その方法には、例えばポータル経由、サーバー上での原データの表示、アラートやレポートの提供などがある。これらのプロセスはコントロールすべきであり、治験実施計画書 (概要レベル) 及び治験実施計画書の関連文書で明確に記述しておくこと。またプロセスのすべての部分はバリデートすること。

Collecting data electronically may offer more convenience to some trial participants and may increase participant compliance, data quality, reduce variability, reduce the amount of missing data (allowing automatic reminders) and potentially reduce data entry errors. Of importance, whilst use of such measures might be of benefit to some trial participants and patient groups, it may be inconvenient for or even result in the exclusion of others. This should be considered when using any data acquisition tool and the choice should be justified.	電子的にデータを収集することは、一部の治験参加者には、より便利であり、さらに参加者の順守を促進し、データ品質を向上させ、バラツキを減らし、(自動的なリマインダーにより) 欠落データの数を減らし、データ入力エラーを減らせるであろう。重要なことは、そのような手段を用いることは、一部の治験参加者や患者グループにとっては有益かもしれないが、他の参加者にとっては不便であり、彼らを結果的に除外してしまう可能性さえある。このことは、データ収集ツールを使用する際に考慮すべきであり、選択を正当化する必要がある。

A5.1.1 Electronic patient reported outcome (ePRO)

A5.1.1.1 System design (システム設計)

Electronic patient reported outcome (ePRO) should be designed to meet the specific needs of the end users. It is recommended to involve representatives of intended site staff and of the intended trial participant population, where relevant, in the development and testing. One of the advantages of using an ePRO system is that the timestamps of data entry are recorded. The timestamp should record the time of the data entry and not only the time of the data submission/transmission.	ePRO は、エンドユーザー特有のニーズを満たすように設計すること。必要に応じて、予定している治験実施施設の職員と予定している治験参加者の代表者を〔ePRO システムの〕開発とテストに関与させることが推奨される。 ePRO システムを使用する利点の 1 つは、データ入力のタイムスタンプが記録されることである。タイムスタンプは、データの提出/送信の時刻だけでなく、データ入力の時刻を記録すること。

Trial participants should be able to view their own previously entered data, unless justified and unless it is against the purpose of the clinical trial design or the protocol. Therefore, the period that data are viewable by the participant should be considered when designing/configuring the ePRO. Decisions about the '*view-period*' should be based on considerations regarding risk for bias on data to be entered. If viewing of recently entered data is not possible by the participant, then there is a risk that the participant could forget if relevant data have been collected. This is especially the case if the planned entry is event- driven. In addition, this prevents an unnecessary burden to site staff, as they will be contacted by trial participants in case of doubt less often.	治験参加者が過去に入力したデータを〔自分で〕閲覧できるようにすること。ただし、正当な理由がある、又は治験デザイン又は治験実施計画書の目的に反するときは、その限りではない。したがって、ePRO を設計/構成設定する際には、参加者がデータを閲覧できる期間を考慮する必要がある。「*閲覧期間*」は、入力データのバイアスのリスクを考慮して決定すべきである。少し前に入力したデータを閲覧できないと、参加者が有効なデータの収集を済ませたかどうか忘れてしまうリスクがある。これは計画された入力がイベント駆動型である場合に特に当てはまる。さらに、〔少し前に入力したデータを閲覧できるようにすれば〕治験参加者が〔入力を済ませたかどうか〕分からなくなって連絡をしてくる頻度が減るため、治験実施施設の職員への不必要な負担が減るであろう。
Logical checks should be in place to prevent unreasonable data changes such as '*time travel*' e.g. going back (months, years in time) or forward into the future based on the protocol design.	「*タイムトラベル*」(例えば、〔データ入力時刻を〕過去 (数か月、数年) に遡ったり、未来に進めたりする) のような、正当性のないデータ変更を防ぐために、治験実施計画書デザインに基づいて論理チェックを実施する必要がある。
It should be considered to include a scheduling/calendar component with alerts or reminders to assist compliance.	〔治験参加者の〕遵守を支援するアラート又はリマインダーを備えたスケジューリング/カレンダーコンポーネントを含めることを検討すること。

A5.1.1.2 Data collection and data transfer (データ収集及びデータ転送)

The same ICH E6 standards apply to data collected via ePRO as to any other method of data collection, i.e. that there are processes in place to ensure the quality of the data, and that all clinical information is recorded, handled and stored in such a way as to be accurately reported, interpreted and verified.	ePRO を介して収集されたデータには、他の方法によるデータ収集と同じく ICH E6 の基準が適用される。つまり、データ品質を確保するとともに、すべての臨床情報が、正確に報告され、解釈され、検証されるような方法で、記録、処理、保存されることを確実にするプロセスを設けること。
An ePRO system typically requires an entry device. Data saved on the device is the original record created by the trial participant. Since the data stored in a temporary memory are at higher risk of physical loss, it is necessary to transfer the data to a durable server at an early stage, by a validated procedure and with appropriate security methods during data transmission. Data should be transferred to the server according to a pre-defined procedure and at pre-defined times. The data saved on the device are considered source data. After the data are transferred to the server via a validated procedure, the original data can be removed from the device as the data on the server are considered certified copies. The sponsor should identify the source data in the protocol and protocol-related documents and should document the time and locations of source data storage.	一般的に、ePRO システムには入力デバイスが必要である。デバイスに保存されるデータが、治験参加者の作成したオリジナル記録となる。一時的にメモリに格納されたデータは物理的に損失するリスクが高いため、早い段階でデータを永続的なサーバーに転送する必要がある。データはバリデート済みの手順により転送し、その際は適切なセキュリティ方法を用いること。データは、予め定められた手順に従って、予め定められた時刻にサーバーに転送すること。デバイスに保存されたデータが原データと見なされる。データがバリデート済みの手順によりサーバーに転送された後は、サーバー上のデータが保証付きコピーと見なされるため、デバイス上のオリジナルデータは削除できる。治験依頼者は、治験実施計画書及び治験実施計画書の関連文書で原データを特定し、原データをいつ、どこに格納するのかを文書化すること。
In addition to the general requirements on audit trails (please refer to section 6.2.), if an ePRO system is designed to allow data correction, the data corrections should be documented, and an audit trail should record if the data saved on the device are changed before the data are submitted.	監査証跡に関する一般的な要件 (6.2 章を参照のこと) に加えて、もし ePRO システムでデータ修正ができるように設計されているならば、データ修正を記録する必要があり、デバイスに保存されたデータが提出前に変更されたかどうかを監査証跡に残す必要がある。

Data loss on devices should be avoided. Procedures should be in place to prevent data loss if web access to the trial participant reported data is interrupted, (e.g. server outage, device battery drained, loss of or unstable internet connection). There should be a procedure in place to handle failed or interrupted data transmission.	デバイスのデータが失われないようにすること。治験参加者からの報告データの Web アクセスが中断 (例：サーバーの停止、デバイスのバッテリーの消耗、インターネット接続断又は不安定な接続) した場合にデータの損失を防ぐための手順を設けておくこと。データ転送が失敗又は中断したときに対処する手順を設けておくこと。
It should be ensured/monitored that the transmission of data from ePRO devices is successfully completed.	ePRO デバイスからのデータ転送を確実に正常完了するようにし、かつそのことを監視すること。
Important actions should be time-stamped in an unambiguous way, e.g. data entries, transfer times and volume (bytes).	重要なアクションに対して、明確に区別ができるような方法でタイムスタンプを付ける必要がある。例えばデータ入力、転送回数、〔転送〕ボリューム (バイト) 〔で区別する〕。

A5.1.1.3 Investigator access (治験責任医師のアクセス)

