EudraLex The Rules Governing Medicinal Products in the European Union
Volume 4 EU Guidelines to Good Manufacturing Practice Medicinal Products for Human and Veterinary Use

Draft Annex 11
Computerised Systems

The Annex has been updated in response to the increased use of computerised systems and the increased complexity of these systems. Consequential amendments are also proposed for Chapter 4 of the GMP Guide.

Annex11はコンピュータ化システムの利用と複雑性の増加に対応し更新した。重要な修正案もGMPガイドの第4章に対して提案された。

Principle　原則

This annex applies to all forms of computerisation used in connection with regulated activities, including process control, documentation and data-processing systems. It also covers development, selection, validation and use of systems. For documentation, the requirements of GMP Chapter 4 shall also be considered.
The introduction of computerised systems into systems of manufacturing, (including storage, distribution, quality control) and other regulated GMP activities, does not alter the need to observe the relevant principles given elsewhere in the Guide. Where a computerised system replaces a manual operation, there should be no resultant decrease in product quality, process control or quality assurance. There should be no increase in the overall risk of product failure.
The validation of computerised systems should enable both the manufacturing authorisation holder, and competent authority, to have a high level of confidence in the integrity of both the processes executed within the controlling computer system(s) and in those processes controlled by and/or linked to the computer system(s).
For proprietary systems, where the supplier will have completed the development life-cycle independently then, depending on the nature of the intended application, the manufacturing authorisation holder/ purchaser may need to assess the development/ validation evidence for the product at the supplier.　(See also clauses 1, 2 and 6 below.)

本 annex はプロセスコントロール、文書化、データ処理システムなどを含む規制作業に関わるあらゆるコンピュータ化された形態に適用される。また、開発、選定、バリデーション、システムの利用も適用範囲である。文書化においては、GMP 第 4 章の要件もまた考慮されるべきである。

コンピュータ化されたシステムの製造システム（保管、物流、品質管理を含む）への導入とその他規制された GMP 活動においても他のガイドで記載された関連原則を遵守する必要性に変わりはない。マニュアルベースの作業をコンピュータ化する際に、結果として製品の品質プロセスコントロールすなわち品質保証を劣化させてはならない。製品欠陥の全般的リスクが増えてもいけない。

コンピュータ化システムのバリデーションは、製薬企業と規制当局両方が、制御のためのコンピュータシステムの中で実行されたプロセスと、コンピュータシステムに管理とリンクをするまたはその一方をするプロセス、両方の完全性において高水準の自信を持つことを可能にしなければならない。

サプライヤが独自にライフサイクルを完遂し開発するパッケージシステム（proprietary systems）では、意図されたアプリケーションのそのものに頼るため、製薬企業/購買者はサプライヤの製品の開発とバリデーションの証拠を調査する必要がでてくることもある。（下記 1、2、6 項も参照）

1. Risk Management　リスク管理

Decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system in respect to its impact on product quality and safety as well as data security and integrity.

バリデーションの拡張とデータの完全性管理に関する決定は、データのセキュリティと完全性同様、根拠を持ち文書化された製品の品質への影響と安全性に関するコンピュータ化システムのリスク評価に基づいていなければならない。

2. Personnel　要員

It is essential that there is the closest co-operation between key personnel, such as users, system administrators, quality assurance and technical staff (both in-house and outsourced) involved with the development, validation, management and use of computerised systems. Persons performing such roles should have appropriate and documented qualifications, training, technical expertise, responsibilities and experience to carry out their assigned duties.

コンピュータ化システムの技術開発、バリデーション、管理、利用に関わるユーザ、システム管理者、品質保証、テクニカルスタッフ（社内と外注の両方）の様なキーとなる要員の間で密に協力し合うことは重要である。

そのような役割を実行する者は、適切かつ文書化された検証、教育、専門技術、責任、割り当てられた任務を果たすための経験を持たなければならない。

3. Validation　バリデーション

The manufacturing authorisation holder's quality management system will need to include policies and plans for the validation of computerised systems, together with up to date listings of systems and their GxP functionality. The validation status of each system should be clear from the Validation Schedule. The extent of validation necessary will depend on the type and complexity of the computerised systems and the manufacturing authorisation holder's documented risk assessments.

