Working document QAS/15.624
September 2015
Draft document for comment

GUIDANCE ON GOOD DATA AND RECORD MANAGEMENT PRACTICES

(SEPTEMBER 2015)

DRAFT FOR COMMENT

Should you have any comments on the attached text, please send these to Dr S. Kopp, Group Lead, Medicines Quality Assurance, Technologies, Standards and Norms (kopps@who.int) with a copy to Ms Marie Gaspard (gaspardm@who.int) by **30 November 2015**.

Medicines Quality Assurance working documents will be sent out electronically only and will also be placed on the Medicines website for comment under "Current projects". If you do not already receive our draft working documents please let us have your email address (to bonnyw@who.int) and we will add it to our electronic mailing list.

SCHEDULE FOR THE PROPOSED ADOPTION PROCESS OF DOCUMENT QAS/15.624:

GUIDANCE ON GOOD DATA AND RECORD MANAGEMENT PRACTICES

Proposal and need for new guidance document discussed at the informal consultation on inspection, good manufacturing practices and risk management guidance in medicines' manufacturing	28–30 April 2014
Concept paper drafted and proposal presented by Mr I. Thrussell, Expert Inspector, Prequalification Team (PQT)-Inspection to the forty-ninth meeting of the WHO Expert Committee on Specifications for Pharmaceutical Preparations	13–17 October 2014
Preparation of draft document by Mr I. Thrussell in close cooperation with colleagues from PQT-Inspection and a drafting group, including Ms M. Cahilly and national inspectors	October 2014–June 2015
Draft discussed at consultation on data management, bioequivalence, good manufacturing practices and medicines' inspection	29 June–1 July 2015
Revised draft document prepared by the authors, the drafting group, based on the feedback received during the consultation and the subsequent WHO workshop on data management	July–August 2015
Document sent out for comments	September 2015
Compilation of comments received	November 2015
Submission to fiftieth meeting of the WHO Expert Committee on Specifications for Pharmaceutical Preparations	12–16 October 2015
Any further action, as needed and recommended by the WHO Expert Committee on Specifications for Pharmaceutical Preparations	

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 recommended to be developed. 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 Pharmaceuticals Preparations received feedback from this informal consultation during its 49th meeting held in October 2014. A concept paper was received from PQT–Inspections for a proposed structure of a new guidance document which was discussed in detail. The concept paper consolidated existing normative principles and gave some illustrative examples on 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 matters. In view of the increasing number of observations made during inspections regarding data management practices the Committee endorsed the proposal.

Following this endorsement, a draft document was prepared by the colleagues from 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 29 June–1 July 2015.

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

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

This first draft is presented herewith for comments.

CONTENTS

page

GUIDANCE ON GOOD DATA AND RECORD MANAGEMENT PRACTICES

1. INTRODUCTION AND BACKGROUND

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 a 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. Data on which these decisions are based should therefore be complete as well as being accurate, legible, contemporaneous, original and attributable; commonly referred to as "ALCOA".

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

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 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 historical control strategies and apply modern quality risk management and sound scientific principles to current business models (such as out-sourcing and globalization) as well as current technologies in use (such as computerized systems).

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

- a quality risk management 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 govern good data management by first setting realistic and achievable expectations for the true and current capabilities of a process, method, environment, personnel, technologies, etc.;
- management should continuously monitor process capabilities and allocate the necessary resources 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; to provide necessary training for personnel; to allocate the necessary resources to the oversight of contract sites and suppliers to ensure adequate quality standards are met, etc.). Active engagement by 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 in failures so that management has an accurate understanding of risks and can then provide the necessary resources to achieve expectations and data quality standards;
- mapping of data processes and application of modern quality risk management and sound scientific principles across the data life cycle;
- modernization of the understanding of all site personnel in the application of good documentation practices 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 that all necessary controls for good documentation practices 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 and metadata, such as 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

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

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 that 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 assure data reliability and this guidance should be considered in conjunction with existing WHO guidelines and references.

