Annex 5

Guidance on good data and record management practices

Background

During an informal consultation on inspection, good manufacturing practices and risk management guidance in medicines' manufacturing held by the World Health Organization (WHO) in Geneva in April 2014, a proposal for new guidance on good data management was discussed and its development recommended. The participants included national inspectors and specialists in the various agenda topics, as well as staff of the Prequalification Team (PQT)–Inspections.

The WHO Expert Committee on Specifications for Pharmaceutical Preparations received feedback from this informal consultation during its forty-ninth meeting in October 2014. A concept paper was received from PQT–Inspections describing the proposed structure of a new guidance document, which was discussed in detail. The concept paper consolidated existing normative principles and gave some illustrative examples of their implementation. In the Appendix to the concept paper, extracts from existing good practices and guidance documents were combined to illustrate the current relevant guidance on assuring the reliability of data and related GXP (good (anything) practice) matters. In view of the increasing number of observations made during inspections that relate to data management practices, the Committee endorsed the proposal.

Following this endorsement, a draft document was prepared by members of PQT–Inspection and a drafting group, including national inspectors. This draft was discussed at a consultation on data management, bioequivalence, good manufacturing practices and medicines' inspection held from 29 June to 1 July 2015.

A revised draft document was subsequently prepared by the authors in collaboration with the drafting group, based on the feedback received during this consultation, and the subsequent WHO workshop on data management.

Collaboration is being sought with other organizations towards future convergence in this area.

1. Introduction

1.1 Medicines regulatory systems worldwide have always depended upon the knowledge of organizations that develop, manufacture and package, test, distribute and monitor pharmaceutical products. Implicit in the assessment and review process is trust between the regulator and the regulated that the information submitted in dossiers and used in day-to-day decision-making is comprehensive, complete and reliable. The data on which these decisions are based should therefore be complete as well as being attributable, legible, contemporaneous, original and accurate, commonly referred to as "ALCOA".

1.2 These basic ALCOA principles and the related good practice expectations that assure data reliability are not new and much high- and mid-level normative guidance already exists. However, in recent years, the number of observations made regarding good data and record management practices (GDRP) during inspections of good manufacturing practice (GMP) (*1*), good clinical practice (GCP) and good laboratory practice (GLP) has been increasing. The reasons for the increasing concern of health authorities regarding data reliability are undoubtedly multifactorial and include increased regulatory awareness and concern regarding gaps between industry choices and appropriate and modern control strategies.

1.3 Contributing factors include failures by organizations to apply robust systems that inhibit data risks, to improve the detection of situations where data reliability may be compromised, and/or to investigate and address root causes when failures do arise. For example, organizations subject to medical product good practice requirements have been using validated computerized systems for many decades but many fail to adequately review and manage original electronic records and instead often only review and manage incomplete and/or inappropriate printouts. These observations highlight the need for industry to modernize control strategies and apply modern quality risk management (QRM) and sound scientific principles to current business models (such as outsourcing and globalization) as well as technologies currently in use (such as computerized systems).

1.4 Examples of controls that may require development and strengthening to ensure good data management strategies include, but are not limited to:

- a QRM approach that effectively assures patient safety and product quality and validity of data by ensuring that management aligns expectations with actual process capabilities. Management should take responsibility for good data management by first setting realistic and achievable expectations for the true and current capabilities of

a process, a method, an environment, personnel, or technologies, among others;

- monitoring of processes and allocation of the necessary resources by management to ensure and enhance infrastructure, as required (for example, to continuously improve processes and methods, to ensure adequate design and maintenance of buildings, facilities, equipment and systems; to ensure adequate reliable power and water supplies; to provide necessary training for personnel; and to allocate the necessary resources to the oversight of contract sites and suppliers to ensure adequate quality standards are met). Active engagement of management in this manner remediates and reduces pressures and possible sources of error that may increase data integrity risks;
- adoption of a quality culture within the company that encourages personnel to be transparent about failures so that management has an accurate understanding of risks and can then provide the necessary resources to achieve expectations and meet data quality standards: a reporting mechanism independent of management hierarchy should be provided for;
- mapping of data processes and application of modern QRM and sound scientific principles throughout the data life cycle;
- ensuring that all site personnel are kept up to date about the application of good documentation practices (GDocP) to ensure that the GXP principles of ALCOA are understood and applied to electronic data in the same manner that has historically been applied to paper records;
- implementation and confirmation during validation of computerized systems and subsequent change control, that all necessary controls for GDocP for electronic data are in place and that the probability of the occurrence of errors in the data is minimized;
- training of personnel who use computerized systems and review electronic data in basic understanding of how computerized systems work and how to efficiently review the electronic data, which includes metadata and audit trails;
- definition and management of appropriate roles and responsibilities for quality agreements and contracts entered into by contract givers and contract acceptors, including the need for risk-based monitoring of data generated and managed by the contract acceptor on behalf of the contract giver;
- modernization of quality assurance inspection techniques and gathering of quality metrics to efficiently and effectively identify risks and opportunities to improve data processes.

2. Aims and objectives of this guidance

2.1 This guidance consolidates existing normative principles and gives detailed illustrative implementation guidance to bridge the gaps in current guidance. Additionally, it gives explanations as to what these high-level requirements mean in practice and what should be demonstrably implemented to achieve compliance.

2.2 These guidelines highlight, and in some instances clarify, the application of data management procedures. The focus is on those principles that are implicit in existing WHO guidelines and that if not robustly implemented can impact on data reliability and completeness and undermine the robustness of decision-making based upon those data. Illustrative examples are provided as to how these principles may be applied to current technologies and business models. These guidelines do not define all expected controls for assuring data reliability and this guidance should be considered in conjunction with existing WHO guidelines and other related international references.

2.3 This guidance is of an evolutionary, illustrative nature and will therefore be subject to periodic review based upon experience with its implementation and usefulness, as well as the feedback provided by the stakeholders, including national regulatory authorities (NRAs).

3. Glossary

The definitions given below apply to the terms used in these guidelines. They may have different meanings in other contexts.

ALCOA. A commonly used acronym for "attributable, legible, contemporaneous, original and accurate".

ALCOA-plus. A commonly used acronym for "attributable, legible, contemporaneous, original and accurate", which puts additional emphasis on the attributes of being complete, consistent, enduring and available – implicit basic ALCOA principles.

archival. Archiving is the process of protecting records from the possibility of being further altered or deleted, and storing these records under the control of independent data management personnel throughout the required retention period. Archived records should include, for example, associated metadata and electronic signatures.

archivist. An independent individual designated in good laboratory practice (GLP) who has been authorized by management to be responsible for the management of the archive, i.e. for the operations and procedures for archiving. GLP requires a designated archivist (i.e. an individual); however, in

other GXPs the roles and responsibilities of the archivist are normally fulfilled by several designated personnel or groups of personnel (e.g. both quality assurance document control personnel and information technology (IT) system administrators) without there being one single person assigned responsibility for control as is required in GLP.

It is recognized that in certain circumstances it may be necessary for the archivist to delegate specific archiving tasks, for example, the management of electronic data, to specific IT personnel. Tasks, duties and responsibilities should be specified and detailed in standard operating procedures. The responsibilities of the archivist and the staff to whom archival tasks are delegated include – for both paper and electronic data – ensuring that access to the archive is controlled, ensuring that the orderly storage and retrieval of records and materials is facilitated by a system of indexing, and ensuring that movement of records and materials into and out of the archives is properly controlled and documented. These procedures and records should be periodically reviewed by an independent auditor.

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

For example, in a paper record, an audit trail of a change would be documented via a single-line cross-out that allows the original entry to remain legible and documents the initials of the person making the change, the date of the change and the reason for the change, as required to substantiate and justify the change. In electronic records, secure, computer-generated, time-stamped audit trails should allow for reconstruction of the course of events relating to the creation, modification and deletion of electronic data. Computer-generated audit trails should retain the original entry and document the user identification, the time/date stamp of the action, as well as the reason for the change, as required to substantiate and justify the action. Computer-generated audit trails may include discrete event logs, history files, database queries or reports or other mechanisms that display events related to the computerized system, specific electronic records or specific data contained within the record.

backup. A backup means a copy of one or more electronic files created as an alternative in case the original data or system are lost or become unusable (for example, in the event of a system crash or corruption of a disk). It is important to note that backup differs from archival in that back-up copies of electronic records are typically only temporarily stored for the purposes of

disaster recovery and may be periodically overwritten. Such temporary back-up copies should not be relied upon as an archival mechanism.

computerized system. A computerized system collectively controls the performance of one or more automated processes and/or functions. It includes computer hardware, software, peripheral devices, networks and documentation, e.g. manuals and standard operating procedures, as well as the personnel interfacing with the hardware and software, e.g. users and information technology support personnel.