製薬企業の QMS（品質管理システム）には、コンピュータ化システムのバリデーションに関するポリシーと計画を含む必要があり、さらに最新の状態に更新されたシステム一覧表とそれらシステムが持つ GxP 関連の機能の一覧表も必要である。

各システムのバリデーション状態は、バリデーションスケジュールによって明らかにしなければならない。

バリデーションの必要性の拡張は、コンピュータ化システムのタイプと複雑性、製薬企業の文書化されたリスク評価に依存するであろう。

For the validation of bespoke or significantly customised computerised systems there should be a process in place that assures the formal assessment and reporting of quality and performance measures for all the life-cycle stages of software and system development, its implementation, qualification and acceptance, operation, modification, re-qualification, maintenance, on-going support and retirement. (With regards to customised systems, the above described controls are required for customisation aspects and their impacts on the whole system)

注文開発または大幅にカスタマイズされたコンピュータ化システムのバリデーションにおいては、公式な品質と性能の調査と報告、ソフトウェアとシステム開発の全ライフサイクル段階の基準、実施、検証と受け入れ、運用、変更、再検証、保守、継続サポート及び廃棄を保証するプロセスが整ってなければならない。（カスタマイズされたシステムに関しては、上記の管理要件はカスタマイズ要件とシステム全体への影響に応じて必要とされる）

The validation documentation should cover all the relevant steps of the specific project life cycle with appropriate methods for measurement and reporting, (e.g. assessment reports and details of quality and test measures), as required. User requirements should be traceable throughout the validation process/ life cycle. Manufacturing authorisation holders should be able to justify and defend their standards, protocols, acceptance criteria, procedures and records in the light of their own documented risk and complexity assessments, aimed at ensuring fitness for purpose and regulatory compliance.

バリデーション文書には、プロジェクトのライフサイクルの全ステップにおいて、適切な基準と報告（例・評価報告書、品質の詳細、テスト基準）のための適切な方法論を含めなければならない。
ユーザ要件は、バリデーションの全プロセス/ライフサイクルを通してトレーサブル（追跡可能）でなければならない。
製薬企業は、標準、計画書（protocol）、受入基準、文書化されたリスクを考慮した手順と記録、複雑性の評価、目的への適合の保証、規制要件遵守に関して、正当化し主張できなければならい。

Validation documentation should include change control and error log records generated during the validation process.

バリデーション文書には､バリデーションプロセス中に発生した変更とエラーログの記録を含まなければならない。

With regard to the testing phase of the validation process:
-Automated testing tools used for validation purposes should be assessed for their adequacy.
- Evidence of challenge testing should be included, particularly system parameter limits, data limits and error handling.

バリデーションプロセスにおけるテストフェーズに関して
- バリデーション目的に使用された自動テスト機器はその適正を調査されなければならない。
- 限界テストの証拠、特にシステムパラメータ範囲、データ範囲、エラー処理が含まれなければならない。

In fitting with best practices for risk assessment and change management, the manufacturing authorisation holder should carry out periodic reviews of computerised systems to determine whether incremental change, system performance issues, or regulatory developments prompt work to reconfirm validation or data integrity. Such reviews should include the current range of functionality, error logs, upgrade history, performance, reliability, security and validation status reports.

最適なリスク評価と変更管理の実行に合致させるため、製薬企業は、変更の増分、システムの性能の問題、バリデーション及びデータの一貫性を再確認するためのすみやかな規制の発展、を決定するためにコンピュータ化システムの定期的レビュを行わなければならない。このようなレビュは現行の一連の機能、エラーログ、最新の履歴、実績、信頼性、セキュリティ、バリデーション状況の報告、を含まなければならない。

Mechanisms for ensuring data integrity in terms of accuracy and reliability(e.g. macros for check of data logic; table field design etc)

- Provisions for data security (access control, views, and internal encryption mechanisms)
- Transaction control/protocols (particularly important with regard to distributed databases)
- Linkages between different databases (the software developed for linking different propriety databases)
- Recovery Mechanisms (recovery of a database to its consistent state after a failure)
- Load testing (to include the current needs and future growth of the database)
- Provisions for post-implementation monitoring of system's performance and growth of the database