3. GLOSSARY

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

archival. Archiving is the process of protecting records from the ability to be further altered or deleted and storing these records under the control of dedicated data management personnel throughout the required records retention period.

audit trail. An audit trail is a process that captures details such as additions, deletions, or alterations of information in a record, either paper or electronic, without obscuring or over-writing the original record. An audit trail facilitates the reconstruction of the history of such events relating to the record regardless of its media, 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 be 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. Whereas, in electronic records, secure, computer-generated, time-stamped audit trails at both the system and record level should allow for reconstruction of the course of events relating to the creation, modification and deletion of electronic data. Computer-generated audit trails shall retain the original entry and document the user ID, time/date stamp of the action, as well as a reason for the action, 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 over-written. 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 business processes. It includes computer hardware, software, peripheral devices, networks, personnel and documentation, e.g. manuals and standard operating procedures.

data. Data means all original records and certified true copies of original records, including source data and metadata and all subsequent transformations and reports of this data, which are 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 sum total of arrangements to ensure that data, irrespective of the format in which it is generated, are recorded, processed, retained and used to ensure a complete, consistent and accurate record throughout the data lifecycle.

data integrity. Data integrity is the degree to which a collection of data is complete, consistent and accurate throughout the data lifecycle. The collected data should be 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 lifecycle. A planned approach to assessing and managing risks to 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 process by which data is created, processed, reviewed, analyzed and reported, transferred, stored and retrieved, and continuously monitored until retired.

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

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

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 attributable, legible, traceable, permanent, contemporaneously recorded, original and accurate.

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

hybrid approach. The term "hybrid approach" 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. For example, where laboratory analysts use computerized instrument systems that create original electronic records and then print a summary of the results. Persons execute a handwritten signature to electronic records, for example, by hand-signing a review checklist that is then securely linked to the electronic records being signed. The hybrid approach requires a secure link between all record types throughout the records retention period.

quality risk management. A systematic process for the assessment, control, communication and review of risks to the quality of the drug (medicinal) product across the product lifecycle (ICH Q9).

metadata. Metadata are data about data that provide the contextual information required to understand those data. Typically, these are data that describe the structure, data elements, interrelationships and other characteristics of data. They also permit data to be attributable to an individual. For example, in weighing the number 8 is meaningless without metadata, i.e. the unit, mg. Other examples of metadata may include the time/date stamp of the activity, the operator ID of the person who performed the activity, the instrument ID used, processing parameters, sequence files, audit trails and other data required to understand data and reconstruct activities.

static record format. A static record format, such as a paper or pdf record, is one that is fixed and allows no or very limited interaction between the user and the record content. For example, once printed or converted to static pdfs, chromatography records lose the

capabilities of being reprocessed or enabling more detailed viewing of baselines or any hidden fields.

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 (ICH Q10 based in part on ISO 9000:2005).

true copy. A true copy is a copy of an original recording of data that has been 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 metadata and the original record format as appropriate.

4. PRINCIPLES

Good data and record management are critical elements of the pharmaceutical quality system and a systematic approach should be implemented to provide a high level of assurance that across the product life cycle all GxP records and data are accurate, consistent, trustworthy and reliable.

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

Applicability to both paper and electronic data. The requirements for good data and record management 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/ computerized to manual/paper-based systems does not in itself remove the need for robust management controls.

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 that are made on the basis of data provided to them by contract acceptors. Contract givers therefore should perform due diligence to assure themselves that contract acceptors have in place appropriate programmes to ensure the veracity, completeness and reliability of provided data.

Good documentation practices: To achieve robust decisions and data sets based need to be reliable and complete. Good documentation practices (GDP) should be followed in order to ensure all records, both paper and electronic, allow the full reconstruction of the related activities.

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.

Elements of effective management governance should include:

- application of modern quality risk management principles and good data management principles to the current quality management system to integrate those elements that assure the validity, completeness and reliability of data. For example, monitoring of risks

and application of appropriate quality metrics can help management gain the awareness necessary for good decision-making to reduce data integrity risks;
- management should ensure 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;
- management should allocate 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;
- management should also make staff 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.

Quality culture. Management, together with the quality unit, should establish and maintain a working environment often referred to as a quality culture that minimizes the risk of non-compliant records and erroneous records and data. An essential element is the transparent and open reporting of deviations, errors, omissions and aberrant results at all levels of the organization. Steps should be taken to prevent and detect and correct weaknesses in systems and procedures that may lead to data errors so as to continually the improve scientific robustness of decision making of the organization.

Quality risk management and sound scientific principles. Assuring robust decision making requires valid and complete data, appropriate quality and risk management systems, adherence to sound scientific and statistical principles. 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 due 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.