Unlike data collected in the electronic case report form (eCRF), ePRO data are not managed (although available for review) by the investigator and are often hosted by a service provider. The investigator is overall responsible for the trial participants' data (including metadata). Those should consequently be made available to the investigator in a timely manner. This will allow the investigator to fulfil their responsibilities for oversight of safety and compliance and thereby minimise the risk of missed adverse events or missing data.	eCRF に収集されるデータとは異なり、治験責任医師は ePRO データを (レビューできるが) 管理していない。また、往々にして ePRO データはサービスプロバイダによりホストされる。治験責任医師は、治験参加者のデータ (メタデータを含む) に対して全体的な責任を負う。以上から治験責任医師がタイムリーに ePRO データを利用できるようにする必要がある。これにより、治験責任医師は〔治験参加者の〕安全性と遵守性を監督する責任を果たすことができ、それにより有害事象の見逃しやデータ欠落のリスクを最小限に抑えることができる。

A5.1.1.4 Data changes (データ変更)

As stated in section 6.2.1. on audit trails, a procedure should be in place to address and document if a data originator (e.g. investigator or trial participant) realises that they have submitted incorrect data by mistake and want to correct the recorded data.	6.2.1 章で監査証跡について述べたが、データオリジネータ (例：治験責任医師や治験参加者) が誤って正しくないデータを提出したことに気づき、記録されたデータを修正したい場合に対処し、記録する手順を設けておくこと。
Data changes for ePRO typically differ from that of other data acquisition tools because trial participants typically do not have the possibility to correct the data in the application. Hence, procedures need to be in place in order to implement changes when needed. This depends on the design of tools and processes and could be in the form of data clarification processes initiated by trial participants on their own reported data or initiated by investigators.	ePRO のデータ変更は、通常、治験参加者がアプリケーション上でデータを修正する可能性がないため、他のデータ収集ツールのデータ変更とは異なる。したがって、必要に応じて、変更を実施するための手順を設けておくこと。これはツールとプロセスがどのように設計されたかによるが、 (治験参加者自身が報告したデータについて開始する、又は治験責任医師が開始する) データクラリフィケーションプロセスの形を取る場合がある。
Data reported should always be reliable. Data clarification procedures introduced by the sponsor or service provider, whether or not described in the protocol should not prohibit changes in trial participant data when justified e.g. if the trial participant realises that the data have not been entered correctly.	報告されるデータは常に信頼できるものとすること。治験依頼者又はサービスプロバイダによって導入されるデータクラリフィケーション手順では、治験実施計画書に記載されているかどうかにかかわらず、正当な理由 (例えば治験参加者が、データが正しく入力されていないことに気付いた場合など) があるときは治験参加者データの変更を禁止すべきではない。

It is expected that the possibility for changes is implemented based on a justified and trial specific risk- assessment and that any changes are initiated in a timely manner by the participant or site staff and in case of the latter is based on a solid source at investigator sites e.g. phone notes or emails from trial participants documenting the communication between sites and trial participants immediately after the error was made/discovered.	〔データ〕変更を行うかどうかは、正当化された、かつ治験ごとのリスクアセスメントに基づいて行うことが期待されている。また、参加者又は治験実施施設の職員がタイムリーに変更を開始することが期待されている。後者の場合、治験実施施設側の確かな情報源(例えば、誤りが発生した/見つかった直後に治験実施施設と治験参加者との間で交わされた連絡を記録する電話メモ又は治験参加者からの電子メール) に基づくこと。
One of the advantages of direct data entry by the trial participant is that recall bias is minimised as the data are entered contemporaneously. Consequently, corrections should not be done at a much later stage without good reason and justification. Whether collected on paper or by electronic means, the regulatory requirements are that all clinical data should be accurately reported and should be verifiable in relation to clinical trials.	治験参加者が直接データ入力することの利点の一つは、データが同時的に入力されるため、記憶違いによるバイアスが最小限に抑えられることである。したがって、かなり後の段階での修正は、適切な理由があり正当化できる場合を除いて、行うべきではない。紙媒体、電子方式のどちらで収集したかにかかわらず、すべての臨床データが正確に報告され、治験に関連して検証可能であることが規制要件である。
It is expected that the number of changes to ePRO data are limited; however, this requires both designs of ePROs that are appropriate to ensure proper understanding by trial participants and appropriate training of trial participants, thereby avoiding entry errors.	ePRO データへの変更回数に制限があることが予想されるが、そのような場合は、入力エラーを回避するために、治験参加者が十分に理解できるような適切な ePRO の設計と、治験参加者への適切なトレーニングの両方が必要となる。

A5.1.1.5 Accountability of devices (デバイスのアカウンタビリティ)

There should be an accountability log of devices handed out to trial participants and this should include the device identification number in order to be reconciled to a particular trial participant.	治験参加者に配布されるデバイスにはアカウンタビリティログが必要である。アカウンタビリティログには、各治験参加者と照合するためのデバイス識別番号を含めること。

A5.1.1.6 Contingency processes (コンティンジェンシープロセス)

Contingency processes should be in place to prevent loss of data critical for participant safety or trial results. In case of device malfunction or loss of devices, there should be a procedure in place to replace the device and to merge data from several devices of a trial participant without losing traceability.	(参加者の安全又は治験結果にとって) 重要なデータの損失を防ぐために、コンティンジェンシープロセスを設けておくこと。デバイスの誤動作又はデバイス紛失時に、デバイスを交換し、トレーサビリティを失うことなく治験参加者の複数のデバイスからのデータをマージするための手順を設けておくこと。

A5.1.1.7 Username and password (ユーザー名とパスワード)

The trial participant's passwords should only be known to the trial participant. The username and password should not be used in a manner that would breach a trial participant's confidentiality. In relation to BYOD, sponsors should ensure that basic user access controls are implemented. When mobile applications are used for data entry, access controls need to be in place to ensure attributability. See section A5.1.3 for further guidance on BYOD.	治験参加者のパスワードは、治験参加者のみが知っているようなものとすること。 ユーザー名とパスワードは、治験参加者の機密性を侵害するような方法で使用してはならない。 BYOD に関連して、治験依頼者は、基本的なユーザーアクセスコントロールが実装されていることを確実にすること。データ入力にモバイルアプリケーションを使用する場合、アクセスコントロールを実施して、帰属性を確実にすること。BYOD の詳細なガイダンスについては、A5.1.3 章を参照のこと。

A5.1.1.8 Training (トレーニング)

Training should be customised to meet the specific needs of the end users.	トレーニングは、エンドユーザー固有のニーズを満たすようにカスタマイズすること。

A5.1.1.9 User support (ユーザーサポート)

Support to the trial participant and the trial site staff should be readily available (e.g. support via phone or email) in order to ensure reliable data and minimise the risk of data loss. Trial participant confidentiality should be ensured at all times, including in the communication process.	データの信頼性を確実にし、データ損失のリスクを最小限に抑えるために、治験参加者と治験実施施設の職員へのサポート (例：電話や電子メールによるサポート) を随時利用できるようにすること。治験参加者の機密性は、いかなるとき (連絡を取っているときも含む) も確実に守ること。

Procedures for service desk, user authentication and access restoration should be implemented.	サービスデスク、ユーザー認証、アクセス復旧の手順を設けておくこと。

A5.1.2 Clinician reported outcome (CRO)

Tools to directly collect clinician reported outcomes should generally follow the same requirements as those described for systems in general and for ePROs. The main difference is the user (investigators, other clinicians, or independent assessors instead of trial participants), not the system requirements. Special attention should be given to access control in order to avoid jeopardising any blinding, when relevant.	Clinician reported outcome を直接収集するツールは、一般システム及び ePRO で説明したものとほぼ同じ要件に従う必要がある。主な違いは、システム要件ではなく、ユーザー (参加者ではなく、治験責任医師、他の臨床医、又は独立した評価者がユーザーとなる) にある。必要に応じて、盲検性が損なわれないようにするために、アクセスコントロールに特別な注意を払う必要がある。

A5.1.3 Bring your own device (BYOD)

