World Health Organization

GUIDELINE ON DATA INTEGRITY

(October 2019)

DRAFT FOR COMMENTS

Please send any comments you may have to Dr Sabine Kopp, Group Lead, Medicines Quality Assurance, Technologies Standards and Norms (kopps@who.int), with a copy to Ms Claire Vogel (vogelc@who.int) by 15 January 2020.

Working documents are sent out electronically and they will also be placed on the WHO Medicines website (http://www.who.int/medicines/areas/quality_safety/quality_assurance/guidelines/en/) for comments under the "Current projects" link. If you wish to receive our draft guidelines, please send your email address to jonessi@who.int and your name will be added to our electronic mailing list.

This draft is intended for a restricted audience only, i.e. the individuals and organizations having received this draft. The draft may not be reviewed, abstracted, quoted, reproduced, transmitted, distributed, translated or adapted, in part or in whole, in any form or by any means outside these individuals and organizations (including the organizations' concerned staff and member organizations) without the permission of the World Health Organization. The draft should not be displayed on any website.

Please send any request for permission to:

Dr Sabine Kopp, Group Lead, Medicines Quality Assurance, Technologies Standards and Norms, Department of Essential Medicines and Health Products, World Health Organization, CH-1211 Geneva 27, Switzerland, email: kopps@who.int.

The designations employed and the presentation of the material in this draft do not imply the expression of any opinion whatsoever on the part of the World Health Organization concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries. Dotted lines on maps represent approximate border lines for which there may not yet be full agreement.

The mention of specific companies or of certain manufacturers' products does not imply that they are endorsed or recommended by the World Health Organization in preference to others of a similar nature that are not mentioned. Errors and omissions excepted, the names of proprietary products are distinguished by initial capital letters.

All reasonable precautions have been taken by the World Health Organization to verify the information contained in this draft.

However, the printed material is being distributed without warranty of any kind, either expressed or implied. The responsibility for the interpretation and use of the material lies with the reader. In no event shall the World Health Organization be liable for damages arising from its use.

This draft does not necessarily represent the decisions or the stated policy of the World Health Organization.

SCHEDULE FOR DRAFT WORKING DOCUMENT QAS/19.819:

GUIDELINE ON DATA INTEGRITY

Description of activity	**Date**
Preparation of the document following recommendation of the Fifty-fourth WHO Expert Committee on Specifications for Pharmaceutical Preparations (ECSPP).	October 2019
Mailing of working document inviting comments, including to the Expert Advisory Panel on the International Pharmacopoeia and Pharmaceutical Preparations (EAP), and posting of the working document on the WHO website for public consultation.	November 2019–January 2020
Consolidation of comments received and review of feedback. Preparation of working document for discussion.	March 2019
Discussion of working document and feedback received during the informal Consultation on Screening Technologies, Laboratory Tools and Pharmacopoeial Specifications for Medicines.	Dates tbc
Discussion of working document and feedback received during the informal Consultation on Regulatory Guidance For Multisource Products.	15-16 May 2020
Preparation of working document for next round of public consultation.	May 2020
Consolidation of comments received and review of feedback. Preparation of working document for discussion.	July 2020
Discussion of working document and feedback received during the public consultation and the above meetings in the informal	Dates tbc

Consultation on Good Practices for Health Products Manufacture and Inspection.	
Mailing of the revised working document inviting comments, including to the EAP, and posting the working document on the WHO website for the second round of public consultation.	July 2020
Consolidation of comments received and review of feedbacks. Preparation of working document for discussion.	End of September 2020
Presentation to the Fifty-fourth ECSPP meeting.	12-16 October 2020
Any other follow-up action as required.	

GUIDELINE ON DATA INTEGRITY

1. INTRODUCTION AND BACKGROUND

1.1. Data governance and data integrity (DI) are important elements in ensuring the reliability of data and information obtained in production and control of pharmaceutical products. The data and information should be complete as well as being attributable, legible, contemporaneous, original and accurate, commonly referred to as meeting "ALCOA" principles.

