Drug Data Management Standard

(Exposure Draft)

Translation graciously provided by the China Working Group of Rx-360

Chapter I General Provisions

Article 1 [Purpose] This standard is established for the purpose of standardizing the management of relevant data during the life cycle of drugs and ensuring drug quality and patients' safe and effective use of drugs in accordance with the *Drug Administration Law of the People's Republic of China* and *Enforcement Regulations on the Drug Administration Law of the People's Republic of China*.

Article 2 [Scope] This standard shall be applicable to drug development, production, circulation and relevant activities, including the organizations and individuals engaged in the clinical trial, contract research (CRO), sub-contract production (CMO) and consignment inspection in the above mentioned activities.

Article 3 [Principle] Data management shall run through the whole data life cycle with the principle of trueness, accuracy, promptness, and traceability, so as to ensure the data integrity.

Article 4 [Principle of good faith] Honesty and trustworthiness shall be adhered to during the implementation of this standard, and no pretended acts are allowed.

Chapter II Quality Management

Part I Principles

Article 5 [Quality system] Data management, as a part of the drug quality management system, shall be provided with relevant management regulations, so as to ensure the data integrity.

Article 6 [Risk management] Quality risk management is an important tool and technical means of data management and shall be carried out through the whole data life cycle.

Article 7 [Quality culture] Senior managers shall attach importance to data integrity, advocate open and transparent culture, and encourage employees to report and talk about data integrity problems timely.

Part II Quality Management System

Article 8 [Basic requirement] Appropriate organizational structure and regulations shall be established to monitor and prevent the risks that may affect data integrity.

Article 9 [Problem investigation] The event that goes against the data integrity requirement shall be investigated according to the deviation treatment procedures that have been approved, so as to find out the primary cause and implement the corrective and preventive actions. When reliability of the submitted materials, product quality, and user safety are found to be directly affected during the investigation, it shall be reported to the drug administration department.

Article 10 [Quality audit] Data integrity implementation shall be taken as a part of self-inspection and periodic review, and be reviewed by top managerial staff.

Article 11 [Consignment management] The requirement for data integrity shall be incorporated by the quality agreement or written contract for consignment or procurement activities, with duties of related parties clearly defined. The entrusting party shall take the final responsibility for data integrity and the decisions made based on the data, and periodically check the entrusted party's implementation of data integrity.

Article 12 [Continuous improvement] Implementation of data integrity during the data life cycle shall be put under appropriate and continuous monitoring all the way. Advanced techniques are encouraged to be adopted to control risks in data integrity, promote the continuous improvement of data management, and promote knowledge management and the continuous improvement of product quality.

Article 13 [Quality risk management] Appropriate risk management tools and management strategies shall be employed according to the possible risks of data integrity in GXP activity, technology, and process, so as to ensure the effective management of data integrity risks in the data life cycle.

Chapter III Personnel

Article 14 [Senior managers] Enterprise senior managers shall be responsible for establishing good corporate quality culture and deploying sufficient human resources and technical resources, so as to ensure that the quality system meets the objective requirement of data integrity in the product life cycle. Senior managers shall take the final responsibility for the drug data integrity of the enterprise.

Article 15 [Responsibility of the management] Managerial staff at all levels shall establish and safeguard a quality management system and relevant management regulations for data integrity; ensure employees' work relating to data integrity is not affected by the pressure or motivation from commercial, political, financial and other organizations; and take an active part in and strengthen the activities that can reduce the data integrity risks in technique, method, environment, personnel and technology.

Article 16 [All employees] All employees shall obey the data management standard and the company's relevant management rules; all employees have the responsibility for reporting any problems concerning data integrity, in case the finished product quality and patients' drug use safety are affected.

Article 17 [Training] All employees whose job involves GXP data shall finish the training on data integrity.