Both ePRO data and clinician reported outcome data may be captured by privately owned devices such as mobile phones, tablets, computers and wearables, i.e. BYOD. This can either be achieved via a web- application with pre-installed browser applications or by installing an application on the device. Solutions can be either a combination of web and application (hybrid) or coded to the device operating system (native).	ePRO データ及び clinician reported outcome データはどちらも、携帯電話、タブレット、コンピュータ、ウェアラブルなどの個人所有デバイス、つまり BYOD によって収集される場合がある。これは、プリインストールされたブラウザアプリケーション上の Web アプリケーションを介して、又はデバイスにアプリケーションをインストールすることによって実現できる。ソリューションは、Web とアプリケーションの組み合わせ (hybrid)、又はデバイス OS にコーディングしたもの (native) のいずれかである。
It is necessary to provide alternative ways of data collection e.g. devices provided by the sponsor, as the trial participants should not be excluded from a trial if not capable of or willing to use BYOD.	治験参加者が BYOD を使用できない、又は使用したくない場合であっても、治験参加者を治験から除外すべきではないため、データ収集の代替方法 (例えば、治験依頼者がデバイスを提供する) を用意しておくこと。

A5.1.3.1 Technical and operational considerations (技術面及び運用面での検討事項)

When using BYOD, a variety of devices, operating systems and where applicable web browsers commonly used, should be considered for the application. It should be ensured that it is not exclusive to one model or operating system.	BYOD を使用する場合は、アプリケーションのために、さまざまなデバイス、OS、及び(該当する場合) 一般的に使用されている Web ブラウザを検討する必要がある。一つのモデル又は OS に限定しないようにすること。
The sponsor should describe the minimum technical specifications for participants' devices (e.g. operating system, web browser and storage capacity). These should take into account which operating systems are still supported by the manufacturer and if bug fixes and security patches have been released, when relevant.	治験依頼者は、参加者のデバイスに求める最低限の技術仕様 (例：OS、Web ブラウザ、ストレージ容量) を明確にする必要がある。その際に、必要に応じて、どの OS が製造元によってまだサポートされているか、またバグ修正やセキュリティパッチがリリースされているか、を考慮すること。
The sponsor should ensure the quality and integrity of the data across all accepted models and versions.	治験依頼者は〔利用を〕許可するすべてのモデルとバージョンについて、データの品質とインテグリティを確実にすること。
The sponsor has no control over the implementation of updates to the operating system or over the applications on the trial participant's device. These aspects should be taken into consideration in their risk evaluation and subsequent validation activities.	治験依頼者は、OS を更新したり、治験参加者のデバイス上のアプリケーションをコントロールしたりすることはできない。このことは、リスク評価とその後のバリデーション活動で考慮に入れること。
The application should use an external source for date and time and should not rely on information from the user's device.	アプリケーションの日付と時刻は、外部ソースを使用すべきであり、ユーザーのデバイスからの情報に依存すべきではない。
Procedures and processes should be in place for when the trial participant discontinues the clinical trial or the clinical trial ends and access to applications and data collection should be terminated.	治験参加者が治験を途中でやめる、又は治験が終了し、アプリケーションへのアクセスとデータ収集を終了する場合の手順とプロセスを設けておくこと。

A5.1.3.2 Considerations on security and trial participant confidentiality

(セキュリティと治験参加者の機密性保持についての検討事項)

The confidentiality of data that could identify trial participants should be protected, respecting the privacy and confidentiality rules in accordance with the applicable regulatory requirements.	治験参加者を特定できるようなデータは、プライバシー及び適用される規制要件に従った機密保持規則を尊重し、その機密性を保護すべきである。
A number of challenges for BYOD are related to security, and security should be ensured at all levels (mobile device security, data breach security, mobile application security, etc.). As mobile devices may be lost or stolen and it cannot be ensured that the trial participants use any authentication methods to secure their device, access control should be at the application level. Section A.4.14 on the use of password managers also applies.	BYOD の多くの課題はセキュリティに関連しており、すべてのレベル (モバイルデバイスのセキュリティ、データ侵害に対するセキュリティ、モバイルアプリケーションのセキュリティなど) でセキュリティを確実にする必要がある。モバイルデバイスは紛失又は盗難に遭う可能性があるが、治験参加者がデバイスを認証により保護しているとは限らないため、アプリケーションレベルでアクセスコントロールを行うこと。パスワードマネージャの使用に関する A.4.14 章も適用される。
Risks linked to known application and operating system vulnerabilities should be minimised.	アプリケーション及び OS の既知の脆弱性に関連するリスクは最小限に抑えること。
The hardware, operating system and applications are all factors that affect the total security status of the device, and there should be procedures in place regarding e.g., when trial participants/clinicians use less secure devices.	ハードウェア、OS、及びアプリケーションはすべて、デバイス全体のセキュリティ状態に影響を与える要因であり、例えば、治験参加者/臨床医が安全性の低いデバイスを使用する場合などに関する手順を設けておくこと。

Data capture by BYOD may require the device to be identified to ensure data attributability. Only information that is needed for proper identification of and service to the user should be obtained. Trial participant confidentiality should be ensured if device identification information is stored. Access to the application and trial participant data may be protected with multiple barriers (e.g. unlock mobile phone, open application, access data).	BYOD によるデータ取集では、データの帰属性を確実にするためにデバイスの識別が必要な場合がある。〔その場合〕ユーザーを適切に識別し、ユーザーにサービスを提供するために必要な情報のみを取得すべきである。デバイスの識別情報を格納する場合、治験参加者の機密性保持を確実にすること。アプリケーション及び治験参加者データへのアクセスは、複数のバリア (例えば、携帯電話をロック解除し、アプリケーションを開き、データにアクセスする) で保護するとよい。
If the device's built-in capabilities for auto fill formula data and/or using photo, video, and global positioning system (GPS) data, etc. are used, this should be described and justified in the protocol. Procedures and processes should ensure that only protocol mandated data are collected, and that the confidentiality of data is maintained. In accordance with the principle of '*data minimisation*' mobile applications should only collect data that are necessary for the purposes of the data processing and not access any other information on the person's device. For example, location data should only be collected if it is necessary for the clinical trial activities and the trial participant must be informed about it in the patient information and agree to it in the consent form.	(定型データを自動的に埋め込んだり、写真、ビデオ、GPS データなどを用いる) デバイス組み込み機能を使用する場合は、治験実施計画書で説明し、正当化する必要がある。手順とプロセスにより、治験実施計画書で定められたデータのみが収集され、データの機密性が維持されることを確実にすべきである。「*データ最小化*」の原則に従い、モバイルアプリケーションは、データ処理の目的に必要なデータのみを収集し、個人のデバイス上の他の情報にアクセスしてはならない。例えば、位置データは、治験活動に必要な場合にのみ収集すべきであり、そのことは治験参加者に関連情報として知らせ、インフォームドコンセント書式で合意する必要がある。

Providers may have end-user licensing agreements or terms of service that allow the sharing of data. This may be in conflict with ICH E6 and (local) legal requirements or require information to be provided to the participant and may require specific informed consent. In some cases, the application may not be suitable for use. If an application is to be installed on a BYOD, the privacy labels/practices (e.g. regarding tracking data, linked and not linked data) should be clearly communicated to the trial participant upfront.	エンドユーザーライセンス契約又はサービス条件で、プロバイダがデータの共有を許されているかもしれないが、これは ICH E6 及び (現地の) 法的要件に抵触する場合があり、参加者への情報提供やインフォームドコンセントが必要になるかもしれない。場合によっては、そのアプリケーションは使用しない方がよいかもしれない。アプリケーションを BYOD にインストールする場合は、(例えば追跡データやリンクされた／されないデータについての) プライバシーラベル【訳注】/慣行を治験参加者に事前に明確に伝えること。 【訳注】プライバシーラベルは、ユーザーがアプリによるユーザーデータの処理方法に関する情報を確認したり、開発者が収集されたデータとその使用方法をユーザーに通知したりするための手段を提供する。
The sponsor should be aware that explicit consent may be required related to the above. The informed consent should describe the type of information that will be collected via ePRO and how that information will be used.	治験依頼者は、上記に関連して〔治験参加者の〕明示的な同意を得ることを求められる可能性があることに留意すること。インフォームドコンセントにおいて、ePRO を介して収集される情報の種類と、その情報がどのように使用されるかについて明確にすること。