- On line archiving of data where applicable

データベースベース及びデータベースを持つシステムのバリデーションは以下を含まなければならない。

- 正確性と信頼性の見地からデータの完全性を保証するメカニズム（例・データロジックをチェックするマクロ、テーブルフィールド設計等）
- データのセキュリティ提供（アクセス制限、閲覧、内部の暗号化メカニズム）
- トランザクションコントロール／プロトコル（分散データベースに関しては特に重要である）
- 異なるデータベース間のリンク連携（リンクした異なる正当性のあるデータベースのために開発されたソフトウェア）
- 復旧構造（故障後のデータベースの一貫した状態への復旧）
- ロードテスト（データベースの現在のニーズと将来的拡張を含むための）
- 次期導入システムの性能とデータベースの拡張のモニタリング提供
- 該当する場合、データのオンライン保管

Spreadsheets should be suitably checked for accuracy and reliability and stored in a manner which ensures the appropriate version control. The calculations should be secured in such a way that formulations are not intentionally or accidentally overwritten. The calculations should be executed with precision displayed on the screen or in reports. Formulations should also be protected from accidental input of in appropriate data type (e.g. text in a numeric field and or a decimal format into integer field).

表計算ソフトは正確性と信頼性を適切に調査され、適切なバージョン管理を保証する方法で保存されなければならない。計算結果はフォーミュレーションが意図的にまたは偶発的に上書きされることがないような方法で保護されなければならない。計算は表示画面上または報告書中で正確さをもって実行されなければならない。フォーミュレーションはまた偶発的な適切なデータタイプの入力から守られなければならない。（例・計算分野または小数フォーマットから整数フィールドへのテキスト）

4. System　システム

An inventory, or listing, of all computerised systems is essential. The inventory should mention the site and purpose of the computerised system. This list should indicate the risk assessed category of each system. Systems that have an influence on regulated activities need to be identified... Manufacturing authorisation holders will need to maintain records detailing the physical and logical arrangements and the infrastructure for controlled, secure environments, together with up to date written detailed descriptions of each system, data flows and interactions with other systems or processes. These should be treated as controlled documents.

全てのコンピュータ化システムの目録、または一覧は必要不可欠である。目録はコンピュータ化システムの位置と目的について示さなければならない。この一覧は各システムのリスク評価区分を示さなければならない。規制活動に影響があるシステムは識別される必要がある…製薬企業は物理的、論理的取り決めと管理されるインフラを詳細にする記録を維持し、環境と一緒に最新の各システムの詳細説明の記述、データフローと他システムまたはプロセスとの連関を確保する必要がある。これらは管理された文書として扱われなければならない。

specifications should be available (including diagrams as appropriate). They should describe the required functions of the system, any modularity and their relationships, its interfaces and external connections, system boundaries, main inputs and outputs, main data types stored, handled or processed, any hardware and software pre-requisites, and security measures. Attention should be paid to the siting of computer hardware in suitable conditions where extraneous factors cannot interfere with the system operation.

現在の仕様書は入手可能（必要に応じてダイアグラムを含む）でなければならない。仕様書にはシステムの要求される機能、モジュール方式とその関係、インターフェースと外部とのコネクション、システム境界、メイン入力及び出力、保存、使用、すなわち処理されたメインデータタイプ、ソフトウェアとハードウェアの前要件、セキュリティ基準が記述されなければならない。ハードウェアコンピュータの外部要素がシステム運用を疎外しない適切な状態への設置には注意が払われなければならない。

5. Software　ソフトウェア

The software is a critical component of a computerised system. The user of such software should take all reasonable steps, to ensure that it has been produced in accordance with an appropriate system of Quality Assurance. The supplier of software should be qualified appropriately; this may include assessment and/ or audit.

ソフトウェアはコンピュータ化システムの重要なコンポネントである。このようなソフトウェアのユーザは品質保証の適切なシステムに従って製造した事を証明するために正当な段階を踏まなければならない。ソフトウェアのサプライヤは適切に検証されなければならない、これには評価と監査両方またはその一方が含まれることもある。

Computerised systems should be designed and developed in accordance with an appropriate quality management system. Documentation supplied with Commercial Off-The-Shelf products should be reviewed by manufacturing authorisation holders to check that user requirements are fulfilled.