1.2. In recent years, the number of observations made regarding the integrity of data, documentation and record management practices during inspections of good manufacturing practice (GMP), good clinical practice (GCP) and good laboratory practice (GLP) has been increasing. Possible causes for this may include (i) too much reliance on human practices; (ii) the use of computerized systems that are not appropriately managed and validated; and (iii) failure to adequately review and manage original data and records.

1.3. Quality risk management (QRM), control strategies and sound scientific principles are required to mitigate such risks. Examples of controls may include, but are not limited to:

- the establishment and implementation of a DI policy;
- the establishment and implementation of procedures that will facilitate compliance with DI requirements and expectations;
- adoption of a quality culture within the company that encourages personnel to be transparent about failures which includes a reporting mechanism;
- application of QRM with identification of all areas of risk to DI through data integrity risk assessment (DIRA) and implementation of appropriate controls to eliminate or reduce risks to an acceptable level throughout the life cycle of the data;
- ensuring sufficient resources to monitor compliance with DI policies and procedures and processes, and facilitate continuous improvement;

- provision of necessary training for personnel in, for example, good practices (GXP), computerized systems and DI;
- implementation and validation of computerized systems appropriate for their intended use;
- definition and management of appropriate roles and responsibilities for quality agreements and contracts entered into by contract givers and contract acceptors.

2. SCOPE

2.1. This guideline provides information, guidance and recommendations to facilitate compliance with DI, GXP in documentation and record keeping requirements.

2.2. The scope of this guideline is designated as 'GXP'. It does not, however, cover medical devices.

2.3. Where possible, this guideline has been harmonised with other published documents. The guideline should be read with other WHO GXP guidelines and publications.

2.4. In line with the current approach in GMP, it recommends a risk-based approach over the life cycle of data. DIRA should be carried out in order to identify and assess areas of risk.

2.5. The principles of this guideline apply to contract givers and contract acceptors. Contract givers are ultimately responsible for the integrity of data provided to them by contract acceptors. Contract givers should therefore ensure that contract acceptors comply with the principles contained in this guideline.

2.6. Efficient risk-based controls and review of data and documents should be identified and implemented. The effectiveness of the controls should be verified.

3. GLOSSARY

(Note: This section will be updated)

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+.

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.

archiving, archival.

Archiving is the process of storage and protecting records from the possibility of being accessed, 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 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.

audit trail.

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

data governance.

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

data life cycle.

All phases of the process by which data are created, recorded, processed, modified, transmitted, reviewed, reported, used, approved, archived and restored until destruction.

electronic signatures.

A signature in digital form (bio-metric or non-biometric) that represents the signatory. This should be equivalent in legal terms to the handwritten signature of the signatory.

good practices (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 GLP, GCP, GMP, good pharmacovigilance practices (GPP) and good distribution practices (GDP).

metadata.

Metadata are data that describe the attributes of other data and provide context and meaning and form an integral part of original records. An audit trail record is an example of metadata.

raw data (source data).

The original record (data) which can be described as the first-capture of information, whether recorded on paper or electronically.

routine data review.

Routine data review is a process where the raw data and metadata are reviewed for their integrity in an individual data set.

periodic data review.
Periodic data review is a process where an audit of the data generated is done, on a periodic basis (e.g. monthly), where data are selected on a random basis to verify the effectiveness of existing control measures and identification of the possibility of unauthorised activity at all interfaces

4. PRINCIPLES OF DATA INTEGRITY AND GOOD DOCUMENTATION PRACTICES

4.1. There should be a written DI policy.

4.2. Senior management is responsible for the establishment and implementation of an effective quality system and a data governance system. This applies to paper and electronic generated data.

4.3. Data should be Attributable, Legible, Contemporaneous, Original, and Accurate (ALCOA) and be Complete, Consistent, Enduring, and Available (+). This is generally referred to as ALCOA+. (There is no difference in expectations regardless of which acronym is used).