Data life cycle. 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 recorded, processed, reviewed, reported, retained, retrieved and subject to ongoing review. In order 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 lifecycle.

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.

Examples include but are not restricted to:

- restricting access to changing clocks for recording timed events;
- ensuring batch records are accessible at locations where activities take place so that ad hoc data recording and later transcription to official records is not necessary;
- controlling the issuance of blank paper templates for data recording so that all printed forms can be reconciled and accounted for;

- restricting user access rights to automated systems in order to prevent (or audit trail) data amendments;
- ensuring automated data capture or printers are attached to equipment such as balances;
- ensuring proximity of printers to relevant activities;
- ensuring ease of access to locations for sampling points (e.g. sampling points for water systems) such that the temptation to take shortcuts or falsify samples is minimized;
- ensuring access to original electronic data for staff performing data checking activities.

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 and updated as necessary.

5. QUALITY RISK MANAGEMENT TO ENSURE GOOD DATA MANAGEMENT

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 good professional practice. These policies should include expected ethics and proper code of conduct to assure the reliability and completeness of data, including mechanisms for staff to report any questions or concerns to management.

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 data integrity and in turn the risk-based and scientific robustness of decisions based upon that data.

Quality risk management is an essential component of an effective data and record validity program. The effort and resource assigned to data and record governance 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 their potential impact on product quality and patient safety and related decision-making.

Control 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, security controls that prevent persons from altering a master processing formula will reduce the probability of invalid and aberrant data occurring. Such preventive measures, when effectively implemented, also reduce the degree of monitoring required to detect uncontrolled change.

Record and data integrity risks should be assessed, mitigated, communicated and reviewed throughout the data life cycle in accordance with the principles of quality risk management. Example 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 management of data integrity risks based upon their specific GxP activities, technologies and processes.

A data management program developed and implemented, based upon sound quality risk management principles, is expected to leverage existing technologies to their full potential, streamline data processes in a manner that not only improves good data management but also the business process efficiency and effectiveness, thereby reducing costs and facilitating continual improvement.

6. MANAGEMENT GOVERNANCE AND QUALITY AUDITS

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 to ensure 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 programs, 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.

The building blocks of behaviours, procedural/policy considerations and basic technical controls together form the basis of a good data governance foundation upon which future revisions can be built. For example, a good data governance program 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 importance of their role in protecting the safety of the patient and the reputation of the organization for quality products and services.

Management should create a work environment in which staff are encouraged to communicate failures and mistakes, including data reliability issues, so that corrective and preventative 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.

Management reviews and regular reporting of quality metrics facilitate these objectives. This requires designation of a quality manager who has direct access to the highest level of management in order to directly communicate risks so that senior management is aware and can allocate resources to address any issues. 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 to help identify opportunities for improvement. For example:

- tracking and trending the occurrence 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;

- regular review of audit trails may reveal incorrect processing of data and help prevent incorrect results from being reported and identify the need for additional training of personnel;

- routine inspections of computerized systems may reveal gaps in security controls that inadvertently allow personnel to access and potentially alter time/date stamps. These findings help raise awareness to management of need to allocate resources to improve computerized systems validation controls;

- monitoring of contract acceptors and tracking and trending of associated quality metrics for these sites help to better 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.

Quality audits of suppliers, self-inspections and risk reviews should identify and inform management of opportunities to improve foundational systems and processes that impact data reliability. Management allocation of resources to these improvements may most efficiently reduce data integrity risks. For example, identifying and addressing technical difficulties of equipment used to perform multiple GxP operations may greatly improve the reliability of data for all of these operations; identifying security conflicts and allocating independent information technology (IT) 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 efficiencies.

All GxP records held by the GxP organization are subject to inspection by health authorities. This includes original electronic data and metadata, such as audit trails maintained in computerized systems. Management – at both contract givers and contract acceptors – should ensure adequate resources and available procedures, computerized systems and system administrator personnel to readily retrieve these records and facilitate such inspections.

7. CONTRACTED ORGANIZATIONS, SUPPLIERS, AND SERVICE PROVIDERS

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 defined in a contract as described in WHO guidelines should comprehensively address the data integrity processes of both parties covering the outsourced work or services provided.