control strategy. A planned set of controls, derived from current protocol, test article or product and process understanding, which assures protocol compliance, process performance, product quality and data reliability, as applicable. The controls should include appropriate parameters and quality attributes related to study subjects, test systems, product materials and components, technologies and equipment, facilities, operating conditions, specifications and the associated methods and frequency of monitoring and control.

corrective and preventive action (**CAPA**, also sometimes called **corrective action/preventive action**) refers to the actions taken to improve an organization's processes and to eliminate causes of non-conformities or other undesirable situations. CAPA is a concept common across the GXPs (good laboratory practices, good clinical practices and good manufacturing practices), and numerous International Organization for Standardization business standards. The process focuses on the systematic investigation of the root causes of identified problems or identified risks in an attempt to prevent their recurrence (for corrective action) or to prevent occurrence (for preventive action).

data. Data means all original records and true copies of original records, including source data and metadata and all subsequent transformations and reports of these data, which are generated or recorded at the time of the GXP activity and allow full and complete reconstruction and evaluation of the GXP activity. Data should be accurately recorded by permanent means at the time of the activity. Data may be contained in paper records (such as worksheets and logbooks), electronic records and audit trails, photographs, microfilm or microfiche, audio- or video-files or any other media whereby information related to GXP activities is recorded.

data governance. The totality of arrangements to ensure that data, irrespective of the format in which they are generated, are recorded, processed, retained and used to ensure a complete, consistent and accurate record throughout the data life cycle.

data integrity. Data integrity is the degree to which data are complete, consistent, accurate, trustworthy and reliable and that these characteristics of the data are maintained throughout the data life cycle. The data should be collected and maintained in a secure manner, such that they are attributable, legible,

contemporaneously recorded, original or a true copy and accurate. Assuring data integrity requires appropriate quality and risk management systems, including adherence to sound scientific principles and good documentation practices.

data life cycle. All phases of the process by which data are created, recorded, processed, reviewed, analysed and reported, transferred, stored and retrieved and monitored until retirement and disposal. There should be a planned approach to assessing, monitoring and managing the data and the risks to those data in a manner commensurate with potential impact on patient safety, product quality and/or the reliability of the decisions made throughout all phases of the data life cycle.

dynamic record format. Records in dynamic format, such as electronic records, that allow for an interactive relationship between the user and the record content. For example, electronic records in database formats allow the user to track, trend and query data; chromatography records maintained as electronic records allow the user (with proper access permissions) to reprocess the data and expand the baseline to view the integration more clearly.

fully-electronic approach. This term refers to use of a computerized system in which the original electronic records are electronically signed.

good data and record management practices. The totality of organized measures that should be in place to collectively and individually ensure that data and records are secure, attributable, legible, traceable, permanent, contemporaneously recorded, original and accurate and that if not robustly implemented can impact on data reliability and completeness and undermine the robustness of decision-making based upon those data records.

good documentation practices. In the context of these guidelines, good documentation practices are those measures that collectively and individually ensure documentation, whether paper or electronic, is secure, attributable, legible, traceable, permanent, contemporaneously recorded, original and accurate.

GXP. Acronym for the group of good practice guides governing the preclinical, clinical, manufacturing, testing, storage, distribution and post-market activities for regulated pharmaceuticals, biologicals and medical devices, such as good laboratory practices, good clinical practices, good manufacturing practices, good pharmacovigilance practices and good distribution practices.

hybrid approach. This refers to the use of a computerized system in which there is a combination of original electronic records and paper records that comprise the total record set that should be reviewed and retained. An example of a hybrid approach is where laboratory analysts use computerized instrument systems that create original electronic records and then print a summary of the results. The hybrid approach requires a secure link between all record types, including paper and electronic, throughout the records retention period. Where hybrid approaches are used, appropriate controls for electronic

documents, such as templates, forms and master documents, that may be printed, should be available.

metadata. Metadata are data about data that provide the contextual information required to understand those data. These include structural and descriptive metadata. Such data describe the structure, data elements, interrelationships and other characteristics of data. They also permit data to be attributable to an individual. Metadata necessary to evaluate the meaning of data should be securely linked to the data and subject to adequate review. For example, in weighing, the number 8 is meaningless without metadata, i.e. the unit, mg. Other examples of metadata include the time/date stamp of an activity, the operator identification (ID) of the person who performed an activity, the instrument ID used, processing parameters, sequence files, audit trails and other data required to understand data and reconstruct activities.

quality metrics. Quality metrics are objective measures used by management and other interested parties to monitor the overall state of quality of a GXP organization, activity or process or study conduct, as applicable. They include measures to assess the effective functioning of quality system controls and of the performance, quality and safety of medicinal products and reliability of data.

quality risk management. A systematic process for the assessment, control, communication and review of risks to the quality of the pharmaceutical product throughout the product life cycle.

senior management. Person(s) who direct and control a company or site at the highest levels with the authority and responsibility to mobilize resources within the company or site.

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

true copy. A true copy is a copy of an original recording of data that has been verified and certified to confirm it is an exact and complete copy that preserves the entire content and meaning of the original record, including, in the case of electronic data, all essential metadata and the original record format as appropriate.

4. Principles

4.1 GDRP are critical elements of the pharmaceutical quality system and a systematic approach should be implemented to provide a high level of assurance that throughout the product life cycle, all GXP records and data are complete and reliable.

4.2 The data governance programme should include policies and governance procedures that address the general principles listed below for a good data management programme. These principles are clarified with additional detail in the sections below.

4.3 **Applicability to both paper and electronic data.** The requirements for GDRP that assure robust control of data validity apply equally to paper and electronic data. Organizations subject to GXP should be fully aware that reverting from automated or computerized to manual or paper-based systems does not in itself remove the need for robust management controls.

4.4 **Applicability to contract givers and contract acceptors.** The principles of these guidelines apply to contract givers and contract acceptors. Contract givers are ultimately responsible for the robustness of all decisions made on the basis of GXP data, including those made on the basis of data provided to them by contract acceptors. Contract givers should therefore perform risk-based, due diligence to assure themselves that contract acceptors have in place appropriate programmes to ensure the veracity, completeness and reliability of the data provided.

4.5 **Good documentation practices.** To achieve robust decisions, the supporting data set needs to be reliable and complete. GDocP should be followed in order to ensure all records, both paper and electronic, allow the full reconstruction and traceability of GXP activities.

4.6 **Management governance.** To establish a robust and sustainable good data management system it is important that senior management ensure that appropriate data management governance programmes are in place (for details see Section 6).

Elements of effective management governance should include:

- application of modern QRM principles and good data management principles that assure the validity, completeness and reliability of data;
- application of appropriate quality metrics;
- assurance that personnel are not subject to commercial, political, financial and other organizational pressures or incentives that may adversely affect the quality and integrity of their work;
- allocation of adequate human and technical resources such that the workload, work hours and pressures on those responsible for data generation and record keeping do not increase errors;
- ensure staff are aware of the importance of their role in ensuring data integrity and the relationship of these activities to assuring product quality and protecting patient safety.

4.7 **Quality culture.** Management, with the support of the quality unit, should establish and maintain a working environment that minimizes the risk of non-compliant records and erroneous records and data. An essential element of the quality culture is the transparent and open reporting of deviations, errors, omissions and aberrant results at all levels of the organization, irrespective of hierarchy. Steps should be taken to prevent, and to detect and correct weaknesses in systems and procedures that may lead to data errors so as to continually improve the robustness of scientific decision-making within the organization. Senior management should actively discourage any management practices that might reasonably be expected to inhibit the active and complete reporting of such issues, for example, hierarchical constraints and blame cultures.

4.8 **Quality risk management and sound scientific principles.** Robust decision-making requires appropriate quality and risk management systems, and adherence to sound scientific and statistical principles, which must be based upon reliable data. For example, the scientific principle of being an objective, unbiased observer regarding the outcome of a sample analysis requires that suspect results be investigated and rejected from the reported results only if they are clearly attributable to an identified cause. Adhering to good data and record-keeping principles requires that any rejected results be recorded, together with a documented justification for their rejection, and that this documentation is subject to review and retention.

4.9 **Data life cycle management.** Continual improvement of products to ensure and enhance their safety, efficacy and quality requires a data governance approach to ensure management of data integrity risks throughout all phases of the process by which data are created, recorded, processed, transmitted, reviewed, reported, archived and retrieved and this management process is subject to regular review. To ensure that the organization, assimilation and analysis of data into information facilitates evidence-based and reliable decision-making, data governance should address data ownership and accountability for data process(es) and risk management of the data life cycle.

4.10 To ensure that the organization, assimilation and analysis of data into a format or structure that facilitates evidence-based and reliable decision-making, data governance should address data ownership and accountability for data process(es) and risk management of the data life cycle.

4.11 **Design of record-keeping methodologies and systems.** Record-keeping methodologies and systems, whether paper or electronic, should be designed in a way that encourages compliance with the principles of data integrity.