4.4. The quality system, including documentation such as procedures and formats for recording data, should be appropriately designed and implemented to provide assurance that records and data meet the principles contained in this guideline.

4.5. Data governance should address data ownership and accountability throughout the life cycle and consider the design, operation and monitoring of processes/systems to comply with the principles of DI, including control over intentional and unintentional changes to data.

4.6. Data governance systems should include:

- training in the importance of DI principles;

- the creation of an appropriate working environment; and
- active encouragement of the reporting of errors, omissions and undesirable results.

4.7. Senior management should be accountable for the implementation of systems and procedures in order to minimise the potential risk to DI, and to identify the residual risk using risk management techniques such as the principles of the International Conference on Harmonisation (ICH) Q9.

4.8. The data governance programme should include policies and procedures addressing data management. Elements of effective management governance should include:

- management oversight and commitment;
- application of QRM;
- good data management principles;
- quality metrics and performance indicators;
- validation;
- change management;
- security and access control;
- configuration control;
- prevention of commercial, political, financial and other organizational pressures;
- prevention of incentives that may adversely affect the quality and integrity of work;
- adequate resources, systems;
- workload and facilities to facilitate the right environment that supports DI and effective controls;
- monitoring;
- record keeping;
- training; and
- awareness of the importance of DI, product quality and patient safety.

4.9. There should be a system for the regular review of documents and data to identify any DI failures. This includes paper records and electronic records in day-to-day work, system and facility audits and self-inspections.

4.10. The effort and resources applied to assure the integrity of the data should be commensurate with the risk and impact of a DI failure.

4.11. Where DI weaknesses are identified, appropriate corrective and preventive actions (CAPA) should be implemented across all relevant activities and systems and not in isolation.

4.12. Significant DI lapses identified should be reported to the national medicine regulatory authority.

4.13. Changing from automated or computerised systems to paper-based manual systems or vice-versa will not in itself remove the need for appropriate DI controls.

4.14. Good documentation practices should be followed to ensure that all records are complete.

4.15. Records (paper and electronic) should be kept in a manner that ensures compliance with the principles of this guideline. These include, but are not limited to:

- restricting the ability to change dates and times for recording events;
- using controlled documents and forms for recording GXP data;
- controlling the issuance of blank paper templates for data recording of GXP activities, with reconciliation;
- defining access and privilege rights to automated systems;
- enabling audit trails;
- having automated data capture systems and printers connected to equipment and instruments in production and quality control where possible;
- ensuring proximity of printers to sites of relevant activities; and

- ensuring access to original electronic data for personnel responsible for reviewing and checking data.

4.16. Data and recorded media should be durable. Ink should be indelible. Temperature-sensitive or photosensitive inks and other erasable inks should not be used, or other means should be identified to ensure traceability of the data over their life cycle.

4.17. Paper should not be temperature-sensitive, photosensitive or easily oxidizable. If this is not feasible or limited, then true or certified copies should be available.

4.18. Systems, procedures and methodology used to record and store data should be periodically reviewed for effectiveness and updated, as necessary, in relation to new technology.

5. QUALITY RISK MANAGEMENT

5.1. The DIRA should be documented. This should cover systems and processes that produce data or, where data are obtained, data criticality and inherent risks.

5.2. The risk assessment should include, for example, computerised systems, supporting personnel, training and quality systems.

5.3. Record and DI risks should be assessed, mitigated, communicated and reviewed throughout the document and data life cycle.

5.4. Where the DIRA has highlighted areas for remediation, prioritisation of actions (including acceptance of an appropriate level of residual risk) and controls should be documented and communicated. Where long-term remediation actions are identified, risk-reducing short-term measures should be implemented to provide acceptable data governance in the interim.

5.5. Controls identified may include organizational and functional controls such as procedures, processes, equipment, instruments and other systems to both prevent and detect situations that may impact on DI. (Examples include appropriate content and design of procedures, formats for recording, access control, the use of computerized systems and other means).

5.6. Controls should cover risks to data. Risks include deletion of, changes to, and excluding data and results from data sets without written authorisation and detection of those activities and events.