A5.1.3.3 Installation and support (インストレーションとサポート)

When using an application, it is recommended that appropriately trained staff assist in the installation even if the application is available through an app-store or service provider platform.	アプリケーションを利用するときは、アプリケーションがアプリストア又はサービスプロバイダプラットフォームから入手できる場合であっても、適切な訓練を受けたスタッフがインストールを支援することを勧める。

Independently of whether the BYOD solution is based on an application installed on the device or a website/web application, the software and the use should be explained thoroughly via targeted training, which may include user manuals, one-to-one training, and multimedia tools. Users of the system should have access to user support e.g. from a help desk. There should be a procedure in place in case an application cannot be installed, or the web service is unavailable on a device, if the device has malfunctioned or the participant has purchased a new device. Helpdesk contacts by users should be logged (participant or site staff study ID, purpose of contact, etc.) with due consideration of protecting participant information.	BYOD ソリューションが、デバイスにインストールされたアプリケーションなのか、Web サイト/Web アプリケーションなのかに関係なく、ソフトウェアとその使用方法を、(ユーザーマニュアル、1 対 1 トレーニング、及びマルチメディアツールなどの) 対象者を絞ったトレーニングにより、徹底的に説明する必要がある。システムユーザーがヘルプデスクなどのユーザーサポートにアクセスできるようにすること。デバイスが誤動作したり、参加者が新しいデバイスを購入することがあるため、アプリケーションをインストールできない、又はデバイスで Web サービスを利用できないようなときに備えた手順を設けておくこと。ユーザーによるヘルプデスクへの連絡内容を記録 (参加者又は治験実施施設の職員の治験 ID、連絡目的など) する必要があるが、参加者情報の保護に十分に配慮すること。
The software and software installation should not limit or interfere with the normal operations of the device. Any unavoidable limitation to the device after installation should be part of the informed consent material.	そのソフトウェアによって、又はソフトウェアをインストールすることによって、デバイスの通常の操作が制限されたり、妨げられるべきではない。インストール後にどうしてもデバイスに制限が出てしまう場合は、その制限をインフォームドコンセントの資料に明記すること。

A5.1.3.4 Uninstallation (アンインストール)

It should be possible to uninstall software or applications without leaving residues on BYOD devices, e.g. entries in the registry, incorrect mappings or file fragments. The user should be able to uninstall at any time without expertise or assistance. The uninstallation process should not compromise the device.	BYOD デバイスに、ゴミ (例えば、レジストリのエントリ、不適切なマッピング、又はファイルのフラグメントなど) を残すことなく、ソフトウェアやアプリケーションをアンインストールできるようにすること。ユーザーは、専門知識や支援なしで、いつでもアンインストールできるようにすること。アンインストールすることでデバイスを危険にさらさないようにすること。

A5.2 Interactive response technology system (IRT システム)

A5.2.1 Testing of functionalities (機能のテスト)

In addition to the content of the sections A2.6, A2.10, of this guideline, sponsors should also consider the issues mentioned below when writing test scripts for user acceptance tests (UAT).	本書の A2.6 章、A2.10 章の内容に加えて、治験依頼者は、ユーザー受入テスト (UAT) のテストスクリプトを作成する際に、以下に示すイシューも考慮する必要がある。

A5.2.1.1 Dosage calculations (服用量の計算)

Where dosage calculations/assignments are made by the IRT system based on user entered data (e.g., trial participant body surface area or weight), and look-up tables (dosage assignment based on trial participant parameters), the tables should be verified against the approved protocol and input data used to test allocations, including test data that would be on a borderline between differing doses. Assigning the incorrect dosage to a trial participant is a significant risk to safety and well-being and such inaccurate assignments should be thoroughly mitigated.	IRT システムが、ユーザーの入力データ (例：治験参加者の体表面積又は体重) 及びルックアップテーブル (治験参加者のパラメータに基づく服用量の割り当て) に基づいて服用量の計算/割り当てを行う場合、その表は、承認されたプロトコル及び割り当てテスト用の入力データ (異なる服用量間の境界線上にあるテストデータを含む) に対して検証する必要がある。治験参加者に誤った服用量を割り当てることは〔治験参加者の〕安全と健康にとって重大なリスクであり、そのような不正確な〔服用量の〕割り当て〔のリスク〕は徹底的に低減すべきである。

A5.2.1.2 Stratified randomisation (層別ランダム化)

Where the randomisation is stratified by factors inputted by the user, all the combinations of the strata should be tested to confirm that the allocation is occurring from the correct randomisation table.	ユーザーによって入力された要因によってランダム化を層別している場合、すべての層の組み合わせをテストして、正しいランダム化テーブルに基づいて割り付けが行われていることを確認すること。

A5.2.1.3 Blinding and unblinding (盲検化と盲検解除)

Unblinded information should only be provided and accessible to pre-identified user roles.	盲検解除された情報は、事前に特定されたユーザーロールに対してのみ提供し、アクセス可能にすること。

A5.2.2 Emergency unblinding (緊急盲検解除)

The process for emergency unblinding should be tested. A backup process should also be in place in case the online-technology emergency unblinding is unavailable. It should be verified that a site's ability for emergency unblinding is effectively available before administering IMP to a trial participant.	緊急盲検解除プロセスをテストしておく必要がある。オンライン技術によって緊急盲検解除できない場合に備えて、バックアッププロセスも設けておく必要がある。 治験参加者に治験薬を投与する前に、治験実施施設がいざというときに緊急盲検解除を実施する能力があることを検証しておく必要がある。

A5.2.3 IRT used for collection of clinical data from the trial site (治験実施施設からの臨床データ収集に用いるIRT)

Where the IRT system is collecting clinical data, important data should be subject to source data verification and/or reconciliation with the same data collected in the data acquisition tool. For example, the data used for stratification may also be contained in the data acquisition tool. Where clinical data is entered into the IRT system and integrated in the electronic data collection (EDC) system (electronic data transfer to EDC) the additional functionality and ICH E6 requirement concerning data acquisition tools (eCRFs) should be addressed in the IRT system requirements and UAT e.g. investigator control of site entered data, authorisation of data changes by the investigator, authorisation of persons entering/editing data in the system by the investigator.	IRT システムが臨床データを収集する場合、重要なデータについて、原データのベリフィケーション、及び (又は) データ収集ツールで収集された同一データとの突合を行うこと。例えば、層別化に使用されるデータもデータ収集ツールで収集されている場合がある。臨床データが IRT システムに入力されてから (EDC へ電子データ転送され) EDC システムで統合される場合、データ収集ツール (eCRF) の追加機能と ICH E6 要件は、IRT システムの要件及び UAT (例えば、治験責任医師による治験実施施設で入力されたデータのコントロール、治験責任医師によるデータ変更の許可、治験責任医師によるシステム内のデータ入力/編集者への許可) として対応すべきである。

A5.2.4 Web-based randomization (Webベースのランダム化)