Chapter IV Data Management

Part I Principles

Article 18 [Data life cycle] Data management shall run through the whole data life cycle that incorporates data generation (or establishment), acquisition, record, processing, review, report, storage, backup, and destruction.

Article 19 [Data type] Data may be classified into the following types:

(I) Data filled in written record after manual observation;

(II) Data generated by an instrument, device or computerized system;

(III) Objective data acquired by using photographing and shooting technology;

(IV) Information deriving from or obtained according to the original data.

Part II Assignment of Data to Person

Article 20 [Traceability] The person who establishes or revises the data can be found by means of the signature in the record. Revision of the critical data that have been entered shall be approved and be accompanied by the record of reasons for revision.

Article 21 [Unique signature] Different users of the computerized system shall not share the account No. for login, or use the same account No. If the computerized system is not available for technical control, relevant procedures shall be established to sign the electronic record, such as written record or record in a comprehensive way, so as to ensure the operation in the record can be traced back to specific persons.

Article 22 [Electronic signature] An electronic signature shall be equivalent to a written form signature, and shall be verified. An electronic image of a person's written signature shall not be used to replace an electronic signature.

Article 23 [Special case] There shall be document specifying the program, scope of application, relevant operator and recorder under the circumstance when another recorder can work to replace the operator to make records only under special occasions (for example: making record may bring risks to products or the work; for example: in a sterile working area, the operator's recording may intervene with the production line). The record shall be made along with the operation; the operator shall timely sign and confirm the record.

Part III Data Legibility and Traceability

Article 24 [Legibility]At any time within the storage life prescribed by relevant laws and regulations during the drug life cycle, data shall be kept legible, traceable, readable, and understandable, and can clearly reproduce the steps or sequence in which the events occur.

Article 25 [Audit trail] When electronic data are established using a computerized system, all data establishment or alteration behaviors shall be recorded by the audit trail function in the computer system or by other satisfactory meta data field, or other functions of the system, so as to ensure traceability of data.

When the existing computerized system has no audit trial function, other methods can be used to replace it, such as log, alteration control, record version control or combination of written record and electronic record, so as to ensure the traceability of documents.

Article 26 [Management of audit trail] Audit trail or other methods that can ensure the traceability can't be altered or closed.

Article 27 [Senior management permission of the system] The person in charge of the operation flow and users shall not be vested with the right to advanced safety access. For example, they shall not be given the right of a system administrator at any level of

the system (including the operating system, application program, data base etc.).

Part IV Synchronous Record of Data

Article 28 [Requirement] When data are generated or observed, they shall be recorded according to relevant programs or regulations and be saved perpetually before the implementation of the next step of operation.

Article 29 [Official record] Original data shall be directly and synchronously written to the official record when GXP activities occur.

Article 30 [Time stamp] The time/date stamp of the computerized system shall be safe and shall not be falsified; Regulations and maintenance programs shall be established to ensure the synchronism of time and date of GXP activities within the scope mentioned.

Part V Consistency of Original Data

Article 31 [Requirement] Original data include the data and information collected for the first time or at the source, and other data required for the purpose of reproducing GXP activities completely.

GXP's requirements for original data include:

(I) Original data shall be reviewed;

(II) The original data that contain the contents and primary meanings of the data and/or the true duplicate and the confirmed duplicate of the original data shall be kept;

(III) During the retention period, the original record shall meet the requirement of this standard, and be easily obtained and read.

Article 32 [Primary record] When several pieces of information is recorded synchronously, there shall be a standard to define the system that will generate and save the data as the reference data. Attributes of the primary record shall be clearly defined in the quality system, and shall not be changed by certain cases.

Article 33 [Data collection and record] There shall be a program to specify the process of data collection and record, and define necessary steps and expected standard. The data collection and record process shall ensure the data can reproduce the complete history of the record object, and data shall be saved in an understandable and readable way.