The organization outsourcing work has 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, such as contracted IT data centres, contracted IT system and database support personnel and cloud computing solution providers.

To fulfil this responsibility, in addition to having their own governance systems, outsourcing organizations should verify the adequacy of comparable systems at the contract acceptor and any significant authorized third parties used by the contract acceptor.

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 evaluation and frequency and approach to monitoring or periodically assessing the contract acceptor should be based upon documented risk assessment that includes an assessment of data processes.

The expected data integrity control strategies should be included in quality agreements and 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 of the data held by the contracted organization 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.

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, in which the data is held, including impact of any laws applicable to that geographic location, should also be considered. Agreements and contracts should establish mutually-agreed upon consequences if the contract acceptor denies, refuses or limits the contract giver's access to their records held by the contract acceptor.

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

8. TRAINING IN GOOD DATA AND RECORD MANAGEMENT

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

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.

Management should also ensure that, at the time of hire and periodically afterwards as needed, all personnel are trained in procedures to ensure GDP for both paper and electronic records. The quality unit should include checks for adherence to GDP 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

The basic building blocks of good GxP data are to follow GDP and then to manage risks to the accuracy, completeness, consistency and reliability of the data throughout its entire period of usefulness – that is, throughout the data life cycle. Each of these essentials – GDP and the data life cycle – are outlined in sections below.

Personnel should follow GDP for both paper records and electronic records in order to assure data integrity. These principles require that documentation have the characteristics of being accurate, legible, contemporaneously recorded, original and attributable (sometimes referred to as ALCOA). These guidelines outline these general ALCOA concepts for both paper and electronic records and provide several examples to aid understanding in the tables below.

World Health Organization

Draft document for comment

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, computer system).

Attributable	
Expectations for paper	**Expectations for electronic**
Attribution of actions in paper records should occur, as appropriate, through the use of: • Initials; • full handwritten signature; or • personal seal.	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; or • electronic signatures, (either biometric or non-biometric).

Special risk management considerations for controls to attribute actions to a unique individual

- *For legally-binding signatures, there should be a verifiable, secure link between unique identifiable, (actual) person signing and the signature event.*

- *Signatures should be executed at the time of signing, with the exception of personal seals that are properly maintained.*

- *Use of a personal seal to sign documents requires additional risk management controls such as procedures that require storage of the seal in a secure location with access limited only to the assigned individual, or other means of preventing potential misuse.*

- *Use of stored digital images of a person's hand-written signature to sign a document is generally not acceptable. This practice compromises the confidence in the authenticity of these signatures when these stored images are not maintained in a secure location with access limited only to the assigned individual or other means of preventing potential misuse, and instead are placed in documents and emails where they can be easily copied and re-used by other persons.*

- *The use of shared and generic log-on credentials should be avoided to ensure that personnel 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 actions may occur (e.g. workstation and server operating systems, etc.). Where adequate technical controls are not available or feasible in legacy electronic systems, combinations of paper and electronic records should be used to meet the requirements to attribute actions to an individual.*

- *A hybrid approach may be used to sign electronic records when the system lacks features for electronic signatures. To execute a hand-written signature to an electronic record, a simple means to do so would be to create a single-page controlled form associated with the written procedures for system use and data review, that would 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 apply a hand-written signature. This paper record with the hand-written 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 certified true copy scanned image of the signature page into the electronic dataset. The hybrid approach is likely to be more burdensome than a fully-electronic approach, therefore, utilizing electronic signatures, whenever available, is recommended.*

- *The use of scribes to record activity on behalf of another operator should be considered only on an exceptional basis and 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 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 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 persons reviewing these records at any point during the records retention period set by the applicable GxP.

Legible, traceable, permanent	
Expectations for paper	**Expectations for electronic**
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 (e.g. that allow persons to detect missing or skipped pages); • controlled issuance of sequentially numbered copies of blank forms (e.g. that allow persons to account for all issued forms); • archival of paper records by independent, designated archivist in secure and controlled paper archives.	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 prior to 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 prior to the next step in the sequence); • use of secure, time-stamped audit trails that independently record operator actions; • configuration settings that limit access to enhanced security rights, (such as the system administrator role that can be used to potentially turn off the audit trails or enable over-writing 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; • strictly controlled configuration and use of data annotation tools in a manner that prevents data in display and prints from being obscured);