6. MANAGEMENT REVIEW

6.1. Compliance with DI policy and procedures should be reported in the periodic management review meetings.

6.2. The effectiveness of the controls implemented should be measured against the quality metrics and performance indicators. These should include for example:

- The tracking and trending of data;
- lapse in DI rates;
- review of audit trails in, for example, production, quality control, GLP, case report forms and data processing;
- routine audits and/or self-inspections including DI and computerized systems; and
- DI lapses at outsourced facilities (contract acceptors).

7. OUTSOURCING

7.1. Outsourcing of activities and responsibilities of each party (contract giver and contract accepter) should be clearly described in written agreements. Specific attention should be given to ensuring compliance with DI requirements.

7.2. Compliance with the principles and responsibilities should be verified during periodic site audits. This should include the review of procedures and data (including raw data and metadata, paper records, electronic data, audit trails and other related data) held by the contracted organization that are relevant to the contract giver's product or services.

7.3. Where data and document retention are contracted to a third party, particular attention should be paid to understanding the ownership and retrieval of data held under that agreement, as well as controls to ensure the integrity of data over their life cycle.

7.4. No activity, including outsourcing databases, should be sub-contracted to a third party without the prior approval of the contract giver.

7.5. All contracted parties should be aware of the requirements relating to data governance, DI and data management.

8. TRAINING

8.1. Personnel should be trained in DI policies and procedures.

8.2. Personnel should agree to abide by DI principles and should be made aware of the potential consequences in cases of non-compliance.

8.3. Personnel should be trained in good documentation practices and measures to prevent and detect DI 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.

9. DATA

9.1. Data may be presented by manually recording an observation, result or other data and information on paper, or electronically recording thereof, by using equipment and instruments including those linked to computerised systems. A combination of manual and electronic systems may also be used.

9.2. The same considerations for DI apply for other data sets (such as photographs, videos, DVD, imagery and chromatography plates) as for the other data sets, together with any additional controls required for that format such as copying, photography or digitisation. There should be a documented rationale for the selection of such a method.

9.3. Where possible, risk-reducing supervisory measures should be implemented.

9.4. Results and data sets require independent verification if deemed necessary from the DIRA or by another requirement.

10. DATA INTEGRITY

10.1. Data integrity (DI) is the degree to which data are complete, consistent, accurate, trustworthy and reliable.

10.2. Risk-based system design and controls should enable the detection of errors, lapses and omissions of results and data during the data life cycle. Controls may include procedural controls, organizational controls and functional controls.

10.3. The DI policy should clearly define what constitutes raw data, source data, metadata and a “complete data set”.

10.4. Data should be contemporaneously recorded, collected and maintained in a secure manner. Controls should ensure that they are attributable, legible, original (or a true copy) and accurate. Assuring DI requires appropriate QRM systems, including adherence to sound scientific principles and good documentation practices.

10.5. Systems should be established and implemented to ensure that all data acquired, processed and reported are in accordance with the principles in this guideline. Data should be:

- A = attributable to the person generating the data
- L = legible and permanent
- C = contemporaneous
- O = original record (or certified true copy)
- A = accurate

10.6. Data governance measures should also ensure that data are complete, consistent, enduring and available throughout the life cycle, where:

- Complete = the data must be whole; a complete set.
- Consistent = the data must be self-consistent.
- Enduring = durable; lasting throughout the data life cycle.
- Available = readily available for review or inspection purposes.

10.7. Original data should be reviewed, retained, complete, enduring and readily retrievable and readable throughout the records retention period.

11. GOOD DOCUMENTATION PRACTICES

11.1. The principles contained in this guideline are applicable to paper and electronic data.

11.2. Specific controls should be identified through DIRA, to ensure the integrity of data and results recorded on paper records. These may include, but are not limited to:

- the use of permanent, indelible ink;
- no use of pencil or erasers;
- the 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 correction fluid or otherwise obscuring the record;
- controlled issuance of bound, paginated notebooks;
- controlled issuance of sequentially numbered copies of blank forms; and
- archival of paper records by independent, designated personnel in secure and controlled archives.