Article 34 [Review of original data] Written regulations for data review shall be established, and control measures such as training and self-inspection shall be taken to ensure the appropriate review and approval of the original record. Data review includes the review of data in both paper and electronic form. Review of electronic data shall not be restricted to the review of paper form record printed in the computerized system; it shall also include the review of meta data.

(I) The written regulations shall, on the basis of sufficient risk assessment, specify the process and contents of review of the original data and relevant meta data, including the frequency, roles and responsibilities, review method, process for treatment of abnormal data or errors and deficits, and evaluation of modifications to the original data, and shall meet the requirements of this standard.

(II)The data review process shall be recorded usually with written or electronic

signature. The written regulations shall define the conditions for a signature after review and approval, so as to ensure the review and approval personnel are clear about their duties for guaranteeing data integrity.

(III) The personnel responsible for original data review shall possess relevant qualifications and have received relevant training on the risks of what is to be reviewed.

(IV) Measures shall be taken to ensure the sample related audit trail, and ensure that the original data and meta data are reviewed and are a part of self-inspection, so as to ensure they meet the requirement of this standard permanently.

(V) If the computerized system can't be used for electronic review, and a written form summary report is printed out, there shall be another person assigned to review the original electronic data and relevant meta data, such as audit trail, so as to ensure the summary that has been printed is representative.

Article 35 [Original data translated into a true copy] If the original data need to be translated into a true copy, written regulations shall be established and measures such as training on review and self-inspection shall be taken to ensure the true copy generated and the translation process can ensure data integrity; main requirements include:

(I) Requirements to the form in which the original record is translated into a true copy include:

1. When the original paper form record is made into a true copy in paper form, the static record format of the original record shall be reserved;

2. When the original paper form document is scanned to an electronic image as a true copy, such as PDF, additional measures shall be taken to protect the electronic image from alteration;

3. When the original electronic data set is made into an electronic true copy, the dynamic record format of the original record shall be reserved;

4. When a handwritten signature is critical to the trueness and reliability of record, all the contents and meanings of the paper form record with the original handwritten signature shall be reserved, such as the signature on the Informed Consent Form in a clinical trial.

(II) When the original data are translated into a true copy, the process shall be confirmed by another person or through other technical means, so as to ensure the true copy has kept all contents and meanings of the original record (namely, the true copy contains all data and meta data, there is no data loss, and the record format that is very important to the meanings and explanations of the record is reserved; when necessary, documents shall be confirmed to be undamaged during the verified backup process).

(III) The review contents of the true copy shall be recorded in appropriate means by the person that confirms the process or during the technical review. The record shall be safely linked to the true copy generated.

Article 36 [Data retention] Safe control and filing regulations shall be established to ensure that the original data or the true copy are protected from intentional or unintentional alterations or loss during the retention period, and ensure that they meet

the requirement of data integrity.

(I) The electronic record shall be backed up, so that data can be restored when a disaster occurs.

(II) The record or true copy shall be kept in another safe place.

(III) The backup and restoration process of electronic data shall be verified. The backup data and filed data shall be readable within the retention period, and shall be tested or inspected periodically to ensure their readability.

(IV) The *Good Laboratory Practice* (GLP) specifies that the person in charge of filing shall be independent parties without related interest.

(V)Electronic data can be filed by creating a true copy or being transferred from one system to other systems, but the data transfer process shall be confirmed or verified and recorded. All contents shall be kept in dynamic format, including meaningful meta data and meanings of all original electronic data, so as to ensure the data can be reproduced.

(VI) The electronic signature shall be kept as a part of the electronic original record, and it shall be correlated with the record and be readable during the retention period of the record.

(VII) The data retention period shall meet the relevant requirement of GXP.

Article 37 [Destruction] Regulations for data destruction shall be established, and an approval shall be obtained for data destruction.

Part VI Accuracy and Trueness of Data

Article 38 [Accuracy] The accuracy and trueness of data means that the data can accurately, truly, effectively, and reliably reflect the event/activity that the data record.