Legible, traceable, permanent	
Expectations for paper	**Expectations for electronic**
	• backup of electronic records to ensure disaster recovery; • 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 persons making those changes and those changes should be time stamped and a reason for the change recorded. 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 have the ability to amend or switch off the audit trails or alternate means of providing traceability of user actions.*

- *Where a computerized system lacks computer-generated audit trails, persons may use alternate 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).*

- *Business process owners and users should not be granted enhanced security access permissions, such as system administrator privileges, at any system level (e.g. operating system, application, database), since these enhanced permissions 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 GDP controls for legible and traceable electronic data.*

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

Contemporaneous

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

Contemporaneous	
Expectations for paper	**Expectations for electronic**
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, etc.); • procedures should require that activities be recorded in paper records with the date of the activity (and time as well, if it is a time-sensitive activity).	Contemporaneous recording of actions in electronic records should occur, as appropriate, through use of: • configuration settings and SOPs, as required, that enforce the committing of electronic data to durable media at the time of the activity and prior to proceeding to the next step or event in the sequence of steps and events; • secure system time/date stamps that cannot be altered by personnel; • procedures and maintenance programs that ensure time/date stamps are synchronized across the GxP operations; • controls that allow for the discerning of the timing of one activity relative to another (e.g. time zone controls).

Special risk management considerations for contemporaneous recording of GxP data

- *Training programmes in GDP should emphasize that it is improper 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 improper to back date 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. If a person makes mistakes on a paper document he or she should make single-line corrections, sign and date and 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 permissions to users to rename, copy, 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 includes 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:

- original data should be reviewed;
- original data and/or certified true and exact 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. UV/Vis, FT-IR, ECG, LC/MS/MS, haematology and chemistry analysers, etc.), original electronic data and metadata in automated production systems (e.g. automated filter integrity testers, SCADA, DCS, etc.), original electronic data and metadata in network database systems (e.g. LIMS, ERP, MES, eCRF / EDC, toxicology databases, deviation and CAPA databases, etc.), handwritten sample preparation information in paper notebooks, printed recordings of balance readings, electronic health records, paper batch records.

Review of original records	
Expectations for paper	**Expectations for electronic**
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 that ensure personnel conduct an adequate review and approval of original paper records, including papers used to record the contemporaneous capture of information; • data review procedures should describe review of relevant metadata. For example, written procedures for review should	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 should describe review of original electronic data and relevant metadata. For example, written

Review of original records	
Expectations for paper	**Expectations for electronic**
require that persons 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; • data review should be documented. On 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 persons 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 should describe 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.	procedures for review should require that persons 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; • data review should be documented. 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 persons 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 should describe 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 persons 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, these risks may go undetected and harm may occur.*

- *Although original records should be reviewed, and persons 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.*

- *A risk-based approach to reviewing data requires process understanding and knowledge of the key quality risks in the given process that may impact patient, product, 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 understanding of the computerized system, the data and metadata and 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 not named these audit trails but may 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 is subject to review, regardless of naming conventions used by the software developer.*

- *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 approach to review of the various types of meaningful metadata, such as audit trials. 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 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.*

- *Systems may be designed to facilitate audit trail review via varied 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 on data review should define the frequency, roles and responsibilities, and approach to review of meaningful metadata, such as audit trials. These procedures should also describe how aberrant data is handled if found during the review. Persons 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 persons 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/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 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 that authenticated and secure electronic signatures be implemented for signing records where required. This would require preservation of the original electronic records, or verified true copy, as well as the necessary software and hardware or other suitable reader equipment to view the records during the records retention period.*

Retention of original records or certified true copies	
Expectations for paper	**Expectations for electronic**
Controls for retention of original paper records or certified true copies of original paper records include, but are not limited to: • controlled and secure storage areas, including archives, for paper records; • designated paper archivist(s) who is independent of GxP operations as is already required by GLP guidelines; • indexing of records to permit ready retrieval; • periodic tests to verify the ability to retrieve archived paper or	Controls for retention of original electronic records or certified true copies of original electronic records include, but are not limited to: • routine back-up copies of original electronic records stored in other location as safeguard in case of disaster that causes loss of the original electronic records; • controlled and secure storage areas, including archives, for electronic records; • designated electronic archivist(s) such as those required in GLP