4.12 Examples include, but are not restricted to:

- restricting the ability to change any clock used for recording timed events, for example, system clocks in electronic systems and process instrumentation;
- ensuring controlled forms used for recording GXP data (e.g. paper batch records, paper case report forms and laboratory worksheets) are accessible at the locations where an activity is taking place, at the time that the activity is taking place, so that ad hoc data recording and later transcription is not necessary;
- controlling the issuance of blank paper templates for data recording of GXP activities so that all printed forms can be reconciled and accounted for;
- restricting user access rights to automated systems to prevent (or audit trail) data amendments;
- ensuring automated data capture or printers are attached and connected to equipment, such as balances, to ensure independent and timely recording of the data;
- ensuring proximity of printers to sites of relevant activities;
- ensuring ease of access to locations of sampling points (e.g. sampling points for water systems) to allow easy and efficient performance of sampling by the operators and therefore minimizing the temptation to take shortcuts or falsify samples;
- ensuring access to original electronic data for staff performing data checking activities.

4.13 Data and record media should be durable. For paper records, the ink should be indelible. Temperature-sensitive or photosensitive inks and other erasable inks should not be used. Paper should also not be temperature-sensitive, photosensitive or easily oxidizable. If this is not feasible or limited (as may be the case in printouts from legacy printers of balance and other instruments in quality control laboratories), then true or certified copies should be available until this equipment is retired or replaced.

4.14 **Maintenance of record-keeping systems.** The systems implemented and maintained for both paper and electronic record-keeping should take account of scientific and technical progress. Systems, procedures and methodology used to record and store data should be periodically reviewed for effectiveness and updated as necessary.

5. Quality risk management to ensure good data management

5.1 All organizations performing work subject to GXP are required by applicable existing WHO guidance to establish, implement and maintain an appropriate quality management system, the elements of which should be documented in their prescribed format, such as a quality manual or other appropriate documentation. The quality manual, or equivalent documentation, should include a quality policy statement of management's commitment to an effective quality management system and to good professional practice. These policies should include a code of ethics and code of proper conduct to assure the reliability and completeness of data, including mechanisms for staff to report any quality and compliance questions or concerns to management.

5.2 Within the quality management system, the organization should establish the appropriate infrastructure, organizational structure, written policies and procedures, processes and systems to both prevent and detect situations that may impact on data integrity and, in turn, the risk-based and scientific robustness of decisions based upon those data.

5.3 QRM is an essential component of an effective data and record validity programme. The effort and resources assigned to data and record management should be commensurate with the risk to product quality. The risk-based approach to record and data management should ensure that adequate resources are allocated and that control strategies for the assurance of the integrity of GXP data are commensurate with their potential impact on product quality and patient safety and related decision-making.

5.4 Strategies that promote good practices and prevent record and data integrity issues from occurring are preferred and are likely to be the most effective and cost-effective. For example, access controls that allow only people with the appropriate authorization to alter a master processing formula will reduce the probability of invalid and aberrant data being generated. Such preventive measures, when effectively implemented, also reduce the amount of monitoring required to detect uncontrolled change.

5.5 Record and data integrity risks should be assessed, mitigated, communicated and reviewed throughout the data life cycle in accordance with the principles of QRM. Examples of approaches that may enhance data reliability are given in these guidelines but should be viewed as recommendations. Other approaches may be justified and shown to be equally effective in achieving satisfactory control of risk. Organizations

should therefore design appropriate tools and strategies for the management of data integrity risks based upon their own GXP activities, technologies and processes.

5.6 A data management programme developed and implemented upon the basis of sound QRM principles is expected to leverage existing technologies to their full potential. This in turn will streamline data processes in a manner that not only improves data management but also the business process efficiency and effectiveness, thereby reducing costs and facilitating continual improvement.

6. Management governance and quality audits

6.1 Assuring robust data integrity begins with management, which has the overall responsibility for the technical operations and provision of resources to ensure the required quality of GXP operations. Senior management has the ultimate responsibility for ensuring that an effective quality system is in place to achieve the quality objectives, and that staff roles, responsibilities and authorities, including those required for effective data governance programmes, are defined, communicated and implemented throughout the organization. Leadership is essential to establish and maintain a company-wide commitment to data reliability as an essential element of the quality system.

6.2 The building blocks of behaviours, procedural/policy considerations and basic technical controls together form the foundation of good data governance, upon which future revisions can be built. For example, a good data governance programme requires the necessary management arrangements to ensure personnel are not subject to commercial, political, financial and other pressures or conflicts of interest that may adversely affect the quality of their work and integrity of their data. Management should also make staff aware of the relevance of data integrity and the importance of their role in protecting the safety of patients and the reputation of their organization for quality products and services.

6.3 Management should create a work environment in which staff are encouraged to communicate failures and mistakes, including data reliability issues, so that corrective and preventive actions can be taken and the quality of an organization's products and services enhanced. This includes ensuring adequate information flow between staff at all levels. Senior management should actively discourage any management practices that

might reasonably be expected to inhibit the active and complete reporting of such issues, for example, hierarchical constraints and blame cultures.

6.4 Management reviews and regular reporting of quality metrics facilitate meeting these objectives. This requires designation of a quality manager who has direct access to the highest level of management and can directly communicate risks, so that senior management is made aware of any issues and can allocate resources to address them. To fulfil this role the quality unit should conduct and report to management formal, documented risk reviews of the key performance indicators of the quality management system. These should include metrics related to data integrity that will help identify opportunities for improvement. For example:

- tracking and trending of invalid and aberrant data may reveal unforeseen variability in processes and procedures previously believed to be robust, opportunities to enhance analytical procedures and their validation, validation of processes, training of personnel or sourcing of raw materials and components;
- adequate review of audit trails, including those reviewed as part of key decision-making steps (e.g. GMP batch release, issuance of a GLP study report or approval of case report forms), may reveal incorrect processing of data, help prevent incorrect results from being reported and identify the need for additional training of personnel;
- routine audits and/or self-inspections of computerized systems may reveal gaps in security controls that inadvertently allow personnel to access and potentially alter time/date stamps. Such findings help raise awareness among management of the need to allocate resources to improve validation controls for computerized systems;
- monitoring of contract acceptors and tracking and trending of associated quality metrics for these sites help to identify risks that may indicate the need for more active engagement and allocation of additional resources by the contract giver to ensure quality standards are met.

6.5 Quality audits of suppliers, self-inspections and risk reviews should identify and inform management of opportunities to improve foundational systems and processes that have an impact on data reliability. Allocation of resources by management to these improvements of systems and processes may efficiently reduce data integrity risks. For example, identifying and addressing technical difficulties with the equipment used to perform multiple GXP operations may greatly improve the reliability

of data for all of these operations. Another example relates to identifying conflicts of interests affecting security. Allocating independent technical support personnel to perform system administration for computerized systems, including managing security, backup and archival, reduces potential conflicts of interest and may greatly streamline and improve data management efficiency.

6.6 All GXP records held by the GXP organization are subject to inspection by the responsible health authorities. This includes original electronic data and metadata, such as audit trails maintained in computerized systems. Management of both contract givers and contract acceptors should ensure that adequate resources are available and that procedures for computerized systems are available for inspection. System administrator personnel should be available to readily retrieve requested records and facilitate inspections.

7. Contracted organizations, suppliers and service providers

7.1 The increasing outsourcing of GXP work to contracted organizations, e.g. contract research organizations, suppliers and other service providers, emphasizes the need to establish and robustly maintain defined roles and responsibilities to assure complete and accurate data and records throughout these relationships. The responsibilities of the contract giver and acceptor, should comprehensively address the processes of both parties that should be followed to ensure data integrity. These details should be included in the contract described in the WHO GXPs relevant to the outsourced work performed or the services provided.

7.2 The organization that outsources work has the responsibility for the integrity of all results reported, including those furnished by any subcontracting organization or service provider. These responsibilities extend to any providers of relevant computing services. When outsourcing databases and software provision, the contract giver should ensure that any subcontractors have been agreed upon and are included in the quality agreement with the contract accepter, and are appropriately qualified and trained in GRDP. Their activities should be monitored on a regular basis at intervals determined through risk assessment. This also applies to cloud-based service providers.

7.3 To fulfil this responsibility, in addition to having their own governance systems, outsourcing organizations should verify the adequacy of the

governance systems of the contract acceptor, through an audit or other suitable means. This should include the adequacy of the contract acceptor's controls over suppliers and a list of significant authorized third parties working for the contract acceptor.

7.4 The personnel who evaluate and periodically assess the competence of a contracted organization or service provider should have the appropriate background, qualifications, experience and training to assess data integrity governance systems and to detect validity issues. The nature and frequency of the evaluation of the contract acceptor and the approach to ongoing monitoring of their work should be based upon documented assessment of risk. This assessment should include an assessment of relevant data processes and their risks.