The control measures taken to ensure the accuracy and trueness of data include, without limitation to:

(I) The equipment and facilities have been confirmed and calibrated, and maintained.

(II) The computerized system that generates, stores, releases or files the electronic record has been verified.

(III) The analysis procedure and production technology have been verified, and the data generation process shall be kept the same as what has been verified.

(IV) GXP record shall be reviewed.

(V) The deviation, doubtful value, and out-of-specification result shall be investigated.

(VI) An enterprise shall establish a sound document and program system, and set up a perfect work flow to reduce errors.

(VII) Adequate training shall be organized for the personnel involved in the activity.

Article 39 [Data processing] Data processing shall be conducted through the program, process, method, and system and equipment that have been verified/confirmed or

proved. The program and training scheme for data processing shall be approved.

Article 40 [Data monitoring] During the data life cycle, data shall be persistently monitored for the purpose of controlling risks, so that rational decisions can be made for deepening technical understandings, promoting knowledge management, and forming continuous improvement.

Chapter V System

Part I Principles

Article 41 [Principles] The system that is used for data acquisition, storage, processing, analysis, review, report, transfer, backup and/or filing and search can be made in paper form, computerized form, or the combination of both, and:

(I) There shall be regulations and/or configuration that can prevent and/or help to discover the intentional or unintentional alteration, deletion, loss, deficit, replacement, transcription, and other nonconforming treatment of data.

(II) When data are saved in both paper and electronic form, the electronic data shall be taken as the original data. The printed piece of dynamic data can't substitute the electronic original data.

(III) Convenience shall be provided for site operation personnel to fill in or input data.

Article 42 [Data management process] Relevant measures shall be taken according to the risks in data generation, record, storage, and use in the process of data management to ensure data integrity.

(I) The data management system shall be designed to define the belongingness of data in the full life cycle, and on the basis of consideration of process/system design, operation, and monitoring, so as to comply with the data integrity principle. This shall include overall control of intentional or unintentional alteration of information.

(II) Management and design of the data life cycle needs scientific and technical understandings and application of the data management process, including quality risk management. The process shall enhance the guarantee of data integrity, and generate an effective and efficient operation flow.

(III) When the data management process or specific data flow has inconsistency, uncertainty, and no acknowledgment, or involves with manual operation or operation in paper form, management of data integrity shall be enhanced.

(IV) A good design of the data flow shall consider each step of the data flow, try best to ensure and enhance control, and ensure all steps are:

1. Consistent;

2. Objective, independent, and reliable;

3. Simple and simplified;

4. Clearly defined and fully understood;

5. Automatic;

6. Scientifically and statistically rational;

7. Recorded according to the good practice.

Part II Requirement

Article 43 [Requirement for paper record] The distribution and reclamation of paper form blank record (including, but not limited to worksheet, laboratory record and batch record) shall be controlled.

Article 44 [Requirement for the computerized system] The computerized data management system, including the computer hardware, software, peripherals, network, cloud infrastructures, operators and relevant documents (such as the user manual and standard operating procedures) shall meet the requirement of the appendix to the *Computerized System*.

Article 45 [Audit trail] The computerized data management system shall be provided with audit trail according to the risk assessment result to record the operations to the system and data; its contents shall include, but not limited to:

(I) Operator, operation time, operating procedure, and operation reason;

(II) Data creation, modification or deletion, reprocessing, renaming, and transfer;

(III) Alterations or modifications to the setting, configuration, parameters and time stamp of the computerized system;

Article 46 [Review of audit trail] Audit trail shall be considered as a part of GXP to be reviewed; the audit trail of alterations of the key GXP data that can directly affect patient's safety or product quality shall be accompanied by relevant data, and be reviewed before the data are finally approved. The audit trail needing periodic review includes, but not limited to:

(I) Alteration of the final product inspection result;

(II) Alteration of sample operation sequence;

(III) Alteration of sample identifier;

(IV) Alteration of key process parameters.