コンピュータ化システムは適切な品質管理システムに従って設計・開発されなければならない。業務用既成製品で提供された文書はユーザ要件を満たしているかチェックするために製薬企業によってレビュされなければならない。

Quality system and audit information relating to suppliers or developers of software and systems implemented by the manufacturing authorisation holder should be made available to inspectors on request, as supporting material intended to demonstrate the quality of the development processes.

製薬企業により導入された品質システムとソフトウェアとシステムのサプライヤとデベロッパに関係する監査情報は開発プロセスの品質の証明を意図したサポートマテリアルとしての査察官の要求に答えられるよう作成されなければならない。

6. Data　データ

The system should include, where appropriate, built-in checks for the correct, secure entry and processing of data, including data transcribed manually from other media, or systems e.g. laboratory notebooks, or reports from other systems or instruments, that are not directly interfaced with the computerised system. Data and document management control systems should be designed to ensure the integrity of data and irrefutable recording of the identity of operators (i.e. shared passwords are disallowed) entering or confirming data as well as the routing and source of data captured or received automatically. Critical systems should be designed and protected to ensure that data and files cannot be changed without appropriate authorisations and with immutable electronic logs recording changes made even at the highest level of access, such as System Administrator.

システムは必要に応じて、内蔵訂正チェック、他メディア及びシステムから手入力で転写されたデータを含むデータの入力と処理の保護、例えば研究室のノート及びコンピュータ化システムに直接適合しない他システム及び機器からの報告を含まなければならない。データと文書の管理システムは、データの完全性とデータの入力及び確定の際のオペレーターの身元の反論の余地のない記録（すなわち共有パスワードは許されない）を自動的に取得及び受け取ったデータのルーティングと情報源同様に保証する設計でなければならない。重要なシステムはデータとファイルが適

切な許可と不変のシステムアドミニストレーターの様な最高レベルのアクセス電子的ログ記録なしには変更されないということを保証するための設計と保護がされなければならない.

7. User testing and the system's fitness for purpose　ユーザテストとシステムの目的への適合性

Before a new, replacement or upgraded computerised system is brought into use, it should have been thoroughly specified, documented, validated, tested and approved as per the foregoing sections of this annex. User staff should also have received documented effective training in the use of such systems (Annex 15 also provides some advice on user acceptance testing). When manual or pre-existing computerised systems are being replaced, it may be appropriate to undertake comparative 'parallel', or 'in-series' testing.

新たに置換及びアップグレードされたコンピュータ化システムは利用段階なる前に、この annex 前述のセクションごとに完全に specified、文書化、バリデーション、テスト、承認、されなければならない。ユーザ社員はまたこのようなシステムの利用に当たって文書化された効果的訓練を受けなければならない（Annex15 はまたユーザ受入テストに助言を提供している)。マニュアル作業及び現在するコンピュータ化システムが切り換わるとき、相対的に同等または連続するテストを引き受けるのが適当であるであろう。

8. Security　セキュリティ

Physical and/or logical controls should be in place to restrict access to computerised systems to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.

物理的、論理的、両方またはその一方の管理はコンピュータ化システムへの資格所持者へのアクセスを規制するために整えなければならない。不正エントリーを防ぐ適切な方法には鍵、パスカード、パスワードを伴う個人コード、バイオメトリックス、コンピュータ機器とデータ保管場所への規制アクセスなどの利用が含まれる事もある。

Access to applications, folders, files and data should be controlled via the permissions detailed within the manufacturing authorisation holder's Information Security Management System (ISMS) (See Chapter 4 in the GMP Guide and also current PI011 from PIC/S).

アプリケーション、フォルダー、ファイル、データへのアクセスは製薬企業の情報セキュリティ管理システム（ISMS）（GMP ガイド第 4 章と PIC/S の current PI011 も参照）にて詳細にされた許可経由で管理されなければならない。

Suitable methods, commensurate to the criticality of data, should be in place to deter and record unauthorised entry and/or or modifications of data. These methods may include time limiting logging, encryption, and re-entry of unique identifier for critical data.

データの重要性に比例した適切な方法は不正エントリーとデータ変更の両方またはその一方を阻止し記録するために整えられなければいけない。これらの方法はログイン時間制限、暗号化、重要なデータへの独自の識別の再エントリーが含まれることもある。

Within the ISMS there should be a defined procedure, that would enable tracking and where possible audit trailing for the issue/alteration, and cancellation of authorisation to system/application/data access.