Retention of original records or certified true copies	
Expectations for paper	**Expectations for electronic**
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; • written procedures, training, review and audit and self- inspection of processes defining conversion, as needed, of original paper record to true copy to include the following steps: 1. copy(ies) is(are) made of the original paper record(s), preserving the original record format, the *static format*, as required (e.g. photocopy, pdf), 2. a second person verifier compares the copy(ies) to original record(s) to determine if the copy preserves the entire *content and meaning* of the original record (i.e. all of the data and metadata are included, no data is missing in the copy, the record format is preserved as important for record meaning), 3. if the copy meets the requirements as a true copy of the original paper record(s), then the verifier documents the verification in a manner securely linked to the copy(ies) indicating it is a true copy, or provides equivalent certification.	guidelines who is independent of GxP operations; • indexing of records to permit ready retrieval; • periodic tests to verify the ability to retrieve archived electronic data from storage locations; • the provisioning of suitable reader equipment, such as software, operating systems and virtualized environments, etc., 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: 1. copy(ies) is(are) made of the original electronic data set, preserving the original record format, the *dynamic format*, as required (e.g. back-up copy of the entire set of electronic data and metadata using a validated back-up process), 2. 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 back-up copy to 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 is missing in the copy, dynamic record format is preserved as important for record meaning, and the file was not corrupted during the execution of the validated back-up process), 3. 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(ies), certifying that it is a true copy.

Special risk management considerations for retention of original records and/or certified 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 in fact been taken and that the quantity and quality of the output are as expected, 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 certified true copies should be complete, consistent and enduring.*

- *A certified 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.*

- *If true copies of original paper records are made by scanning the original paper and converting to an electronic image, such as pdf, then additional measures to protect the electronic image from further alteration are required (e.g. storage in secure network location with limited access only to electronic archivist personnel, measures to control potential use of annotation tools or other means of preventing further alteration of the copy).*

- *Considerations should be given to preservation where necessary of the full content and meaning of original hand-signed paper records, especially when the hand-written 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 trail and related application integrity.*

- *Certified true copies of electronic records should preserve the dynamic format of the original electronic data as essential to preserving the meaning of the original electronic data. 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. Also, for example, preserving the dynamic format of clinical study data captured in an electronic case report form (eCRF) system allows searching, 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.

- *Preserving the original electronic data in electronic form is also important since data in dynamic format facilitates greater usability of the data for subsequent processes. For example, 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 certified true copies of original electronic data as verified back-up copies that are then secured in electronic archives, another option to create a certified 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.*

Accurate

The term “accurate” means data are correct, truthful, 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, maintain, distribute or archive electronic records;
- 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.

A few of these controls applied to the data life cycle are mentioned 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 independent verification and release for use by a second authorized person. For example, to detect and manage risks associated with critical data, procedures would require verification by a second person, such as quality unit personnel, of: calculation formulae 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; 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. These risk management measures help ensure accurate results.*

- *To ensure the accuracy of sample weights recorded on paper printout from the balance, the balance would be appropriately calibrated and maintained prior to use. 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.*

(blank page)

World Health Organization

10. DESIGNING SYSTEMS TO ASSURE DATA QUALITY AND RELIABILITY

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 GDP are adhered to for both paper and electronic records should be considered and implemented.

Validation to assure GDP for electronic data

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 GDP will be implemented and that data integrity risks will be properly managed throughout the data life cycle.

WHO Annex 4 provides a more comprehensive presentation of validation considerations. Some of the key aspects of validation that help assure GDP for electronic data will be addressed to include, but are not limited to, the following:

user involvement. Users should be adequately involved in validation activities to define critical data and data lifecycle 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; others.

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

Example activities include, but are not be limited to:

- documenting configuration specifications for commercial off-the-shelf (COTS) systems as well as user-developed systems, as applicable;
- restricting security configuration settings for system administrators to independent persons, where technically feasible;
- disabling configuration settings that allow over-writing and reprocessing of data without traceability;
- restricting access to time/date stamps;
- for systems to be used in clinical trials, configuration and design controls should be implemented to protect the blinding of the trial, for example, by restricting access to who can view randomization data that may be stored electronically.