Where justified, sponsor or investigator/sponsor may also use a web-based application to create randomisation lists for clinical trials. When using a web-service, the process to evaluate the suitability of the system and GCP compliance as well as the fitness for purpose of the created randomization list should be documented. The version of the service used, and where applicable, the seed should be maintained.	正当な理由がある場合、治験依頼者又は治験責任医師/治験依頼者は、Web ベースのアプリケーションを使用して治験のランダム化リストを作成してもよい。Web サービスを使用する場合、システムの適切さ、GCP への準拠を評価するプロセス、及び作成されたランダム化リストが目的に合っていることを文書化しておく必要がある。使用しているサービスのバージョン及び、必要に応じて乱数種を維持管理すること。
Ad hoc randomization via a web-service is not recommended as randomization distribution is unknown, the sponsor is not in control of the process e.g. the seed may vary.	Web サービスを介したアドホックなランダム化は、ランダム化の分布が不明であり、治験依頼者がプロセスをコントロールしていない (例えば乱数種が変わるかもしれない) ため勧められない。

The sponsor should ensure that the process of randomisation can be reconstructed via retained documentation and data and that a final randomisation schedule is retained.	治験依頼者は、ランダム化のプロセスを保存された文書とデータから再構築でき、かつ最終的なランダム化スケジュールが保持されるようにすること。

A5.3 Electronic informed consent (電子的インフォームドコンセント)

Ethics committees will review all material related to the informed consent process. Before the implementation of an electronic consent procedure is considered, the sponsor should ensure that the electronic consent procedure is GCP compliant and legally acceptable in accordance with the requirements of the independent ethics committees concerned and of the national regulatory authorities.	倫理委員会は、インフォームドコンセントプロセスに関連するすべての資料をレビューする。治験依頼者は、電子的同意取得手順の実装を検討する前に、電子的同意取得手順がGCP に準拠し、かつ関係する独立倫理委員会及び国の規制当局の定める要件に従い、かつ法的に許容されるものであることを確実にする必要がある。
The principles of consent as set out in legislation and guidance should be the same regardless of whether the process involves a computerised system. A hybrid approach could be considered, where national requirements preclude cern parts of an electronic informed consent procedure. At present, in some countries failure to provide '*written on paper*' proof of a trial participant's informed consent is considered a legal offense.	法律及びガイダンスに定められている同意の原則は、プロセスにコンピュータ化システムを用いるかどうかに関係なく、等しくあるべきである。国の要件が電子的インフォームドコンセント手順の一部【訳注】を認めない場合はハイブリッドアプローチを検討してもよい。現在、一部の国では、治験参加者のインフォームドコンセントについて「*紙に書かれた*」証拠を提供しないことが法律違反と見なされている。 【訳注】cern parts of …の "cern"は certain の誤記と解釈して訳した。

An electronic informed consent refers to the use of any digital media (e.g. text, graphics, audio, video, podcasts or websites) firstly to convey information related to the clinical trial to the trial participant and secondly to document informed consent via an electronic device (e.g. mobile phones, tablets or computers). The electronic informed consent process involves electronic provision of information, the procedure for providing the opportunity to inquire about details of the clinical trial including the answering of questions and/or electronic signing of informed consent. For example, it would be possible for the trial participant to sign informed consent on a paper form following provision of the information electronically or the information and informed consent could be entirely electronic. If using a 'wet ink' signature together with an electronic informed consent document (a hybrid approach), the patient information, the informed consent document and the signature should be indisputably linked. The method of obtaining an informed consent should ensure the broadest possible access to clinical trials. Alternative methods for provision of information and documentation of informed consent should be available for those unable or unwilling to use electronic methods. Any sole use of electronic informed consent should be justified and described in the protocol.	電子的インフォームドコンセントとは、最初に治験に関連する情報を治験参加者にデジタルメディア (例：テキスト、グラフィックス、オーディオ、ビデオ、ポッドキャスト、又は Web サイト) を使用して伝え、次に電子デバイス (例：携帯電話、タブレット、又はパソコン) によりインフォームドコンセントを記録することである。電子的インフォームドコンセントには、情報の電子的提供、治験の詳細 (質問への回答を含む) についての問い合わせ機会を提供する手順、及び (又は) インフォームドコンセントへの電子署名といったプロセスが含まれる。例えば、治験参加者は、電子的に情報の提供を受けた後、紙のインフォームドコンセント書式へ署名をしてもよいし、情報〔提供〕とインフォームドコンセントを完全に電子的に行ってもよい。「ウェットインク」署名を電子的インフォームドコンセント文書と一緒に使用する場合 (ハイブリッドアプローチ) 、患者情報、インフォームドコンセント文書、及び署名を、明確に関連付ける必要がある。インフォームドコンセントを取得する方法は、〔治験参加者が〕治験〔の情報〕に可能な限り広範なアクセスを確実にするものであること。電子的な方法を使用できない、又は使用したくない者でも利用できるように、インフォームドコンセントの情報と文書を提供するための代替方法を提供すること。電子的インフォームドコンセントのみを使用するのであれば、そのことを正当化し、治験実施計画書に記載すること。

A5.3.1 Provision of information about the clinical trial (治験に関する情報の提供)

The trial participants should have been informed of the nature, objectives, significance, implications, the expected benefit, risks, and inconveniences of the clinical trial in an interview with the investigator, or another member of the investigating team delegated by the principal investigator. The interview should take into account the individual disposition (e.g. comorbidities, patient references, etc.) of the potential participant (or legal representative). This interview should allow interaction, the asking of questions and allow confirmation of the trial participant's identity and not just simply the provision of information. The interview should be conducted in person or, it could be done remotely where this can be justified and is allowed nationally and if approved by an ethics committee using electronic methods that allow for two- way communication in real time. Whichever method is used it is important that confidentiality is maintained, and therefore communication methods should be private/secure. Consideration should be given as to how the system would be presented to the ethics committee for approval so that it captures the functionality of the system and the experience of the potential trial participant using it. Direct system access should be provided to the ethics committee upon request in a timely manner.	治験参加者には、治験責任医師との面談、又は主任治験責任医師から委任された治験チームの別メンバーとの面談により、治験の性質、目的、重要性、影響、予想される利益、リスク、及び不便さについて知らせておくこと。面談では、潜在的な参加者 (又は法定代理人) の個々の性質 (例：併存疾患、患者の紹介) を考慮すること。この面談では、単に情報を提供するだけでなく、対話や質問を行うようにし、治験参加者の身元を確認するようにすること。面談は対面で実施すべきであるが、正当化され、国内で許可され、かつ倫理委員会によって承認されている場合は、リアルタイムでの双方向通信可能な電子的方法を使用してリモートで実施してもよい。どちらの方法を使用する場合でも、機密性を維持することが重要であるため、通信方法はプライベートで安全なものにする必要がある。倫理委員会の承認を受けるためにシステムをどのように説明すればよいか検討し、説明の中でシステム機能、及びシステムを使用する潜在的な治験参加者の経験について触れること。要求があったときは倫理委員会に対してタイムリーにシステムへの直接アクセスを提供すること。

Provision of the information electronically may improve the trial participants' understanding of what taking part in the clinical trial will involve. Computerised systems could facilitate features to assess the participant's understanding e.g. via questions at key points, which self-evaluate trial participants' understanding as they work their way through the information. This, in turn, can be used to highlight areas of uncertainty to the person seeking consent so that they can cover this area in more detail with the trial participant.	治験参加者は、電子的に情報提供することにより、治験に参加するとはどういうことなのかについて理解を深められる。例えば、重要な個所で質問するなどして、参加者の理解度を評価する機能をコンピュータ化システムに持たせることで、治験参加者が情報を読み進めるうちに理解度を自己評価することができる。またこの機能を使用することで、同意を取得しようとしている人の理解があやふやなところを明確にすることができ、その部分をより詳細にカバーすることができる。

A5.3.2 Written informed consent (書面によるインフォームドコンセント)