12. COMPUTERIZED SYSTEMS

(Note. This section highlights some specific aspects relating to the use of computerized systems. It is not intended to repeat the information presented in the other WHO Guidelines here, such as the WHO Guideline on Computerized systems, WHO Guideline on Validation, and WHO Guideline on Good Chromatography Practices. See references.)

12.1. The computerized system selected should suitable for its intended use.

12.2. Where GXP systems are used to acquire, record, store or process data, management should have appropriate knowledge of the risks that the system and users may have on the data.

12.3. Suitably configured and validated software should be used where instruments and equipment with computerised systems are used. The potential for manipulation of data should be eliminated during the data life cycle.

12.4. Where electronic systems with no configurable software and no electronic data retention (e.g. pH meters, balances and thermometers) are used, controls should be put in place to prevent manipulation of data and repeat testing to achieve the desired result.

12.5. Appropriate means of detection for lapses in DI principles should be in place. Additional means should be implemented where stand-alone systems with a user-configurable output is used, for example, Fourier-transform infrared spectroscopy (FTIR) and UV spectrophotometers.

12.6. All records that are defined by the data set should be reviewed and retained. Reduced effort and/or frequency may be justifiable.

Access and privileges

12.7. There should be a documented system in place that defines the access and privileges of users of computerized systems. The paper and electronic records should be in line with the electronic information including the creation and deletion of users.

12.8. Access and privileges should be in accordance with the responsibility and functionality of the individual with appropriate controls to ensure DI (e.g. no modification, deletion or creation of data outside the application is possible).

12.9. A limited number of personnel, with no conflict of interest in data, should be appointed as system administrators. Certain privileges such as data deletion, database amendment or system configuration changes should not be assigned to administrators without justification - and such activities should only be done with documented evidence of authorization by another responsible person. Records should be maintained.

12.10. Unique usernames and passwords should be used for systems as appropriate.

12.11. Programmes and methods (such as acquisition and processing methods) should ensure that data meet ALCOA principles. Where results or data are processed using a different method/parameters than the acquisition method should be recorded. Audit trails and details should allow reconstruction of all data processing activities.

12.12. Data transfer should not result in any changes to the content or meaning of the data. The transfer should be tracked in the audit trail.

12.13. Data transfer should be validated.

Audit Trail

12.14. GXP systems should provide for the retention of audit trails. Audit trails should reflect, for example, users, dates, times, original data and results, changes and reasons for changes.

12.15. Audit trails should be enabled when software is installed, and remain enabled all times. Proof of enabling and verification during the life cycle of data should be maintained.

12.16. Where add-on software or legacy systems are used (with no audit trail), mitigation measures may be taken for defined temporary periods. This should be addressed within defined timelines.

12.17. Routine data review should include a review of audit trails. Evidence should be maintained.

Electronic signatures

12.18. Each electronic signature should be appropriately controlled. An electronic signature should be:

- validated;
- attributable to an individual;
- free from alteration and manipulation; and
- compliant with the requirements of international standards.

12.19. An inserted image of a signature or a footnote indicating that the document has been electronically signed is not adequate.

Data review and approval

12.20. There should be a documented procedure for the routine and periodic review, as well as approval of data.

12.21. CAPAs should be recorded where errors, discrepancies or omissions are identified.

12.22. A conclusion following the review of original data, metadata and audit trail records should be documented, signed and dated.

Data backup, retention, and restoration

12.23. Data should be backed up and archived according to written procedures. The validated procedures and controls should ensure the protection of data and records.

12.24. Data and records should be kept in a secure area which provides appropriate protection. Access should be controlled.

12.25. Retention periods should be defined in authorized procedures.

12.26. Records reflecting documented reasons for the destruction of data should be maintained.

12.27. Backup and restoration processes should be validated and periodically tested, including verification of data size, completeness and accuracy of data and metadata.