7.5 The expected data integrity control strategies should be included in quality agreements and in written contract and technical arrangements, as appropriate and applicable, between the contract giver and the contract acceptor. These should include provisions for the contract giver to have access to all data held by the contracted organization that are relevant to the contract giver's product or service as well as all relevant quality systems records. This should include ensuring access by the contract giver to electronic records, including audit trails, held in the contracted organization's computerized systems as well as any printed reports and other relevant paper or electronic records.

7.6 Where data and document retention is contracted to a third party, particular attention should be paid to understanding the ownership and retrieval of data held under this arrangement. The physical location where the data are held, and the impact of any laws applicable to that geographical location, should also be considered. Agreements and contracts should establish mutually agreed consequences if the contract acceptor denies, refuses or limits the contract giver's access to their records held by the contract acceptor. The agreements and contracts should also contain provisions for actions to be taken in the event of business closure or bankruptcy of the third party to ensure that access is maintained and the data can be transferred before the cessation of all business activities.

7.7 When outsourcing databases, the contract giver should ensure that if subcontractors are used, in particular cloud-based service providers, they are included in the quality agreement and are appropriately qualified and trained in GRDP. Their activities should be monitored on a regular basis at intervals determined through risk assessment.

8. Training in good data and record management

8.1 Personnel should be trained in data integrity policies and agree to abide by them. Management should ensure that personnel are trained to understand and distinguish between proper and improper conduct, including deliberate falsification, and should be made aware of the potential consequences.

8.2 In addition, key personnel, including managers, supervisors and quality unit personnel, should be trained in measures to prevent and detect data issues. This may require specific training in evaluating the configuration settings and reviewing electronic data and metadata, such as audit trails, for individual computerized systems used in the generation, processing and reporting of data. For example, the quality unit should learn how to evaluate configuration settings that may intentionally or unintentionally allow data to be overwritten or obscured through the use of hidden fields or data annotation tools. Supervisors responsible for reviewing electronic data should learn which audit trails in the system track significant data changes and how these might be most efficiently accessed as part of their review.

8.3 Management should also ensure that, at the time of hire and periodically afterwards, as needed, all personnel are trained in procedures to ensure GDocP for both paper and electronic records. The quality unit should include checks for adherence to GDocP for both paper records and electronic records in their day-to-day work, system and facility audits and self-inspections and report any opportunities for improvement to management.

9. Good documentation practices

9.1 The basic building blocks of good GXP data are to follow GDocP and then to manage risks to the accuracy, completeness, consistency and reliability of the data throughout their entire period of usefulness – that is, throughout the data life cycle.

Personnel should follow GDocP for both paper records and electronic records in order to assure data integrity. These principles require that documentation has the characteristics of being attributable, legible, contemporaneously recorded, original and accurate (sometimes referred to as ALCOA). These essential characteristics apply equally for both paper and electronic records.

9.2 **Attributable.** Attributable means information is captured in the record so that it is uniquely identified as executed by the originator of the data (e.g. a person or a computer system).

9.3 **Legible, traceable and permanent.** The terms legible and traceable and permanent refer to the requirements that data are readable, understandable, and allow a clear picture of the sequencing of steps or events in the record so that all GXP activities conducted can be fully reconstructed by the people reviewing these records at any point during the records retention period set by the applicable GXP.

9.4 **Contemporaneous.** Contemporaneous data are data recorded at the time they are generated or observed.

9.5 **Original.** Original data include the first or source capture of data or information and all subsequent data required to fully reconstruct the conduct of the GXP activity. The GXP requirements for original data include the following:

- original data should be reviewed;
- original data and/or true and verified copies that preserve the content and meaning of the original data should be retained;
- as such, original records should be complete, enduring and readily retrievable and readable throughout the records retention period.

9.6 **Accurate.** The term "accurate" means data are correct, truthful, complete, valid and reliable.

9.7 Implicit in the above-listed requirements for ALCOA are that the records should be **complete, consistent, enduring and available** (to emphasize these requirements, this is sometimes referred to as ALCOA-plus).

9.8 Further guidance to aid understanding as to how these requirements apply in each case and the special risk considerations that may need to be taken into account during implementation are provided in Appendix 1.

10. Designing and validating systems to assure data quality and reliability

10.1 Record-keeping methodologies and systems, whether paper or electronic, should be designed in a way that encourages compliance and assures data quality and reliability. All requirements and controls necessary to ensure GDRP should be adhered to for both paper and electronic records.

Validation to assure good documentation practices for electronic data

10.2 To assure the integrity of electronic data, computerized systems should be validated at a level appropriate for their use and application. Validation should address the necessary controls to ensure the integrity of data, including original electronic data and any printouts or PDF reports from the system. In particular, the approach should ensure that GDocP will be implemented and that data integrity risks will be properly managed throughout the data life cycle.

10.3 The "Supplementary guidelines on good manufacturing practices: validation" (WHO Technical Report Series, No. 937, 2006, Annex 4 (*2–4*)[1] provide a more comprehensive presentation of validation considerations. The key aspects of validation that help assure GDocP for electronic data include, but are not limited to, the following.

10.4 **User involvement.** Users should be adequately involved in validation activities to define critical data and data life cycle controls that assure data integrity.

- Examples of activities to engage users may include: prototyping, user specification of critical data so that risk-based controls can be applied, user involvement in testing to facilitate user acceptance and knowledge of system features, and others.

10.5 **Configuration and design controls.** The validation activities should ensure configuration settings and design controls for GDocP are enabled and managed across the computing environment (including both the software application and operating systems environments).

Activities include, but are not limited to:

- documenting configuration specifications for commercial off-the-shelf systems as well as user-developed systems, as applicable;
- restricting security configuration settings for system administrators to independent personnel, where technically feasible;
- disabling configuration settings that allow overwriting and reprocessing of data without traceability;
- restricting access to time/date stamps.

[1] Currently under review.

For systems to be used in clinical trials, configuration and design controls should be in place to protect the blinding of the trial, for example, by restricting access to randomization data that may be stored electronically.

10.6 **Data life cycle.** Validation should include assessing risk and developing quality risk mitigation strategies for the data life cycle, including controls to prevent and detect risks throughout the steps of:

- data generation and capture;
- data transmission;
- data processing;
- data review;
- data reporting, including handling of invalid and atypical data;
- data retention and retrieval;
- data disposal.

Activities might include, but are not limited to:

- determining the risk-based approach to reviewing electronic data and audit trails based upon process understanding and knowledge of potential impact on products and patients;
- writing SOPs defining review of original electronic records and including meaningful metadata such as audit trails and review of any associated printouts or PDF records;
- documenting the system architecture and data flow, including the flow of electronic data and all associated metadata, from the point of creation through archival and retrieval;
- ensuring that the relationships between data and metadata are maintained intact throughout the data life cycle.

10.7 **SOPs and training.** The validation activities should ensure that adequate training and procedures are developed prior to release of the system for GXP use. These should address:

- computerized systems administration;
- computerized systems use;
- review of electronic data and meaningful metadata, such as audit trails, including training that may be required in system features that enable users to efficiently and effectively process data and review electronic data and metadata.

10.8 Other validation controls to ensure good data management for both electronic data and associated paper data should be implemented as deemed appropriate for the system type and its intended use.

11. Managing data and records throughout the data life cycle

11.1 Data processes should be designed to adequately mitigate and control and continuously review the data integrity risks associated with the steps of acquiring, processing, reviewing and reporting data, as well as the physical flow of the data and associated metadata during this process through storage and retrieval.

11.2 QRM of the data life cycle requires understanding the science and technology of the data process and their inherent limitations. Good data process design, based upon process understanding and the application of sound scientific principles, including QRM, would be expected to increase the assurance of data integrity and to result in an effective and efficient business process.

11.3 Data integrity risks are likely to occur and to be highest when data processes or specific data process steps are inconsistent, subjective, open to bias, unsecured, unnecessarily complex or redundant, duplicated, undefined, not well understood, hybrid, based upon unproven assumptions and/or do not adhere to GDRP.

11.4 Good data process design should consider, for each step of the data process, ensuring and enhancing controls, whenever possible, so that each step is:

- consistent;
- objective, independent and secure;
- simple and streamlined;
- well-defined and understood;
- automated;
- scientifically and statistically sound;
- properly documented according to GDRP.

Examples of considerations for each phase of the data life cycle are provided below.

11.5 **Data collection and recording.** All data collection and recording should be performed following GDRP and should apply risk-based controls to protect and verify critical data.

11.6 *Example consideration.*

Data entries, such as the sample identification for laboratory tests or the recording of source data for inclusion of a patient in a clinical trial, should be verified by a second person or entered through technical means such as barcoding, as appropriate for the intended use of these data. Additional controls may include locking critical data entries after the data are verified and review of audit trails for critical data to detect if they have been altered.

11.7 **Data processing.** To ensure data integrity, data processing should be done in an objective manner, free from bias, using validated/qualified or verified protocols, processes, methods, systems, equipment and according to approved procedures and training programmes.