ISMS ではトラッキング、可能であれば入力・改ざんの監査証跡とシステム、アプリケーション、データアクセスの承認取り消しを可能にする手順が定義されなければいけない。

Mechanisms for the detection of attempts of unauthorised access, to the system, files and data should be considered based on a risk assessment so that appropriate action may be taken.

システム、ファイル、データへの不正アクセスの試みの発見メカニズムは適切な行動がとれるようリスク評価に基づき考察されなければならない。

9. Accuracy Checks　セキュリティセキュリティチェック

For critical data entered manually or transferred from another system (for example the weight and batch number of an ingredient during dispensing, or the keying in of laboratory data), there should be an additional check on the accuracy of the record which is made prior to further processing of these data. This check may be done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be evaluated in a risk assessment and as part of validation. (See also sections 7 to 9 above)

他のシステムから手入力または移動された重要なデータにおいては（例えば調剤中の材料の重量とバッチ番号、及び研究データの keying in）、それらのデータの追加処理をする前の記録の正確さを追加チェックしなければならない。重要性と間違った及び不正確なシステムへの入力により見込まれる結果はリスク評価とバリデーションの一環として評価されなければならない。（上記 7 節～9 節も参照）

If a computerised system controls a critical process (where criticality determination is based on the risk assessment, as documented by a manufacturing authorisation holder), an independent secondary check of critical parameters of such a process should be in place.

コンピュータ化システムが重要なプロセスを管理する場合（重要な決定が製薬企業により文書化されたリスク評価の場合）、そのようなプロセスの重要なパラメータの独立した二次的チェックが整っていなければならない。

10. Audit Trails　監査証跡

The system should enable the recording of the unique identity of operators entering or confirming critical data. Any entry or alteration of critical data should be authorised and recorded with the reason for the change. Consideration should be given to building into the system the creation of a complete record of all entries and amendments (a system generated "audit trail"). (See also sections 7 to 10 above and Chapter 4 (4.9)) Audit trails need to accurately reflect changes. (For example if a relevant electronic record is created using a number of data fields, all these data fields need to be linked within the audit trail. The aim is to know at any given time point what the information was.) Audit trails need to be available and convertible to human readable form.

システムは重要なデータを入力、確定したオペレーターの独自の身元の記録を可能にしなければならない。全ての重要なデータの入力と変更は許可され変更の理由と共に記録されなければならない。全ての入力と修正の完全な記録を作成するシステム（‘監査証跡’を残したシステム）の確立は考慮されるべきである。（上記 7 項から 10 項と第 4 章（4.9）も参照）監査証跡は正確に変更を反映する必要がある。（例えば該当する電子記録が多数のデータフィールドを利用して作成された場合、これらの全てのデータフィールドは監査証跡の中でリンクされなければならない。その目的とは情報を得た全てのタイムポイントを把握することである）監査証跡は入手可能で人が読める形に出力可能でなければならない。

11. Signatures　署名

Electronic records may be signed electronically or by applying a hand-written signature to a printed copy of the record. This is only acceptable if all relevant meta- data is included in the printout. Electronic signatures and identification by biometric means are expected to:

- be legally equivalent to hand-written signatures,
- be linked to their respective record,
- include the time and date that they were applied.

電子記録には、電子署名か、印刷した紙媒体に手書き署名が付されているかもしれない。
これは全ての該当メタデータが印刷に含まれている場合にのみ認められる。
電子署名とバイオメトリックス方式による識別には以下を要求する。

- 手書き署名と法的に同等であること
- 各記録にリンクしていること
- 署名された時間と日付を含むこと

Country specific national legislations may apply to the requirements and controls for electronic records and linked electronic signatures, or identities. Printed copies of electronically compiled and electronically signed documents should be traceable via printed links to the original electronic transaction.　(See also section 20, below)

国毎の法律は、電子記録とリンクした電子的署名の要件と管理、及び識別に適応される可能性がある。
電子的に編集した文書に電子的に署名が付したものを印刷した紙媒体は、印刷されたリンクによって、オリジナルの電子トランザクションを追跡できなければならない。

12. Change control and configuration management　変更管理とコンフィグレーション管理

Alterations to any component of a computerised system should only be made in accordance with a defined procedure within the manufacturing authorisation holder's Change and Risk Management policies/procedures. These should include provision for the evaluation of the impact of the change on product quality and data and system integrity, scoping any necessary validation work, reporting, reviewing approving and implementing the change.