Article 47 [Verification] The computerized data management system shall be verified according to the requirement for the appendix to the *Computerized System*, so as to ensure the system has the desired usage; for example, to confirm:

(I) The design and configuration that can ensure the data integrity in the application program and operating system (ALCOA), including audit trail, can be started and effective during system operation;

(II) Each workflow has been verified;

(III) The data generated and the report that is output can meet the customer's requirement;

(IV) The user right class complies with its setting and configuration;

(V) The alteration of system date and time, product standard, process parameters and testing method is controlled;

(VI) Configuration and design control of the computerized data management system for clinical trial shall ensure the blindness of the trial, for example, by means of restriction of the personnel who can check the electronically stored non-blind data.

Article 48 [Data safety] The data management system shall be provided with safety measures to ensure the data safety. Common measures include, but not limited to:

(I) Only authorized persons have the right to data storage or processing and the right to enter the documentation room.

(II) The user name is only licensed to the employees who need it in job and who have been authorized.

(III) Users can log in through their unique user name and password.

(IV) There are regulations and training ensuring that when users do not use the system, they can log off or lock screen.

(V) When there is no operation, the system can automatically exit or lock screen within the specified time.

(VI) User password shall be changed within a preset time. A program shall be established or time shall be set in the system to remind users to change the password and forbid the users to use the password that has been used before to log on the system.

Article 49 [System replacement] Replacement of the computerized data management system (including replacement of version and system) shall ensure the data integrity in the system before and after the replacement.

Article 50 [Disaster recovery] Regulations on the operation continuance, system maintenance and disaster recovery shall be established for the computerized data management system, so as to ensure the data integrity during the maintenance, operation continuance and disaster recovery of the system.

Chapter VI Supplementary Provisions

Article 51 [Special requirement] This standard specifies the basic requirement for relevant data in the drug life cycle. The special requirement for clinical trial data, laboratory data, and pharmaceutical equipment data shall be established separately by China Food and Drug Administration in an appendix.

Article 52 [Substitution method] Enterprises can adopt recognized substitution method to meet the requirement of this standard.

Article 53 [Terminology] The following terms bear the meanings as below in this standard:

(I) ALCOA

A common acronym for "trueness, accuracy, promptness and traceability"

(II)Audit trail

Audit trail is a process to catch detailed information, such as addition, deletion, or revision of information in the record; it can be made in both paper and electronic form,

and won't affect or cover the original record. Audit trail can restore or reproduce the history of the event relating to the record and neglect the recording media, such as "who, what, what time, and why" of an action. For example, in a paper form record, the audit trail for revision will be marked using the crossed single line that can ensure the original input is legible and readable; the initials of the name of the person responsible for revision, and the revision date and reasons will also be recorded; the process will be confirmed as required with an explanation of the reasons for the revision. For the electronic record, the safe audit trail system that is generated by the company with a time stamp shall allow the restoration or reproduction of the process of electronic data creation, modification, and deletion relating to an event at the system and record level. The audit trail generated by a computer shall keep the user ID of the original input and document, as well as the action time/date stamp, and action reasons, and confirm and state the reasons for the action as required. The audit trail information generated by a computer may include the discrete event log, history file, database inquiry or report, or other mechanisms that can show the event relating to the special electronic record or special data contained in the record in the computerized system.

(III) Data

Data refer to all original records and the certified true copy of original records that are made during GXP activity and are allowed to sufficiently and completely reproduce and evaluate GXP activity, including source data and meta data, and all subsequent conversions and reports of the data. Data shall be accurately recorded in a fixed way during the activity. Data can be contained in a paper record (such as worksheet and log book), electronic record and audit trail, photo, microfilm or fiche, audio or video document, or any other media that can be used to record relevant information about GXP activity .