The informed consent of the trial participant should be in writing and electronic methods for documenting the trial participant's informed consent should ensure that the informed consent form is signed and personally dated by at least two (natural) persons; the trial participant or the trial participant's legal representative, and the person who conducted the informed consent discussion. The identity of the persons signing should be ensured. The method used to document consent should follow national legislation with regard to e.g. acceptability of electronic signatures (see section 4.8.), and in some countries '*wet ink*' signature will be required.	治験参加者のインフォームドコンセントは書面で行う必要があり、電子的な方法を用いて治験参加者のインフォームドコンセントを記録する場合は、インフォームドコンセント書式に、少なくとも 2 名の (自然) 人 (すなわち、治験参加者又は治験参加者の法定代理人、及びインフォームドコンセントの話し合いを執り行った者) が署名し、各人が日付を入れるようにすること。署名者の身元を確かめること。 同意を記録するために用いる方法は、例えば電子署名 (4.8 章参照) を用いてよいかどうかについて、国内法に従う必要がある。また一部の国では「*ウェットインク*」署名が必要となる。

There should be no ambiguity about the time of signature. The system should use timestamps for the audit trail for the action of signing and dating by the trial participant and investigator or qualified person who conducted the informed consent interview, which cannot be manipulated by system settings. Any alterations of the document should invalidate the electronic signature.	署名された時刻が不正確であってはならない。システムでは、治験参加者及び治験責任医師又はインフォームドコンセントの面談を実施した適格な者が、署名し日付を記入したことを記録する監査証跡においてシステム設定で改ざんできないようなタイムスタンプを用いるようにすること。〔署名された〕文書が変更されたときは、電子署名を無効にすること。
If an electronic signature is used, it should be possible for monitors, auditors, and inspectors to access the signed informed consent forms and all information regarding the signatures, including the audit trail.	電子署名が使用されている場合、モニター、監査者、及び査察官が、署名済みのインフォームドコンセント書式及び署名に関するすべての情報 (監査証跡を含む) にアクセスできるようにすること。
Secure archiving should ensure availability and legibility for the required retention period.	安全にアーカイブし、要求される保存期間を通じて可用性と判読性を確実にすること。

A5.3.3 Trial participant identity (治験参加者の認証)

It should always be possible to verify the identity of a trial participant with documentation available to the investigator. Documentation which makes it possible to demonstrate that the person entering the electronic '*signature*' was indeed the signatory, is required. The electronic signing should be captured by the audit trail.	治験責任医師が入手できる文書から治験参加者の身元を常に確認できるようにすること。電子「*署名*」を実行する者が本当の署名者であることを証明できるような文書が必要である。電子署名の実行は、監査証跡に記録すべきである。
Where consent is given remotely, and the trial participant is required at some point to visit a clinical trial site for the purposes of the trial, verification should be done in person e.g. by using information from an official photo identification if such an ID document is required in the trial site country.	ある時点においてリモートで同意をした治験参加者に、治験のために治験実施施設に来てもらう必要が生じたときは、本人に対して対面で、例えば治験を実施する国で身分証明書が必要とされるのであればそのような公式の写真付き身分証明書の情報を使用して、本人確認を行うこと。

A5.3.4 Sponsor notification on the consent process
(同意取得プロセスについての治験依頼者への通知)

Notification to the sponsor should only contain essential, non-personal identifiable information to allow the sponsor to have an overview of how many trial participants have been enrolled in a clinical trial so far and which versions of the electronic informed consent form have been used. Remote access to personal identifiable information in the electronic system should only be permitted for the corresponding participant, legal representative, investigator, monitor, auditor, or inspector. Any unjustified accesses, which lead to the disclosure of non-pseudonymised information, are likely to be viewed as an infringement of data privacy laws.	治験依頼者への通知には、重要かつ個人を特定できない情報だけを含めるようにし、これまでに治験に登録された治験参加者の人数や使用された電子的インフォームドコンセント文書書式の版数についての概要が把握できるようにすること。電子システム内にある、個人を特定できる情報へのリモートアクセスは、当該参加者、法定代理人、治験責任医師、モニター、監査人、又は治験責任医師にのみ許可すべきである。正当化できないアクセスにより匿名化されていない情報がさらされてしまうといった結果につながる場合、個人データ保護法の侵害と見なされる可能性がある。

A5.3.5 Trial participant confidentiality (治験参加者の機密性)

As for all other computerised systems in clinical trials, the confidentiality of data that could identify trial participants should be protected, respecting the privacy and confidentiality rules in accordance with applicable national and EU regulatory requirements.	治験における他のすべてのコンピュータ化システムと同様に、適用される国内及び EU の規制要件に従った個人情報及び機密保持の規則を尊重し、治験参加者を特定できるデータの機密性を保護すべきである。

A5.3.6 Trial participant access (治験参加者のアクセス)

Potential trial participants (or, where applicable, their legal representative) should be provided with access to written information about the clinical trial prior to seeking their informed consent. The trial participant should be provided with their own copy of the informed consent documentation (including all accompanying information and all linked information) once their consent has been obtained. This includes any changes to the data (documents) made during the process.	潜在的な治験参加者 (又は、該当する場合はその法定代理人) に対して、インフォームドコンセントを求める前に、治験に関する書面情報へのアクセスを提供すること。同意が得られたら、インフォームドコンセント文書 (すべての付属情報及びすべてのリンクされた情報を含む) の治験参加者用コピーを治験参加者に提供すること。そこにはプロセスの過程で発生したデータ (文書) のすべての変更も含まれる。
The information about the clinical trial should be a physical hard copy or electronic copy in a format that can be downloaded. The copy should be available immediately to the trial participant.	治験に関する情報は、物理的なハードコピー又はダウンロード可能なフォーマットの電子コピーとする必要がある。コピーは、治験参加者が即座に入手できるようにすること。

A5.3.7 Investigator responsibilities (治験責任医師の責任)

The investigator should take appropriate measures to verify the identity of the potential trial participant (see section A5.3.3) and ensure that the participant has understood the information given. The informed consent documents are essential documents that should be available at the trial site in the investigator TMF for the required retention period (see section A5.3.9). The investigator should retain control of the informed consent process and documentation (e.g. signed informed consent forms) and ensure that personal identifiable data are not inappropriately disclosed beyond the site. The system used should not limit the investigator's ability to ensure that trial participants' confidentiality is protected with appropriate access and retention controls in the system. The investigator should ensure an appropriate process for the copy of the informed consent documentation (information sheet and signed consent form) to be provided to the trial participant. All versions of signed and dated electronic consents should be available to the trial participant for the duration of and after the trial. The system used should ensure that the investigator can grant and revoke access to the electronic informed consent system to monitors, auditors and regulatory authority inspectors.	治験責任医師は、潜在的な治験参加者の本人確認を行うための適切な手段 (A5.3.3 章を参照) を講じるとともに、参加者が与えられた情報を理解していることを確実にすること。インフォームドコンセント文書は必須文書であり、治験実施施設において、必要な保存期間 (A5.3.9 章を参照) を通じて、治験責任医師の TMF で利用できるようにすること。治験責任医師は、インフォームドコンセントプロセスと文書 (例：署名済みのインフォームドコンセント書式) をコントロールし、個人を特定できるデータが治験実施施設外に不適切に開示されないようにする必要がある。治験責任医師は〔記録への〕アクセスと保存についての適切なシステムコントロールを保持し、治験参加者の機密性を確実に保護する必要があるが、使用するシステムはその能力を制限するものであってはならない。治験責任医師は、インフォームドコンセント文書 (情報シート及び署名付き同意書) のコピーを治験参加者に提供する適切なプロセスを確実にすること。治験期間中及び治験終了後を通じて、〔いつでも〕治験参加者が、署名と日付の記入された電子的インフォームドコンセント文書のすべてのバージョンを入手できるようにすること。使用するシステムでは、治験責任医師が、モニター、監査者、及び規制当局の査察官に対して電子的インフォームドコンセントシステムへのアクセスを、許可及び取り消しできるようにすること。

A5.3.8 Version control and availability to sites (バージョンコントロールと治験実施施設)