11.8 *Example considerations.*

GXP organizations should take precautions to discourage testing or processing data towards a desired outcome. For example:

- to minimize potential bias and ensure consistent data processing, test methods should have established sample acquisition and processing parameters, established in default version-controlled electronic acquisition and processing method files, as appropriate. Changes to these default parameters may be necessary during sample processing, but these changes should be documented (who, what, when?) and justified (why?);
- system suitability runs should include only established standards or reference materials of known concentration to provide an appropriate comparator for the potential variability of the instrument. If a sample (e.g. a well-characterized secondary standard) is used for system suitability or a trial run, written procedures should be established and followed and the results included in the data review process. The article under test should not be used for trial run purposes or to evaluate suitability of the system;
- clinical and safety studies should be designed to prevent and detect statistical bias that may occur through improper selection of data to be included in statistical calculations.

11.9 **Data review and reporting.** Data should be reviewed and, where appropriate, evaluated statistically after completion of the process to determine whether outcomes are consistent and compliant with established standards. The evaluation should take into consideration all data, including atypical, suspect or rejected data, together with the reported data. This includes a review of the original paper and electronic records.

11.10 For example, during self-inspection, some key questions to ask are: Am I collecting all my data? Am I considering all my data? If I have excluded some data from my decision-making process, what is the justification for doing so, and are all the data retained, including both rejected and reported data?

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

11.12 Whenever out-of-trend or atypical results are obtained they should be investigated. This includes investigating and determining corrective and preventive actions for invalid runs, failures, repeats and other atypical data. All data should be included in the dataset unless there is a documented scientific explanation for their exclusion.

11.13 During the data life cycle, data should be subject to continuous monitoring, as appropriate, to enhance process understanding and facilitate knowledge management and informed decision-making.

11.14 *Example considerations*

To ensure that the entire set of data is considered in the reported data, the review of original electronic data should include checks of all locations where data may have been stored, including locations where voided, deleted, invalid or rejected data may have been stored.

11.15 **Data retention and retrieval.** Retention of paper and electronic records is discussed in the section above, including measures for backup and archival of electronic data and metadata.

11.16 *Example consideration*

1) Data folders on some stand-alone systems may not include all audit trails or other metadata needed to reconstruct all activities. Other metadata may be found in other electronic folders or in operating system logs. When archiving electronic data, it is important to ensure that associated metadata are archived with the relevant data set or securely traceable to the data set through appropriate documentation. The ability to successfully retrieve from the archives the entire data set, including metadata, should be verified.

2) Only validated systems are used for storage of data; however, the media used for the storage of data do not have an indefinite lifespan. Consideration must be given to the longevity of media and the environment in which they are stored. Examples include the fading of microfilm records, the decreasing readability of the coatings of optical media such as compact disks (CDs) and digital versatile/video disks (DVDs), and the fact that these media may become brittle. Similarly, historical data stored on magnetic media will also become unreadable over time as a result of deterioration.

12. Addressing data reliability issues

12.1 When issues with data validity and reliability are discovered, it is important that their potential impact on patient safety and product quality and on the reliability of information used for decision-making and applications is examined as a top priority. Health authorities should be notified if the investigation identifies material impact on patients, products, reported information or on application dossiers.

12.2 The investigation should ensure that copies of all data are secured in a timely manner to permit a thorough review of the event and all potentially related processes.

12.3 The people involved should be interviewed to better understand the nature of the failure and how it occurred and what might have been done to prevent and detect the issue sooner. This should include discussions with the people involved in data integrity issues, as well as supervisory personnel, quality assurance and management staff.

12.4 The investigation should not be limited to the specific issue identified but should also consider potential impact on previous decisions based upon the data and systems now found to be unreliable. In addition, it is vital that the deeper, underlying root cause(s) of the issue be considered, including potential management pressures and incentives, for example, a lack of adequate resources.

12.5 Corrective and preventive actions taken should not only address the identified issue, but also previous decisions and datasets that are impacted, as well as deeper, underlying root causes, including the need for realignment of management expectations and allocation of additional resources to prevent risks from recurring in the future.

References and further reading

References

1. WHO good manufacturing practices for pharmaceutical products: main principles. In: WHO Expert Committee on Specifications for Pharmaceutical Preparations: forty-eighth report. Geneva: World Health Organization; 2014: Annex 2 (WHO Technical Report Series, No. 986), also available on CD-ROM and online.
2. Supplementary guidelines on good manufacturing practice: validation. In: WHO Expert Committee on Specifications for Pharmaceutical Preparations: fortieth report. Geneva: World Health Organization; 2006: Annex 4 (WHO Technical Report Series, No. 937).
3. Supplementary guidelines on good manufacturing practice: validation. Qualification of systems and equipment. In: WHO Expert Committee on Specifications for Pharmaceutical Preparations: fortieth report. Geneva: World Health Organization; 2006: Annex 4, Appendix 6 (WHO Technical Report Series, No. 937).
4. Supplementary guidelines on good manufacturing practices: validation. Validation of computerized systems. In: WHO Expert Committee on Specifications for Pharmaceutical Preparations: fortieth report. Geneva: World Health Organization; 2006: Annex 4, Appendix 5 (WHO Technical Report Series, No. 937).

Further reading

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

Good automated manufacturing practice (GAMP) good practice guide: electronic data archiving. Tampa (FL): International Society for Pharmaceutical Engineering (ISPE); 2007.

Good automated manufacturing practice GAMP good practice guide: A risk-based approach to GxP compliant laboratory computerized systems, 2nd edition. Tampa (FL): International Society for Pharmaceutical Engineering (ISPE); 2012.

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

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

Official Medicines Control Laboratories Network of the Council of Europe: Quality assurance documents: PA/PH/OMCL (08) 69 3R – Validation of computerised systems – core document (https://www.edqm.eu/sites/default/files/medias/fichiers/Validation_of_Computerised_Systems_Core_Document.pdf) and its annexes:

- PA/PH/OMCL (08) 87 2R – Annex 1: Validation of computerised calculation systems: example of validation of in-house software (https://www.edqm.eu/sites/default/files/medias/fichiers/NEW_Annex_1_Validation_of_computerised_calculation.pdf).
- PA/PH/OMCL (08) 88 R – Annex 2: Validation of databases (DB), laboratory information management systems (LIMS) and electronic laboratory notebooks (ELN) (https://www.edqm.eu/sites/default/files/medias/fichiers/NEW_Annex_2_Validation_of_Databases_DB_Laboratory_.pdf).

- PA/PH/OMCL (08) 89 R – Annex 3: Validation of computers as part of test equipment (https://www.edqm.eu/sites/default/files/medias/fichiers/NEW_Annex_3_Validation_of_computers_as_part_of_tes.pdf).

Title 21 Code of Federal Regulations (21 CFR Part 11): Electronic records; electronic signatures. US Food and Drug Administration. The current status of 21 CFR Part 11 Guidance is located under Regulations and Guidance at: http://www.fda.gov/cder/gmp/index.htm — see background: http://www.fda.gov/OHRMS/DOCKETS/98fr/03-4312.pdf.

PIC/S guide to good manufacturing practice for medicinal products annexes: Annex 11 – Computerised systems. Geneva: Pharmaceutical Inspection Co-operation Scheme.

PIC/S PI 011-3 Good practices for computerised systems in regulated GxP environments. Geneva: Pharmaceutical Inspection Co-operation Scheme.

WHO good manufacturing practices for active pharmaceutical ingredients. In: WHO Expert Committee on Specifications for Pharmaceutical Preparations: forty-fourth report. Geneva: World Health Organization; 2010: Annex 2 (WHO Technical Report Series, No. 957).

WHO good practices for pharmaceutical quality control laboratories. In: WHO Expert Committee on Specifications for Pharmaceutical Preparations: forty-fourth report. Geneva: World Health Organization; 2010: Annex 1 (WHO Technical Report Series, No. 957).

Appendix 1

Expectations and examples of special risk management considerations for the implementation of ALCOA (-plus) principles in paper-based and electronic systems

Organizations should follow good documentation practices (GDocP) in order to assure the accuracy, completeness, consistency and reliability of the records and data throughout their entire period of usefulness – that is, throughout the data life cycle. The principles require that documentation should have the characteristics of being attributable, legible, contemporaneously recorded, original and accurate (sometimes referred to as ALCOA).

The tables in this appendix provide further guidance on the implementation of the general ALCOA requirements for both paper and electronic records and systems. In addition, examples of special risk management considerations as well as several illustrative examples are provided of how these measures are typically implemented.

These illustrative examples are provided to aid understanding of the concepts and of how successful risk-based implementation might be achieved. These examples should not be taken as setting new normative requirements.

Attributable. Attributable means information is captured in the record so that it is uniquely identified as having been executed by the originator of the data (e.g. a person or computer system).