13. CORRECTIVE AND PREVENTIVE ACTIONS

13.1. Where organizations use computerized systems (e.g. for GXP data acquisition, processing, interpretation, reporting) which do not meet current GMP requirements, a workplan towards upgrading such systems should be documented and implemented to ensure compliance with current GMP.

13.2. When GMP lapses in DI are identified, root cause analysis, impact and risk assessment should be carried out. Appropriate CAPAs should be established and implemented. Health authorities and other relevant organizations should be notified if the investigation identifies significant impact or risk to materials, products, patients, reported information or data in application dossiers, clinical trial reports, and so on..

References and further reading

(Note: This section will be updated)

1. WHO Basic Principles in Good Manufacturing Practices

2. WHO Guideline on Validation

3. WHO Guideline on Computerized Systems

4. WHO Guideline on Good Chromatography Practices

5. Medicines and Healthcare Products Guideline

6. U.S. Food and Drug Administration Guideline

7. Pharmaceutical Inspection Convention and Pharmaceutical Inspection Co-operation Scheme (PIC/S) Guideline

8. International Society for Pharmaceutical Engineering (ISPE) Baseline

ANNEX 1

EXAMPLES IN DATA INTEGRITY MANAGEMENT

This Annex reflects on some examples in data integrity (DI) management, to support the main text on DI. It should be noted that these are examples and are intended for the purpose of clarification only.

Example 1: Quality risk management and data integrity risk assessment

Risk management is an important part of good manufacturing practices (GMP). Risks should be identified and assessed, control identified and implemented to assist manufacturers in preventing possible DI lapses.

As an example, a Failure Mode and Effects Analysis (FMEA) model (or any other tool) can be used to identify and assess the risks relating to any system where data are, for example, acquired, processed, recorded, saved and archived. Based on severity, occurrence and detection classification and an overall risk priority number or risk factor, corrective and preventive action (CAPA) should be identified, implemented and assessed for its effectiveness.

		Severity		
OCCURRENCE		LOW	MEDIUM	HIGH
	LOW	🟩		
	MEDIUM		🟨	
	HIGH			🟥
		HIGH	MEDIUM	LOW
		Detection		

For example, if during the weighing of a sample, the entry of the date was not contemporaneously recorded on the worksheet but the date is available on the print-out from a weighing balance and log book for the balance for that particular activity, this is still considered

DI. The risk is however different when there is no other means of traceability for the activity. When assessing the risk relating to the lapse in DI, the severity could be classified as "low" (the data is available on the print-out); it does not happen on a regular basis (occurrence is "low"), and it could easily be detected by the reviewer (detection is "high") – therefore the overall risk factor may be considered low. The root cause as to why the record was not made in the analytical report at the time of weighing should still be identified and the appropriate action taken to prevent this from happening.

Example 2: Good documentation practices in data integrity

Documentation should be managed with care. These should be appropriately designed to assist in eliminating erroneous entries, manipulation and human error.

Paper systems

Formats

Formats should be designed and prepared to enable personnel to record the correct information at the right time. Provision should be made for entries such as dates, time (start, finish), signatures, initials, results, batch numbers, equipment identification numbers andso on. The system should prompt the personnel to make the entries at the appropriate step.

Blank forms

The use of blank forms is not encouraged. Where blank forms are used (e.g. to supplement worksheets, laboratory notebooks and master production and control records), appropriate controls have to be in place and may include, for example, a numbered set of blank forms issued which are reconciled upon completion. Similarly, bound paginated notebooks, stamped or formally issued by a document control group, allow the detection of unofficial notebooks and any gaps in notebook pages. Authorization may include two or three signatures with dates, for example, "prepared by" or "entered by", "reviewed by" and "approved by".

Error in recording data

Entries of data and results (electronic and paper records) should be free from mistakes. Entries should be made with care. Where incorrect information had been recorded, this may be corrected provided that the reason for the error is documented, the original entry remains readable, and the correction is signed and dated.