The electronic informed consent information (electronic trial participant information and informed consent form) may be subject to updates and changes during the course of the trial. Regardless of the nature of the change or update, the new version containing relevant information has to receive the favourable opinion/approval of the ethics committee(s) prior to its use. Additional information should be made available to the ethics committee(s) concerning technical aspects of the electronic informed consent procedure to ensure continued understanding of the informed consent processes. Only versions approved by the ethics committee(s) should be enabled and used for the informed consent process and documentation. Release of electronic trial participant information and informed consent forms to the sites prior to IRB/IEC approval should be prevented. The system should prevent the use of obsolete versions of the information and informed consent document.	電子的インフォームドコンセントの情報 (電子的な治験参加者情報及びインフォームドコンセント書式) は、治験の過程で更新及び変更される可能性がある。変更又は更新の性質に関係なく、関連情報を含む新しいバージョンを使用する前に、倫理委員会の好意的な意見/承認を受けなければならない。電子的インフォームドコンセント手順の技術的側面に関する追加情報を倫理委員会に提供し、インフォームドコンセントプロセスについて継続的に理解が得られるようにすること。倫理委員会によって承認されたバージョンのみを有効にして、インフォームドコンセントプロセスと文書化に使用すること。電子的な治験参加者情報とインフォームドコンセント書式は、IRB/IEC の承認を得るまでは治験実施施設に公開しないようにすること。システムでは、古いバージョンの情報やインフォームドコンセント文書が使用されることを防ぐようにすること。

A5.3.9 Availability in the investigator's part of the trial master file (治験責任医師担当部分のTMFの可用性)

All documents of the informed consent procedure (including all accompanying information and all linked information) are considered to be essential documents and should be archived as such. Replacement of the documents with copies is only acceptable if the copies are certified copies (see section 6.5.).	インフォームドコンセント手順のすべての文書 (すべての付属情報及びすべてのリンクされた情報を含む) は、必須文書と考えられるため、然るべくアーカイブする必要がある。文書のコピーによる差し替えは、保証付きコピーの場合にのみ認められる (6.5 章を参照) 。

A5.3.10 Withdrawal from the trial (治験参加の同意撤回)

There should be procedures and processes in place for a trial participant to be able to withdraw their consent. If there is a possibility for the trial participant to withdraw from the trial through the computerised system, it should be ensured that such a withdrawal of consent generates an alert to the investigator in order to initiate the relevant steps as per protocol and according to the extent of withdrawal. Any withdrawal of informed consent should not affect the results of activities already carried out, such as the storage and use of data obtained on the basis of informed consent before withdrawal.	治験参加者が同意を撤回できるようにするための手順とプロセスを設けておくこと。治験参加者がコンピュータ化システムを介して治験参加を撤回する可能性があるのであれば、同意撤回のアラートが確実に発せられるようにして、治験責任医師が治験実施計画書に従って撤回の程度に応じた手順を開始できるようにする必要がある。〔同意が〕撤回されたとしても、撤回前のインフォームドコンセントに基づいて実施された活動結果 (取得されたデータ保存及び利用など) に影響を与えないようにすること。

Annex 6 Clinical systems (付属書 6 臨床システム)

As stated in sections 2. and 4.6., computerised systems implemented at the trial site are also within the scope of this guideline, and the general approach towards computerised systems used in clinical practice is that the decision to use a system in a clinical trial should be risk proportionate and justified pre-trial.	2 章及び 4.6 章で述べたように、治験実施施設に実装されているコンピュータ化システムも本ガイドラインの適用範囲に含まれており、臨床業務に用いるコンピュータ化システムに対する一般的なアプローチとして、そのシステムを治験で使用するかどうかの判断をリスクに応じたものとし、治験開始前に正当化する必要がある。
This section is dedicated to specific and additional considerations regarding electronic medical records and other systems implemented at sites, which are primarily used in clinical practice but are also generating clinical trial data.	本章では、主に診療の現場で用いられる一方で治験データも生成するような、治験実施施設に実装された電子医療記録及びその他のシステムについての特徴的かつ追加的な考慮事項について述べる。
For computerised systems built specifically for data collection in clinical trials please refer to the relevant sections of this guideline.	治験データ収集専用に構築されたコンピュータ化システムについては、本ガイドラインの関連章を参照のこと。

A6.1 Purchasing, developing, or updating computerised systems by sites
(治験実施施設によるコンピュータ化システムの購入／開発／アップデート)

The investigator/institution should have adequate facilities for a clinical trial. This also applies to the computerised systems of the institution if considered to be used for clinical trial purposes. It is recommended that institutions planning to perform clinical trials consider whether system functionality is fit for the clinical trial purpose. This should also be considered prior to the introduction of a new electronic medical record or equipment planned to be used in clinical trials (e.g. scanners, X-ray, electrocardiograms), or prior to changes to existing systems.	治験責任医師/治験実施医療機関は、治験のために十分な設備を備えている必要がある。このことは、医療機関のコンピュータ化システムを治験目的で使用することを考えている場合にも当てはまる。治験の実施を計画している医療機関には、システムの機能が治験の目的に合っているかどうかを検討することを勧める。このことは、治験で使用するための新しい電子医療記録や機器 (例：スキャナー、X 線、心電図) を導入する前、又は既存システムを変更する前に検討すること。
To ensure that system requirements related to GCP compliance (e.g. audit trail for an electronic medical record) are addressed, experienced clinical trial practitioners should be involved by the institution in the relevant steps of the procurement and validation processes.	GCP 適合に関連するシステム要件 (例：電子医療記録の監査証跡) に確実に対処するために、医療機関は、調達及びバリデーションのプロセスの必要な場面で、経験豊富な治験実務者を関与させること。
As many systems are designed with different configuration options, it should be ensured that the systems are configured in a GCP compliant manner.	多くのシステムではさまざまな構成設定の選択肢を提供するよう設計されているため、システムが GCP に適合した方法で構成設定されていることを確実にすること。

A6.2 Site qualification by the sponsor (治験依頼者による治験実施施設の適格性評価)

As part of the site qualification, the sponsor should assess the systems in use by the investigator/institution to determine whether the systems are fit for their intended use in the clinical trial (e.g. include an audit trail). The assessment should cover all computerised systems used in the clinical trial and should include consideration of the rights, safety, dignity and wellbeing of trial participants and the quality and integrity of the trial data. If the systems do not fulfil the requirements, the sponsor should consider whether to select the investigator/institution. The use of systems not fulfilling requirements should be justified, either based on planned implementation of effective mitigating actions or a documented impact assessment of residual risks.	治験依頼者は、治験実施施設の適格性評価の一環として、治験責任医師/治験実施医療機関が使用しているシステムのアセスメントを行い、システムが治験で意図した用途に適合しているかどうか (例：監査証跡があるか) を判断すること。アセスメントは、治験で使用されるすべてのコンピュータ化システムをカバーする必要があり、治験参加者の権利、安全、尊厳、健康、及び治験データの品質とインテグリティを考慮するものであること。 システムが要件を満たさない場合、治験依頼者はその治験責任医師/治験実施医療機関を選定するかどうかを検討すること。要件を満たさないシステムを使用する場合は、効果的なリスク低減措置の計画的な実施、又は残存リスクの影響の文書化されたアセスメントにより正当化すべきである。

A6.3 Training (トレーニング)

If the use of the systems in the context of a specific trial is different from the use in clinical practice e.g. different scanning procedures, different location of files, different requirements regarding documentation etc., trial specific training is required.	特定の治験におけるシステムの使用方法が臨床業務での使用方法と異なる場合 (例えば異なるスキャン手順、異なるファイル格納場所、異なる文書要件など) 治験固有のトレーニングが必要となる。

A6.4 Documentation of medical oversight (医学的監督についての記録)