Attributable	
Expectations for paper records	**Expectations for electronic records**
Attribution of actions in paper records should occur, as appropriate, through the use of: • initials; • full handwritten signature; • personal seal; • date and, when necessary, time.	Attribution of actions in electronic records should occur, as appropriate, through the use of: • unique user logons that link the user to actions that create, modify or delete data; • unique electronic signatures (can be either biometric or non-biometric); • an audit trail that should capture user identification (ID) and date and time stamps; • signatures, which must be securely and permanently linked to the record being signed.

Special risk management considerations for controls to ensure that actions and records are attributed to a unique individual

- For legally-binding signatures, there should be a verifiable, secure link between the unique, identifiable (actual) person signing and the signature event. Signatures should be permanently linked to the record being signed. Systems which use one application for signing a document and another to store the document being signed should ensure that the two remain linked to ensure that the attribution is not broken.
- Signatures and personal seals should be executed at the time of review or performance of the event or action being recorded.
- Use of a personal seal to sign documents requires additional risk management controls, such as handwritten dates and procedures that require storage of the seal in a secure location with access limited only to the assigned individual, or equipped with other means of preventing potential misuse.
- Use of stored digital images of a person's handwritten signature to sign a document is not acceptable. This practice compromises confidence in the authenticity of these signatures when these stored images are not maintained in a secure location, access to which is limited only to the assigned individual, or equipped with other means of preventing potential misuse, and instead are placed in documents and emails where they can be easily copied and reused by others. Legally binding, handwritten signatures should be dated at the time of signing and electronic signatures should include the time/date stamp of signing to record the contemporaneous nature of the signing event.
- The use of hybrid systems is discouraged, but where legacy systems are awaiting replacement, mitigating controls should be in place. The use of shared and generic logon credentials should be avoided to ensure that actions documented in electronic records can be attributed to a unique individual. This would apply to the software application level and all applicable network environments where personnel may perform actions (e.g. workstation and server operating systems). Where such technical controls are not available or feasible, for example, in legacy electronic systems or where logon would terminate an application or stop the process running, combinations of paper and electronic records should be used to meet the requirements to attribute actions to the individuals concerned. In such cases, original records generated during the course of GXP

activities must be complete and must be maintained throughout the records retention period in a manner that allows the full reconstruction of the GXP activities.

- A hybrid approach might exceptionally be used to sign electronic records when the system lacks features for electronic signatures, provided adequate security can be maintained. The hybrid approach is likely to be more burdensome than a fully-electronic approach; therefore, utilizing electronic signatures, whenever available, is recommended. For example, the execution and attribution of an electronic record by attachment of a handwritten signature may be performed through a simple means that would create a single-page controlled form associated with the written procedures for system use and data review. The document should list the electronic dataset reviewed and any metadata subject to review, and would provide fields for the author, reviewer and/or approver of the dataset to insert a handwritten signature. This paper record with the handwritten signatures should then be securely and traceably linked to the electronic dataset, either through procedural means, such as use of detailed archives indexes, or technical means, such as embedding a true-copy scanned image of the signature page into the electronic dataset.
- Replacement of hybrid systems should be a priority.
- The use of a scribe to record an activity on behalf of another operator should be considered only on an exceptional basis and should only take place where:
  - the act of recording places the product or activity at risk, e.g. documenting line interventions by aseptic area operators;
  - to accommodate cultural differences or mitigate staff literacy/language limitations, for instance, where an activity is performed by an operator, but witnessed and recorded by a supervisor or officer.

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

Legible, traceable and permanent

The terms legible, traceable and permanent refer to the requirements that data are readable, understandable and allow a clear picture of the sequencing of steps or events in the record so that all GXP activities conducted can be fully reconstructed by people reviewing these records at any point during the records retention period set by the applicable GXP.

Legible, traceable, permanent	
Expectations for paper records	**Expectations for electronic records**
Legible, traceable and permanent controls for paper records include, but are not limited to: • use of permanent, indelible ink; • no use of pencil or erasures; • use of single-line cross-outs to record changes with name, date and reason recorded (i.e. the paper equivalent to the audit trail); • no use of opaque correction fluid or otherwise obscuring the record; • controlled issuance of bound, paginated notebooks with sequentially numbered pages (i.e. that allow detection of missing or skipped pages); • controlled issuance of sequentially numbered copies of blank forms (i.e. that allow all issued forms to be accounted for); • archival of paper records by independent, designated personnel in secure and controlled paper archives (archivist is the term used for these personnel in quality control, good laboratory practices (GLP) and good clinical practices (GCP) settings. In good manufacturing practices (GMP) settings this role is normally designated to specific individual(s) in the quality assurance unit);	Legible, traceable and permanent controls for electronic records include, but are not limited to: • designing and configuring computer systems and writing standard operating procedures (SOPs), as required, that enforce the saving of electronic data at the time of the activity and before proceeding to the next step of the sequence of events (e.g. controls that prohibit generation and processing and deletion of data in temporary memory and that instead enforce the committing of the data at the time of the activity to durable memory before moving to the next step in the sequence); • use of secure, time-stamped audit trails that independently record operator actions and attribute actions to the logged-on individual; • configuration settings that restrict access to enhanced security permissions (such as the system administrator role that can be used to potentially turn off the audit trails or enable overwriting and deletion of data), only to persons independent of those responsible for the content of the electronic records; • configuration settings and SOPs, as required, to disable and prohibit the ability to overwrite data, including prohibiting overwriting of preliminary and intermediate processing of data;

Table *continued*

Legible, traceable, permanent	
Expectations for paper records	**Expectations for electronic records**
• preservation of paper/ink that fades over time where their use is unavoidable.	• strictly controlled configuration and use of data annotation tools in a manner that prevents data in displays and printouts from being obscured; • validated backup of electronic records to ensure disaster recovery; • validated archival of electronic records by independent, designated archivist(s) in secure and controlled electronic archives.

Special risk management considerations for legible, traceable and permanent recording of GXP data

- When computerized systems are used to generate electronic data, it should be possible to associate all changes to data with the people who make those changes, and those changes should be time-stamped and a reason for the change recorded where applicable. This traceability of user actions should be documented via computer-generated audit trails or in other metadata fields or system features that meet these requirements.
- Users should not be able to amend or switch off the audit trails or alternative means of providing traceability of user actions.
- The need for the implementation of appropriate audit trail functionality should be considered for all new computerized systems. Where an existing computerized system lacks computer-generated audit trails, personnel may use alternative means such as procedurally-controlled use of logbooks, change control, record version control or other combinations of paper and electronic records to meet GXP regulatory expectations for traceability to document the what, who, when and why of an action. Procedural controls should include written procedures, training programmes, review of records and audits and self-inspections of the governing process(es).

- When archival of electronic records is used, the archiving process should be done in a controlled manner to preserve the integrity of the records. Electronic archives should be validated, secured and maintained in a state of control throughout the data life cycle. Electronic records archived manually or automatically should be stored in secure and controlled electronic archives, accessible only by independent, designated archivists or by their approved delegates.

  Appropriate separation of duties should be established so that business process owners, or other users who may have a conflict of interest, are not granted enhanced security access permissions at any system level (e.g. operating system, application and database). Further, highly privileged system administrator accounts should be reserved for designated technical personnel, e.g. information technology (IT) personnel, who are fully independent of the personnel responsible for the content of the records, as these types of accounts may include the ability to change settings to overwrite, rename, delete, move data, change time/date settings, disable audit trails and perform other system maintenance functions that turn off the good data and record management practices (GDRP) controls for legible and traceable electronic data. Where it is not feasible to assign these independent security roles, other control strategies should be used to reduce data validity risks.

  – To avoid conflicts of interest, these enhanced system access permissions should only be granted to personnel with system maintenance roles (e.g. IT, metrology, records control, engineering), that are fully independent of the personnel responsible for the content of the records (e.g. laboratory analysts, laboratory management, clinical investigators, study directors, production operators and production management). Where these independent security role assignments are not feasible, other control strategies should be used to reduce data validity risks.

It is particularly important that individuals with enhanced access permissions understand the impact of any changes they make using these privileges. Personnel with enhanced access should therefore also be trained in data integrity principles.

Contemporaneous

Contemporaneous data are data recorded at the time they are generated or observed.

Contemporaneous	
Expectations for paper records	**Expectations for electronic records**
Contemporaneous recording of actions in paper records should occur, as appropriate, through use of: • written procedures, and training and review and audit and self-inspection controls that ensure personnel record data entries and information *at the time of the activity directly in official controlled documents* (e.g. laboratory notebooks, batch records, case report forms); • procedures requiring that activities be recorded in paper records with the date of the activity (and time as well, if it is a time-sensitive activity); • good document design, which encourages good practice: documents should be appropriately designed and the availability of blank forms/ documents in which the activities are recorded should be ensured; • recording of the date and time of activities using synchronized time sources (facility and computerized system clocks) which cannot be changed by unauthorized personnel. Where possible, data and time recording of manual activities (e.g. weighing) should be done automatically.	Contemporaneous recording of actions in electronic records should occur, as appropriate, through use of: • configuration settings, SOPs and controls that ensure that data recorded in temporary memory are committed to durable media upon completion of the step or event and before proceeding to the next step or event in order to ensure the permanent recording of the step or event at the time it is conducted; • secure system time/date stamps that cannot be altered by personnel; • procedures and maintenance programmes that ensure time/date stamps are synchronized across the GXP operations; • controls that allow for the determination of the timing of one activity relative to another (e.g. time zone controls); • availability of the system to the user at the time of the activity.