製薬企業のリスク管理と変更管理のポリシー／手順のなかで定められた手順に従ってのみ、コンピュータ化システムの全てのコンポネントの変更はされなければならない。

13. Printouts　印刷物

Printouts of records must indicate if any of the data has been changed since the original entry. For complex systems it may also be necessary for inspectors to be able to access and study electronic systems records on-line (e.g. databases, chromatography, process control, etc.).

記録の印刷は、オリジナルの入力からデータに変更があったかどうかを示すものでなければならない。
複雑なシステムの場合、査察官がオンラインでシステムの電子記録（例えば、データベース、クロマトグラフィ、プロセスコントロール等）にアクセスし、調査できることが必要となるかもしれない。

14. Data Storage　データ保管

Data should be secured by both physical and electronic means against wilful or accidental damage, in accordance with item '4.9' of the Guide and the manufacturing authorisation holder's information security management requirements. The storage media used should have been subjected to evaluation for quality, reliability and durability by or on behalf of the manufacturing authorisation holder. Stored data should be checked for accessibility, durability, readability and accuracy. The mechanism of checking should not present a risk to the current data on the system. If changes are proposed to the computer equipment or its programs, the above mentioned checks should be performed at a frequency appropriate to the storage medium being used. Access to data must be ensured throughout the retention period.

データは、ガイドの'4.9'項や製薬企業の情報セキュリティ管理要件に従って、物理的、電子的手段両方によって故意または偶発的なダメージから保護しなければならない。

利用される保存メディアは、品質、信頼性、耐久性の評価を、製薬企業（または代理となる者）によって受けなければならない。

保管したデータは、アクセス可能性、耐久性、見読性、正確性をチェックしなければならない。

チェックのメカニズムは、システム上の現在のデータに対してリスクを与えてはならない。

コンピュータ機器及びプログラムに変更が計画される場合、利用する保存媒体に適する頻度で、上記のチェックを実施しなければならない。データへのアクセスは、全保存期間を通して保証しなければならない。

15. Back Up; Migration; Archiving; Retrieval　バックアップ、移行、保管、復旧

Regular backups of all relevant data should be done. Back-up data should be stored at a separate and secure location. Integrity and accuracy of back-up data should be checked during or on completion of the back-up process.

該当する全てのデータは定期的バックアップされなければならない。バックアップデータは、離れた安全な場所に保管しなければならない。バックアップデータの完全性と正確性は、バックアッププロセス中または完了時にチェックしなければならない。

If the system does not have a capacity to retain records for the period specified in chapter 4, then the data must be suitably archived. The archived data should be secured by physical and/or electronic means against wilful and/or accidental damage. This data should be checked for accessibility, durability, readability and integrity. If changes are made to the computer equipment or its programs, then the ability to restore the data should be checked.

4 章で特定した期間、システムが記録を保持できる能力（Capacity）を持たない場合、データは適切に保管されなければならない。

保管データは物理的、電子的の両方またはその一方の方法で、故意または偶発的によるダメージから保護されなければならない。このデータはアクセス可能性、耐久性、見読性、完全性をチェックされなければならない。

コンピュータ機器またはプログラムに変更が加えられた場合、データがリストアできることをチェックしなければならない。

Backup, archiving, retrieval and restoration (recovery) practices need to be defined, tested and established in accordance with the manufacturing authorisation holder's QMS, ISMS and risk management requirements.

バックアップ、保管、修正、修復（復旧）の実行は製薬企業の QMS 、ISMS、リスク管理要件に従って定義され、テストされ、確立されなければならない。

16. Business Continuity　業務の継続性

For the availability of computerised systems supporting critical regulatory or lifesaving processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system). The time required to bring the alternative arrangements into use should be minimal and appropriate for a particular system. These arrangements should be adequately documented and tested.

重要な規制及び救命プロセスをサポートするコンピュータ化システムの安定供給においては、システムが故障した際のプロセスの継続的サポートを保証する準備をしなくてはならない（例えば手動及び代替のシステム）。代替の処置が利用段階に至るまでの要求される時間は特定のシステムに対して最小限かつ適切でなければならない。これらの処置は適切に文書化かつテストされなければならない。

17. Incident Management　障害管理

System failures and data errors should be tracked, recorded, analysed and corrective actions should be implemented as appropriate. Any procedures to be followed if the system fails or breaks down should be defined and verified.