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 steps of:

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

Example activities might include, but not be limited to:

- determining the risk-based approach to reviewing electronic data and audit trails based upon process understanding and knowledge of potential data impact to product and patient;
- 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 flow of electronic data and all associated metadata, from point of creation through archival and retrieval;
- ensuring relationships between data and metadata are maintained intact throughout data life cycle.

SOPs and training. The validation activities should ensure 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 provide users with ability to efficiently and effectively process data and review electronic data and metadata.

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 ACROSS THE DATA LIFE CYCLE

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 across this process through storage and retrieval.

Quality risk management 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 quality risk management, would be expected to increase the assurance of data integrity as well as result in an effective and efficient business process.

Data integrity risks are likely to occur and be highest when data processes or specific data process steps are inconsistent, subjective, open to bias, unsecured, unnecessarily complex or redundant, undefined, not well understood, manual or paper-based, based upon unproven assumptions and/or not adhering to GDP.

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

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

Example considerations for each phase of the data lifecycle are illustrated below.

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

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, as appropriate for the intended use of this data. Additional controls may include locking critical data entries after the data is verified and review of audit trails for critical data to detect if these had been altered.

Data processing. To ensure data integrity, data processing should occur 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.

Example considerations. GxP organizations should take precautions to discourage testing or processing data toward 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. well characterized secondary standard) is used for system suitability or 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.*

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 or suspect data or rejected data, together with the reported data. This includes a review of the original paper and electronic records.

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?

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.

Whenever out of trend or atypical results are obtained they should be investigated. This includes investigating and determining corrective and preventative 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 its exclusion.

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 to continuously improve. For example, quality metrics data gathered during continuous process verification and analytical method verification and through annual product reviews of data such as adverse events and product complaints help inform efforts to continually enhance product safety, efficacy and quality as well as to inform discovery efforts, such as identifying novel biomarkers for disease that may lead to future product development.

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.

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

Example consideration. 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 results, it will be important to ensure associated metadata are archived with the 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.

12. ADDRESSING DATA RELIABILITY ISSUES

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

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.

Persons 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 persons involved in the data integrity issues, as well as supervisory personnel, quality assurance and management.

The investigation should not be limited to the specific immediate issue identified but should also consider potential impact on historical events. In addition, it will be very important that the deeper, underlying root cause(s) of the issue be considered, including potential management pressures and incentives, including lack of adequate resources that may have led to the issue.

Corrective and preventative actions taken should not only address the identified issue, but also historical events and datasets, 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.

13. REFERENCES AND FURTHER READING

*[**Note from the Secretariat**: Proposals for additional references are being sought.]*

1. WHO good manufacturing practices for Pharmaceutical products: main principles, Annex 2, WHO Technical Report Series 986, 2014.

2. WHO Good manufacturing practices for active pharmaceutical ingredients, Annex 2, WHO Technical Report Series, No. 957, 2010.

3. WHO good practices for pharmaceutical quality control laboratories, WHO Technical Report Series, No. 957, 2010.

4. Supplementary guidelines in 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).

5. Supplementary guidelines in good manufacturing practice: 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).

6. *Good automated manufacturing practice (GAMP) Good Practice Guides: Validation of laboratory computerized systems*. International Society for Pharmaceutical Engineering (ISPE), 2005.

7. *Good automated manufacturing practice (GAMP) Good Practice Guides: Electronic data archiving*. International Society for Pharmaceutical Engineering (ISPE),2007.

8. *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.

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

10. 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*
(http://www.edqm.eu/site/Validation_of_Computerised_Systems_Core_Documentpdf-en-8390-2.html) and its annexes:

– PA/PH/OMCL (08) 87 2R — Annex 1: Validation of computerised calculation systems: example of validation of in-house software
– (http://www.edqm.eu/site/NEW_Annex_1_Validation_of_computerised_calculationpdf-en-8391-2.html)
– PA/PH/OMCL (08) 88 R — Annex 2: Validation of Databases (DB), Laboratory Information Management Systems (LIMS) and Electronic Laboratory Notebooks (ELN)
(http://www.edqm.eu/site/NEW_Annex_2_Validation_of_Databases_DB_Laboratory_pdf-en-8392-2.html) ,
– PA/PH/OMCL (08) 89 R — Annex 3: Validation of computers as part of test equipment
(http://www.edqm.eu/site/NEW_Annex_3_Validation_of_computers_as_part_of_tespdf-en-8393-2.html).

***