Special risk management considerations for contemporaneous recording of GXP data

- Training programmes in GDocP should emphasize that it is unacceptable to record data first in unofficial documentation (e.g. on a scrap of paper) and later transfer the data to official documentation (e.g. the laboratory notebook). Instead, original data should be recorded directly in official records, such as approved analytical worksheets, immediately at the time of the GXP activity.
- Training programmes should emphasize that it is unacceptable to backdate or forward date a record. Instead the date recorded should be the actual date of the data entry. Late entries should be indicated as such with both the date of the activity and the date of the entry being recorded. If a person makes mistakes on a paper document he or she should make single-line corrections, sign and date them, provide reasons for the changes and retain this record in the record set.
- If users of stand-alone computerized systems are provided with full administrator rights to the workstation operating systems on which the original electronic records are stored, this may inappropriately grant permission to users to rename, copy or delete files stored on the local system and to change the time/date stamp. For this reason, validation of the stand-alone computerized system should ensure proper security restrictions to protect time/date settings and ensure data integrity in all computing environments, including the workstation operating system, the software application and any other applicable network environments.

Original

Original data include the first or source capture of data or information and all subsequent data required to fully reconstruct the conduct of the GXP activity. The GXP requirements for original data include the following:

- original data should be reviewed;
- original data and/or true and verified copies that preserve the content and meaning of the original data should be retained;
- as such, original records should be complete, enduring and readily retrievable and readable throughout the records retention period.

Examples of original data include original electronic data and metadata in stand-alone computerized laboratory instrument systems (e.g. ultraviolet/visible spectrophotometry (UV/Vis), Fourier transform infrared spectroscopy (FT-IR),

electrocardiogram (ECG), liquid chromatography-tandem mass spectrometry (LC/MS/MS) and haematology and chemistry analysers), original electronic data and metadata in automated production systems (e.g. automated filter integrity testers, supervisory control and data acquisition (SCADA) and distributed control system (DCS)), original electronic data and metadata in network database systems (e.g. laboratory information management system (LIMS), enterprise resource planning (ERP), manufacturing execution systems (MES), electronic case report form/electronic data capture (eCRF/EDC), toxicology databases, and deviation and corrective and preventive action (CAPA) databases), handwritten sample preparation information in paper notebooks, printed recordings of balance readings, electronic health records and paper batch records.

Review of original records	
Expectations for paper records	**Expectations for electronic records**
Controls for review of original paper records include, but are not limited to: • written procedures and training and review and audit and self-inspection controls to ensure that personnel conduct an adequate review and approval of original paper records, including those used to record the contemporaneous capture of information; • data review procedures describing review of relevant metadata. For example, written procedures for review should require that personnel evaluate changes made to original information on paper records (such as changes documented in cross-out or data correction) to ensure these changes are appropriately documented, and justified with substantiating evidence and investigated when required;	Controls for review of original electronic records include, but are not limited to: • written procedures and training and review and audit and inspection controls that ensure personnel conduct an adequate review and approval of original electronic records, including human readable source records of electronic data; • data review procedures describing review of original electronic data and relevant metadata. For example, written procedures for review should require that personnel evaluate changes made to original information in electronic records (such as changes documented in audit trails or history fields or found in other meaningful metadata) to ensure these changes are appropriately documented and justified with substantiating evidence and investigated when required;

Table *continued*

Review of original records	
Expectations for paper records	**Expectations for electronic records**
• documentation of data review. For paper records this is typically signified by signing the paper records that have been reviewed. Where record approval is a separate process this should also be similarly signed. Written procedures for data review should clarify the meaning of the review and approval signatures to ensure that the people concerned understand their responsibility as reviewers and approvers to assure the integrity, accuracy, consistency and compliance with established standards of the paper records subject to review and approval; • a procedure describing the actions to be taken if data review identifies an error or omission. This procedure should enable data corrections or clarifications to be made in a GXP-compliant manner, providing visibility of the original record and audit-trailed traceability of the correction, using ALCOA principles.	• documentation of data review. For electronic records, this is typically signified by electronically signing the electronic data set that has been reviewed and approved. Written procedures for data review should clarify the meaning of the review and approval signatures to ensure that the personnel concerned understand their responsibility as reviewers and approvers to assure the integrity, accuracy, consistency and compliance with established standards of the electronic data and metadata subject to review and approval; • a procedure describing the actions to be taken if data review identifies an error or omission. This procedure should enable data corrections or clarifications to be made in a GXP-compliant manner, providing visibility of the original record and audit trailed traceability of the correction, using ALCOA principles.

Special risk management considerations for review of original records

- Data integrity risks may occur when people choose to rely solely upon paper printouts or PDF reports from computerized systems without meeting applicable regulatory expectations for original records. Original records should be reviewed – this includes electronic records. If the reviewer only reviews the subset of data provided as a printout or PDF, risks may go undetected and harm may occur.
- Although original records should be reviewed, and all personnel involved are fully accountable for the integrity and reliability of the subsequent decisions made based upon original records, a risk-based review of the content of original records is recommended.

- Systems typically include many metadata fields and audit trails. It is expected that during validation of the system the organization will establish – based upon a documented and justified risk assessment – the frequency, roles and responsibilities, and the approach used to review the various types of meaningful metadata, such as audit trails. For example, under some circumstances, an organization may justify periodic review of audit trails that track system maintenance activities, whereas audit trails that track changes to critical GXP data with a direct impact on patient safety or product quality would be expected to be reviewed each and every time the associated data set is being reviewed and approved – and prior to decision-making. Certain aspects of defining the audit trail review process (e.g. frequency) may be initiated during validation and then adjusted over time during the system life cycle, based upon risk reviews and to ensure continual improvement.
- A risk-based approach to reviewing data requires process understanding and knowledge of the key quality risks in the given process that may impact patients, products, compliance and the overall accuracy, consistency and reliability of GXP decision-making. When original records are electronic, a risk-based approach to reviewing original electronic data also requires an understanding of the computerized system, the data and metadata, and the data flows.
- When determining a risk-based approach to reviewing audit trails in GXP computerized systems, it is important to note that some software developers may design mechanisms for tracking user actions related to the most critical GXP data using metadata features and may not have named these "audit trails" but may instead have used the naming convention "audit trail" to track other computer system and file maintenance activities. For example, changes to scientific data may sometimes be most readily viewed by running various database queries or by viewing metadata fields labelled "history files" or by review of designed and validated system reports, and the files designated by the software developer as audit trails alone may be of limited value for an effective review. The risk-based review of electronic data and metadata, such as audit trails, requires an understanding of the system and the scientific process governing the data life cycle so that the *meaningful metadata* are subject to review, regardless of the naming conventions used by the software developer.
- Systems may be designed to facilitate audit trail review by various means; for example, the system design may permit audit trails to be reviewed as a list of relevant data or by a validated exception reporting process.

- Written procedures for data review should define the frequency, roles and responsibilities and approach to review of meaningful metadata, such as audit trails. These procedures should also describe how aberrant data are to be handled if found during the review. Personnel who conduct such reviews should have adequate and appropriate training in the review process as well as in the software systems containing the data subject to review. The organization should make the necessary provisions for personnel reviewing the data to access the system(s) containing the electronic data and metadata.
- Quality assurance should also review a sample of relevant audit trails, raw data and metadata as part of self-inspection to ensure ongoing compliance with the data governance policy and procedures.
- Any significant variation from expected outcomes should be fully recorded and investigated.
- In the hybrid approach, which is not the preferred approach, paper printouts of original electronic records from computerized systems may be useful as summary reports if the requirements for original electronic records are also met. To rely upon these printed summaries of results for future decision-making, a second person would have to review the original electronic data and any relevant metadata such as audit trails, to verify that the printed summary is representative of all results. This verification would then be documented and the printout could be used for subsequent decision-making.
- The GXP organization may choose a fully electronic approach to allow more efficient, streamlined record review and record retention. This would require authenticated and secure electronic signatures to be implemented for signing records where required. This, in turn, would require preservation of the original electronic records, or true copy, as well as the necessary software and hardware or other suitable reader equipment to view the records during the records retention period.
- System design and the manner of data capture can significantly influence the ease with which data consistency can be assured. For example, and where applicable, the use of programmed edit checks or features such as drop-down lists, check boxes or branching of questions or data fields based on entries are useful in improving data consistency.
- Data and their metadata should be maintained in such a way that they are available for review by authorized individuals, and in a format that is suitable for review for as long as the data retention requirements apply. It is desirable that the data should be maintained

and available in the original system in which they were generated for the longest possible period of time. When the original system is retired or decommissioned, migration of the data to other systems or other means of preserving the data should be used in a manner that preserves the context and meaning of the data, allowing the relevant steps to be reconstructed. Checks of accessibility to archived data, irrespective of format, and including relevant metadata, should be undertaken to confirm that the data are enduring, and continue to be available, readable and understandable by a human being.