(IV) Meta data

Meta data are the data about data, and they provide the contextual information required for understanding these data. Usually, these data describe the structure, data element, correlation and other data characteristics. Meta data also allow the data to be owned personally. For example, during weighing, the figure 8 without meta data is meaningless, unless there is a unit, mg. Other examples of meta data may include the activity time/date stamp, ID of the operator of activity, instrument ID, process parameters, document serial number, audit trail, and other data required for understanding the data and reproducing the activity.

(V) Data management

The sum of operations that can ensure the record, processing, save, and use of data can be completely, conformably and accurately recorded during the full data life cycle despite of the format of generation

(VI) Data integrity

Data integrity refers to the degree by which the data collection is complete, conformable, and accurate during the full data life cycle. The data collected shall be assignable, legible, and recorded synchronously, and shall be the original data or true copy, and are accurate. To ensure the data integrity, an appropriate quality and risk management system is required, including abiding by rational scientific principles and good practice.

(VII) Data life cycle

It refers to a planning method used for the evaluation and management of data risk, so as to ensure the data conformity with the decisions that can potentially affect the patient's safety, product quality and/or that are made in all stages of data creation, processing, review, analysis, report, transfer, storage, and retrieval, persistent monitoring, and retirement.

(VIII) Dynamic record format

It means the record made in a dynamic format, such as the electronic record that allows interactions between the user and the contents recorded. For example, the electronic record made in the format of a database allows tracing, trend analysis and inquiry of data; the chromatogram record maintained through electronic record allows users to reprocess the data, check the hidden fields through appropriate access right, and magnify the baseline to check the point more clearly.

(IX) Mixed mode

It refers to the computerized system that is a comprehensive collection of record combining the original electronic record and paper record. The collection of record shall be reviewed and kept. For example, in a lab, the analyst uses the computerized instrumentation system to create the original electronic record, and then print the result summary. Personnel marks a handwritten signature on the electronic record, for example, by signing the review list manually and then safely connecting it to the electronic record that is being signed. The mixed mode requires a safe connection between all types of records during the full record retention period.

(X) Primary record

When the data collected or retained synchronously through different ways come into conflict with each other, the primary record, namely the master data in the computerized system in the Appendix of GMP, shall be the primary basis for judgment.

(XI) Computerized system

It refers to a computerized system that can control one or more automated operation flows in a centralized way. It includes the computer hardware, software, peripherals, network, personnel and documentations, such as the manual and standard operating procedures.

(XII) Filing

Filing, which runs through the specified record retention period, is to protect the records from further modifications or deletion under the control by specialized data management staff, and to store these records.

(XIII) Backup

A backup refers to the duplicate established for one or more electronic documents when the original data or system are lost or become unavailable (such as, with system crash or disk damage). It is noteworthy that a backup is different from filing. Backup of electronic record is only for the purpose of disaster recovery and it's only stored temporarily, and may be periodically covered. The duplicate that is backed up shall not be considered as filing.

(XIV) Good practice

Among these guiding principles, good practice refers to the measures that can jointly or independently guarantee the documents, whether in paper form or electronic form, are assignable, legible, traceable, permanent, recorded synchronously, original, and accurate.

(XV) Senior manager

The personnel of the highest rank that can command and control the company or site, and have the right to and responsibility for mobilizing the company or site resources (partially based on ICH Q10 of ISO9000:2005)

(XVI) Quality risk management

The system process for evaluation, control, exchange and review of risks in the drug (medical) product life cycle (ICH Q9)

(XVII) GXP

Acronym of the good practice used to standardize the activities of the drugs, biological products, and medical devices under supervision and administration before clinical trial, and during clinical trial, production, and marketing, such as the Good Laboratory Practice, Good Clinical Practice, Good Manufacturing Practice, and Good Supply Practice

(XVIII)Senior executives

The manager and controller of the highest rank in a company or its affiliated area, having the right to and responsibility for mobilizing the company or site resources

Article 54 [Implementation] This standard will be implemented as of _____, 2016.