Example 3: Data entry

Data entry includes examples such as sample receiving registration, sample analysis result recording, logbook entries, registers, batch manufacturing record entries, and information in case report forms. The recording of source data on paper records should be in indelible ink and free from errors. Direct entry into electronic records should be done by responsible, appropriately trained individuals. Entries should be traceable to an individual (in electronic records thus having a unique username and password) and traceable to the date (and time, where possible). Where appropriate, the entry should be verified by a second person or entered through technical means such as bar-coding, where possible, 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.

Example 4: Dataset

All data should be included in the dataset unless there is a documented, justifiable, scientific explanation and procedure for the exclusion of any result or data. Whenever out of trend or atypical results are obtained, they should be investigated in accordance with written procedures. This includes investigating and determining CAPA for invalid runs, failures, repeats and other atypical 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 and metadata should not be found in other electronic folders or in other operating system logs. Electronic data should be archived in accordance with a standard operating procedure. It is important to ensure that associated metadata are archived with the relevant data set or securely traceable to the data set through relevant documentation. It should be possible to successfully retrieve data and datasets from the archives. This includes metadata. This should be done in accordance with a procedure and verified at defined intervals.

Example 5: Enduring

Data and metadata should be readable during the life cycle of the data. Risks 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. Data and records should be stored in an appropriate manner, under the appropriate conditions.

Example 6: Attributable

Data should be attributable, thus being traceable to an individual. In paper records, this could be done through the use of initials, full handwritten signature or personal seal. In electronic records, this could be done through the use of unique user logons that link the user to actions that create, modify or delete data; or unique electronic signatures which can be either biometric or non-biometric. An audit trail that captures user identification (ID), date and time stamps, and the electronic signature must be securely and permanently linked to the signed record.

Example 7: Contemporaneous

Personnel should record data and information at the time these are generated and acquired. For example, when a sample is weighed or prepared, the weight of the sample (date, time, name of the person, balance identification number) should be recorded at that time and not before or at a later stage. In the case of electronic data, these should be automatically date and time stamped. The use of hybrid systems is discouraged but where legacy systems are awaiting replacement, documented mitigating controls should be in place. (Replacement of hybrid systems should be a priority with a documented CAPA plan). 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, for example, the act of recording places the product or activity at risk, such as, documenting line interventions by aseptic area operators.

Example 8: Changes

When changes are made to any result or data, the change should be traceable to the person who made the change, the date, time and reason for the change. In electronic systems, this traceability should be documented via computer generated audit trails or in other metadata fields or system features that meet these requirements. Where an existing computerized system lacks computer-generated audit trails, personnel may use alternative means such as procedurally controlled use of log-books, 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.

Example 9: 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 (*see the definition of raw data*). In some cases, the electronic data (electronic chromatogram acquired through high-performance liquid chromatography (HPLC)) may be the original data, and in other cases, the recording of the temperature on a log sheet in a room - by reading the value on a data logger – may be considered the original data. Original data should be reviewed. Proof of review should be presented (e.g. as a signature (reviewed by:) and date of the 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. 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.

Example 10: Controls

Based on the outcome of the data integrity risk assessment (DIRA) (which should cover all areas of data governance and data management) – appropriate and effective controls should be identified and implemented to assure that all data, whether in paper records or electronic records, will meet ALCOA+ principles. Examples of controls may 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 acquire, process, generate, maintain, distribute or archive electronic records;
- validation of systems to ensure that the integrity of data will remain while transmitting between/among computerized systems;
- validation of analytical procedures;
- validation of production processes;
- review of GXP records; and
- investigation of deviations, doubtful, out of trend and out of specifications results.

Points to consider 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;
- formulae for calculations entered into spreadsheets;

- master data entered into the laboratory information management system (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. Once verified, these critical data fields should normally be locked to prevent further modification and only be modified through a formal change control process;
- the process of data transfer between systems should be validated;
- the migration of data into and exported from systems requires specific planned testing and control; and
- when the activity is time-critical, printed records should display the date and time stamp.

***