Retention of original records or true copies	
Expectations for paper records	**Expectations for electronic records**
Controls for retention of original paper records or true copies of original paper records include, but are not limited to: • controlled and secure storage areas, including archives, for paper records; • a designated paper archivist(s) who is independent of GXP operations is required by GLP guidelines; in other GXPs the roles and responsibilities for archiving GXP records should be defined and monitored (and should normally be the responsibility of the quality assurance function or an independent documentation control unit); • indexing of records to permit ready retrieval; • periodic tests at appropriate intervals based upon risk assessment, to verify the ability to retrieve archived paper or static format records; • the provision of suitable reader equipment when required, such as microfiche or microfilm readers if original paper records are copied as true copies to microfilm or microfiche for archiving;	Controls for retention of original electronic records or true copies of original electronic records include, but are not limited to: • routine back-up copies of original electronic records stored in another location as a safeguard in case of disaster that causes loss of the original electronic records; • controlled and secure storage areas, including archives, for electronic records; • a designated electronic archivist(s) such as is required in GLP guidelines who is independent of GXP operations (the designated personnel should be suitably qualified and have relevant experience and appropriate training to perform their duties); • indexing of records to permit ready retrieval; • periodic tests to verify the ability to retrieve archived electronic data from storage locations. The ability to retrieve archived electronic data from storage locations should be tested during the validation of the electronic archive. After validation the ability to retrieve archived electronic data from the storage locations should be periodically reconfirmed, including retrieval from third-party storage;

Table *continued*

Retention of original records or true copies	
Expectations for paper records	**Expectations for electronic records**
• written procedures, training, review and audit, and self-inspection of processes defining conversion, as needed, of an original paper record to true copy should include the following steps: – a copy/copies is/are made of the original paper record(s), preserving the original record format, the *static format*, as required (e.g. photocopy, scan), – the copy/copies need to be compared with the original record(s) to determine if the copy preserves the entire content and meaning of the original record, that metadata are included, that no data are missing in the copy. The way that the record format is preserved is important for record meaning if the copy is to meet the requirements of a true copy of the original paper record(s), – the verifier documents the verification in a manner securely linked to the copy/copies indicating it is a true copy, or provides equivalent certification.	• the provision of suitable reader equipment, such as software, operating systems and virtualized environments, to view the archived electronic data when required; • written procedures, training, review and audit and self-inspection of processes defining conversion, as needed, of original electronic records to true copy to include the following steps: – a copy/copies is/are made of the original electronic data set, preserving the original record format, the *dynamic format*, as required (e.g. archival copy of the entire set of electronic data and metadata made using a validated back-up process), – a second person verifier or technical verification process (such as use of *technical hash*) to confirm successful backup) whereby a comparison is made of the electronic archival copy with the original electronic data set to confirm the copy preserves the entire content and meaning of the original record (i.e. all of the data and metadata are included, no data are missing in the copy, any dynamic record format that is important for record meaning and interpretation is preserved and the file was not corrupted during the execution of the validated back-up process), – if the copy meets the requirements as a true copy of the original, then the verifier or technical verification process should document the verification in a manner that is securely linked to the copy/copies, certifying that it is a true copy.

Special risk management considerations for retention of original records and/or true copies

- Data and document retention arrangements should ensure the protection of records from deliberate or inadvertent alteration or loss. Secure controls should be in place to ensure the data integrity of the record throughout the retention period. Archival processes should be defined in written procedures and validated where appropriate.
- Data collected or recorded (manually and/or by recording instruments or computerized systems) during a process or procedure should show that all the defined and required steps have been taken and that the quantity and quality of the output are as expected, and should enable the complete history of the process or material to be traced and be retained in a comprehensible and accessible form. That is, original records and/or true copies should be complete, consistent and enduring.
- A true copy of original records may be retained in lieu of the original records only if the copy has been compared to the original records and verified to contain the entire content and meaning of the original records, including applicable metadata and audit trails.
- If true copies of original paper records are made by scanning the original paper and conversion to an electronic image, such as PDF, then additional measures to protect the electronic image from further alteration are required (e.g. storage in a secure network location with access limited to electronic archivist personnel only, and measures taken to control potential use of annotation tools or other means of preventing further alteration of the copy).
- Consideration should be given to preservation where necessary of the full content and meaning of original hand-signed paper records, especially when the handwritten signature is an important aspect of the overall integrity and reliability of the record and in accordance with the value of the record over time. For example, in a clinical trial it may be important to preserve original hand-signed informed consent records throughout the useful life of this record as an essential aspect of the trial and related application integrity.
- True copies of electronic records should preserve the dynamic format of the original electronic data as this is essential to preserving the meaning of the original electronic data, e.g. if the old software or equipment is retired. For example, the original dynamic electronic spectral files created by instruments such as FT-IR, UV/

Vis, chromatography systems and others can be reprocessed, but a pdf or printout is fixed or static and the ability to expand baselines, view the full spectrum, reprocess and interact dynamically with the data set would be lost in the PDF or printout. As another example, preserving the dynamic format of clinical study data captured in an eCRF system allows searching and querying of data, whereas a pdf of the eCRF data, even if it includes a PDF of audit trails, would lose this aspect of the content and meaning of the original eCRF data. Clinical investigators should have access to original records throughout the study and records retention period in a manner that preserves the full content and meaning of the source information. It may be decided to maintain complete copies of electronic data as well as PDF/printed summaries of these electronic data in the archives to mitigate risks of a complete loss of ability to readily view the data should the software and hardware be retired. However, under these circumstances, especially for data that support critical decision-making, even if PDF/printed summaries are maintained, the complete copies of electronic data should continue to be maintained throughout the records retention period to allow for investigations that may be necessary under unexpected circumstances, such as application integrity investigations.

- Preserving the original electronic data in electronic form is also important because data in dynamic format facilitate usability of the data for subsequent processes. For example, having temperature logger data maintained electronically facilitates subsequent tracking and trending and monitoring of temperatures in statistical process control charts.
- In addition to the option of creating true copies of original electronic data as verified back-up copies that are then secured in electronic archives, another option for creating a true copy of original electronic data would be to migrate the original electronic data from one system to another and to verify and document that the validated data migration process preserved the entire content, including all meaningful metadata, as well as the meaning of the original electronic data.
- Electronic signature information should be retained as part of the original electronic record. This should remain linked to the record and be readable throughout the retention period, regardless of the system used for archiving the records.

Accurate

The term "accurate" means data are correct, truthful, complete, valid and reliable.

For both paper and electronic records, achieving the goal of accurate data requires adequate procedures, processes, systems and controls that comprise the quality management system. The quality management system should be appropriate to the scope of its activities and risk-based.

Controls that assure the accuracy of data in paper records and electronic records include, but are not limited to:

- qualification, calibration and maintenance of equipment, such as balances and pH meters, that generate printouts;
- validation of computerized systems that generate, process, maintain, distribute or archive electronic records;
- systems must be validated to ensure their integrity while transmitting between/among computerized systems;
- validation of analytical methods;
- validation of production processes;
- review of GXP records;
- investigation of deviations and doubtful and out-of-specifications results; and
- many other risk management controls within the quality management system.

Examples of these controls applied to the data life cycle are provided below.

Special risk management considerations for assuring accurate GXP records

- The entry of critical data into a computer by an authorized person (e.g. entry of a master processing formula) requires an additional check on the accuracy of the data entered manually. This check may be done by independent verification and release for use by a second authorized person or by validated electronic means. For example, to detect and manage risks associated with critical data, procedures would require verification by a second person, such as a member of the quality unit staff, of: calculation formulas entered into spreadsheets; master data entered into LIMS such as fields for specification ranges used to flag out-of-specification values on the certificate of analysis; and other critical master data, as appropriate.

In addition, once verified, these critical data fields would be locked to prevent further modification, when feasible and appropriate, and only modified through a formal change control process.

- The validity of the data capture process is fundamental to ensuring that high-quality data are produced.
- Where used, standard dictionaries and thesauruses, tables (e.g. units and scales) should be controlled.
- The process of data transfer between systems should be validated.
- The migration of data into and export from systems requires specific planned testing and control.
- Time may not be critical for all activities. When the activity is time-critical, printed records should display the time/date stamp.

For example: To ensure the accuracy of sample weights recorded on a paper printout from the balance, the balance would be appropriately calibrated before use and properly maintained. In addition, synchronizing and locking the metadata settings on the balance for the time/date settings would ensure accurate recordings of time/date on the balance printout.