The investigator should be able to demonstrate their medical oversight of the clinical trial when electronic medical records are used. Where all or part of the entries into the medical records are made by a research nurse/dedicated data entry staff it can be difficult to reconstruct the investigator's input. The system should allow the investigator to document the assessment and acknowledgement of information entered into the system by others.	電子医療記録が〔治験に〕利用される場合、治験責任医師は、治験について医学的な監督を行っていることを示す必要がある。医療記録への入力のすべて又は一部を研究看護師/データ入力専門スタッフが行う場合、治験責任医師による入力を再構築することは難しいかもしれない。システムでは、他者によってシステム入力された情報を治験責任医師がアセスメントし承認したことを記録できるようにすること。

A6.5 Confidentiality (機密性保持)

Pseudonymised copies of electronic medical records may be provided to sponsors, or service providers working on their behalf, outside the clinical environment e.g. if needed for endpoint adjudication or safety assessments according to the protocol. National regulations need to be followed by the sites. In such cases there should be: • procedures in place at the site to redact copies of medical records, in order to protect the trial participants' identity, before transfer; • security measures in place, which are relevant to the process, including pseudonymisation and redaction; • a copy of the pseudonymised records and a proof of the transfer made at the site; • organisational and technical procedures in place on the receiving side to ensure that the requirements of the data protection regulation are met.	例えば治験実施計画書に従って、エンドポイントの判定又は安全性評価に必要な場合など、電子医療記録の匿名化されたコピーが治験実施環境の外で治験依頼者又はその代理として働くサービスプロバイダに提供される場合がある。治験実施施設は国の規制に従う必要があり、次のようにする必要がある。 • 治験参加者の身元が割れないように、治験実施施設において、転送前に医療記録から名前を墨消しする手順を設ける。 • プロセスに関連する適切なセキュリティ方策を設ける。匿名化や編集など。 • 匿名化の記録のコピーと治験実施施設で転送を実施したことの証明を保持する。 • 受信側において、データ保護規則の要件が確実に満たされるようにするための組織的及び技術的手順を設ける。

Due to the sensitive nature of information documented in medical records, the extent to which sponsors request these data should be ethically and scientifically justified and limited to specific critical information. Any planned collection of redacted copies of medical records by the sponsor should be described in the protocol, or related documents, and should be explicit in the patient information.	医療記録に記録される情報は機密であるため、治験依頼者が要求するデータの範囲は、倫理的及び科学的に正当化され、かつ治験に関連する重要な情報に限定すべきである。治験依頼者が名前を墨消しした医療記録のコピーを計画的に収集するような場合は、そのことを治験実施計画書又は関連文書に記載する必要があり、患者〔向けの〕情報に明示すること。

A6.6 Security (セキュリティ)

Security measures that prevent unauthorised access to data and documents should be maintained. Please refer to section 5.4. regarding more details on the general requirements for security systems, which are equally applicable to research institutions.	データや文書へ許可のないアクセスを防止するセキュリティ方策を維持管理すること。 セキュリティシステムの一般的な要件の詳細については 5.4 章を参照のこと。これは医療機関にも同様に適用される。

A6.7 User management (ユーザー管理)

Robust procedures on user management should be implemented (see Annex 3). For systems deployed by the investigator/institution, the investigator should ensure that individuals have secure and attributable access appropriate to the tasks they are delegated to in the trial. Robust processes for access rights are particularly important in trials where parts of the information could unblind the treatment. Such information should only be accessible to unblinded staff.	ユーザー管理に関する堅牢な手順を実装すること (付属書 3 を参照)。 治験責任医師/治験実施医療機関が導入したシステムにおいて、治験責任医師は、各人が、それぞれ委任された治験のタスクに合った、安全で帰属性のあるアクセス権を持つことを確実にすること。 アクセス権についての堅牢なプロセスは、情報の一部が治療の盲検化解除につながってしまうような治験では特に重要である。このような情報は、盲検化の対象となっていない職員のみがアクセスできるようにすること。

A6.8 Direct access (直接アクセス)

Sponsor representatives (monitors and auditors) and inspectors should have direct, read-only access to all relevant data for all trial participants as determined by the monitors, auditors or inspectors while taking the collected data and the clinical trial protocol into account. This may require access to several different sections or modules of the respective (medical) record e.g. imaging. This requires the use of a unique identification method e.g. username and password.	治験依頼者の代表者 (モニター及び監査者) 及び査察官には、すべての治験参加者についての、すべての関連データへの直接の読み取り専用アクセス権を持たせるようにする。〔どのデータが必要かは〕モニター、監査者、又は査察官が、収集されたデータ及び治験実施計画書を考慮しながら決定する。そのため、それぞれの (医療) 記録の異なる部分や (例えば、画像などの) 別モジュールへのアクセスが必要になる場合があることから (例えば、ユーザー名とパスワードのような) ユニークな識別方法を用いる必要がある。
The access of monitors, auditors and inspectors should be restricted to the trial participants (including potential participants screened but not enrolled in the trial) and should include access to audit trails.	モニター、監査者、及び査察官がアクセスする対象は、治験参加者 (スクリーニングを通ったものの治験に登録されていない潜在的な参加者を含む) に制限すべきであり、アクセスを監査証跡に記録する必要がある。
If the site has accepted to provide remote access, appropriate security measures and procedures should be in place to support such access without jeopardising patient rights and data integrity and national legislation.	治験実施施設がリモートアクセスでの提供を認めているのであれば、適切なセキュリティ方策と手順を設けておき、患者の権利、データインテグリティ、及び国内法を脅かすことなくリモートアクセスをサポートできるようにすること。

A6.9 Trial specific data acquisition tools (治験固有のデータ収集ツール)

The electronic medical record contains information, which is crucial for the management of patients and are designed to fulfil legal requirements.	電子医療記録に含まれる情報は、患者の管理に不可欠であり、法的要件を満たすように設計されている。
Any trial specific data acquisition tools implemented cannot replace the medical record and their use should not result in a depletion of relevant information in the medical record.	治験固有のデータ収集ツールは医療記録に代わりうるものではなく、それを使用することで医療記録の関連情報を削除してしまうようなことがあってはならない。

Monitoring activities should not be limited to information in the data acquisition tools and should also consider relevant information in the medical record. Please also refer to the published qualification opinion on eSource Direct Data Capture (DDC) EMA/CHMP/SAWP/483349/2019.	モニタリング活動は、データ収集ツールの情報に限定せずに、医療記録の関連情報も考慮すること。 eSource Direct Data Capture (DDC) EMA/CHMP/SAWP/483349/2019 に関する公開された qualification opinion も参照のこと。

A6.10 Archiving (アーカイビング)

Appropriate archiving should be in place to ensure long term readability, reliability, retrievability of electronic data (and metadata), in line with regulatory retention requirements. Please also refer to section 6.11. Requirements for the retention of clinical trial data and documents are frequently different from requirements for other data and documents held by the investigators. It should be ensured that there is no premature destruction of clinical trial data in case of e.g. institution relocation or closure. It is the responsibility of the sponsor to inform the hospital, institution or practice as to when these documents will no longer need to be retained. There are specific requirements for backup, etc. of electronic data, which can be seen in section 6.8 and which are equally applicable to research institutions. Please also refer to the guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic) EMA/INS/GCP/856758/2018.	規制上の保存要件に沿って、電子データ (及びメタデータ) の長期的な見読性、信頼性、検索可能性を確実にするために、適切なアーカイブを実施すること。6.11 章も参照のこと。治験に関するデータ及び文書の保存要件は、往々にして治験責任医師が保持する他のデータ及び文書に対する要件とは異なる。例えば医療機関の移転又は閉鎖などの場合に、治験データが保存期間満了前に破棄されないようにする必要がある。これらの文書を保管する必要がなくなる時期を病院、医療機関、診療所に通知するのは治験依頼者の責任である。 電子データのバックアップなどについては 6.8 章に示す特定の要件があり、研究機関にも同様に適用される。guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic) EMA/INS/GCP/856758/2018 も参照のこと。 【訳注】Guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic) (EMA/INS/GCP/856758/2018) の和訳については、https://bunzen.co.jp/ 参照。