システム障害とデータエラーは追跡、記録、分析され、必要に応じて修正措置を導入するべきである。システム障害及び故障があった場合に従うべき全ての手順は定義と確認をされなければならない。

18. Suppliers　サプライヤ

When outside agencies, suppliers, or other parties are used to provide, install, configure, integrate, validate, maintain or modify a computerised system or related service or for data processing, there should be a formal agreement including a clear statement of the responsibilities of that outside body.

外部のエージェンシー、サプライヤ、及び他の団体をインストール、設定、integrate、バリデーション、コンピュータ化システムの維持及び変更、及び関係サービス、及びデータ処理をするために利用した場合、外部団体の責任の明確な記述を含む公式の取り決めがなければならない。

As the holder of the Manufacturing Authorisation must ensure that the medicinal product(s) is fit for its intended use, the competence and reliability of a supplier are key factors when selecting a product or service provider. The need for a supporting audit should be based on a risk assessment (in respect to the system's impact on product quality and safety, as well as data security and integrity) to determine whether the computerised system has been designed and developed, and is maintained, in accordance with an appropriate quality management system. Ongoing technical support from suppliers should be documented in a written contract.

製薬企業は医療用製品が意図された利用に合致することを保証しなくてはならないので、製品およびサービスプロバイダを選ぶ際サプライヤの適正と信頼性は鍵となる要素である。供給される監査の必要性はコンピュータ化システムが適切な品質管理システムに従って設計、開発、維持されているか決定出来るようリスク評価（データのセキュリティと完全性同様、システムの製品の品質・安全性への影響に関する）に基づいていなければならない。サプライヤからの継続技術サポートは書面による契約に文書化されなければならない。

19. Batch Release　バッチリリース

When the release of batches for sale or supply is carried out using a computerised system, the system should allow for only a Qualified Person to certify the release of the batches and it should clearly identify and record the person releasing the batches. Any certification produced by computerised systems should be clearly cross-linked to the identity of the certifying person. Names should be clearly stated and transactions traceable for verification or audit purposes from both the electronic records and paper printouts- to time, date, context and identities (human or electronic source) for all GMP related transactions.

バッチの販売及び提供のリリースがコンピュータ化システムを利用してされた場合、そのシステムは有資格者にのみバッチリリースを認定することを許し、バッチをリリースした者の身元を明らかにし記録しなければならない。全てのコンピュータ化システムによって作成された認証は明確に認証者の身元にクロスリンクしなければならない。名前は明確に記述され、また業務は評価及び監査目的に対して、GMP 関係の業務に対する電子記録と紙への印刷物両方から、時間、日付、前後関係、識別（人物及び電子情報源）いたるまで、対監査性がなければならない。

Further guidance on security considerations and risk management in regulated applications will be found in PIC/S publication PI011-1 (August 2003) 'Good practices for computerised systems in 'GxP' regulated environments' and in ISO 17799 'A code of practice for information security management'.

規制アプリケーションでのセキュリティ考慮とリスク管理の更なるガイダンスは PIC/S の出版 PI011-1「GxP 規制環境においてのコンピュータ化システムの Good practices」（2003 年 8 月出版）と ISO 17799「実行コードの情報セキュリティ管理」の中に見つかります。

Industry best practice publications are available from ISPE (International Society of Pharmaceutical Engineers), PDA (Parenteral Drug Association),and other sources. PIC/S guidance on the validation of these systems and other matters will be found in PI011-1 'Good Practices for Computerised Systems in Regulated 'GxP' Environments'

業界の best practice の出版物は ISPE（国際製薬技術協会）、PDA（非経口製剤研究協会）、また他の情報源等から入手可能である。これらのシステムとその他の件についての PIC/S ガイダンスは「GxP 規制環境においてのコンピュータ化システムの Good practices」の中に見つかります。

In the context or electronic records the term 'written' means 'recorded, or documented on media, paper, electronic or other substrate'.

電子記録またはその文脈においては「written」は「記録された、またはメディア、紙、電子及びその他被印刷物に文書化されたもの」を意味する。