

衛生福利部食品藥物管理署委辦計畫  
「精進無菌製劑製造品質達國際標準之研究」

**無菌/生物製劑人員 GMP 教育訓練(一)**

日期：(北區)民國 114 年 4 月 8 日

(南區)民國 114 年 4 月 1 日

主辦單位：衛生福利部食品藥物管理署

承辦單位：(TPDA)社團法人中華無菌製劑協會

# 講 師 資 料

張簡雅青 博士 / 社團法人中華無菌製劑協會常務理事

## 時 間 表

| 時間          | 內容  | 講師人選           |
|-------------|---|----------------|
| 09:30-09:40 | 長官致詞  | TFDA<br>監管組代表  |
| 09:40-11:00 | 藥品優良製造規範-數據管理及完整性作業指引(1)<br><ul style="list-style-type: none"> <li>- Introduction &amp; Purpose &amp; Scope</li> <li>- Data governance system</li> <li>- Organisational influences on successful data integrity management</li> </ul>   | 張簡雅青<br>博 士    |
| 11:00-11:10 | 休 息   |                |
| 11:10-12:30 | 藥品優良製造規範-數據管理及完整性作業指引(2)<br><ul style="list-style-type: none"> <li>- General data integrity principles and enablers</li> <li>- Specific data integrity considerations for paper-based systems</li> <li>- Specific data integrity considerations for computerised systems</li> </ul> | 張簡雅青<br>博 士    |
| 12:30-13:30 | 午 餐   |                |
| 13:30-14:50 | 藥品優良製造規範-數據管理及完整性作業指引(3)<br><ul style="list-style-type: none"> <li>- Data integrity considerations for outsourced activities</li> <li>- Regulatory actions in response to data integrity findings</li> <li>- Remediation of data integrity failures</li> </ul>                      | 張簡雅青<br>博 士    |
| 14:50-15:00 | 休 息   |                |
| 15:00-16:20 | 數據完整性(DI)案例分享<br><ul style="list-style-type: none"> <li>- 美國查廠缺失案例</li> </ul>   | 張簡雅青<br>博 士    |
| 16:20-16:30 | 交流討論及課後測驗   | TFDA 長官<br>及講師 |



# 目 錄

## 頁次

|   |     |
|---|-----|
| ◆ Data Management & Integrity in GMP/GDP Environments .....                               | 4   |
| ◆ Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments..... | 5   |
| - Introduction.....   | 7   |
| - Purpose.....  | 10  |
| - Scope.....  | 14  |
| - Data governance system.....   | 15  |
| - Organisational influences on successful data integrity management..                     | 28  |
| - General data integrity principles and enablers.....                                     | 45  |
| - Specific data integrity considerations for paper-based systems.....                     | 61  |
| - Specific data integrity considerations for computerised systems.....                    | 83  |
| - Data integrity considerations for outsourced activities.....                            | 127 |
| - Regulatory actions in response to data integrity findings.....                          | 134 |
| - Remediation of data integrity failures.....   | 141 |
| - Glossary.....   | 150 |
| ◆ US FDA Data Integrity 483.....  | 156 |

# 無菌/生物製劑人員 GMP教育訓練(一)

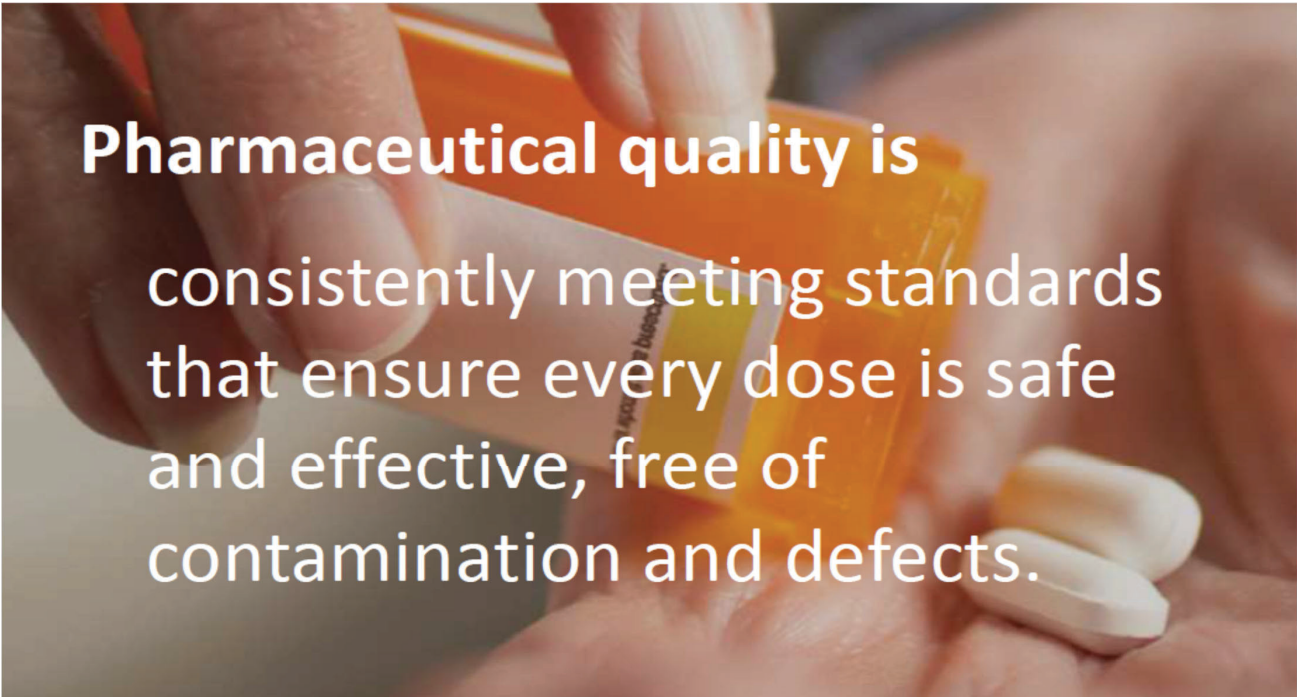
2025/4/1, 2025/4/8

1



**Patients expect safe and effective  
medicine with every dose they take.**

2



**Pharmaceutical quality is**  
consistently meeting standards  
that ensure every dose is safe  
and effective, free of  
contamination and defects.

3



**It is what gives patients confidence**  
in their *next* dose of medicine.

4

# Quality Management Maturity In *YOUR* company

# Data Management & Integrity in GMP/GDP Environments

2025/4/1, 2025/4/8

Eileen Changchien

1

## Learning Objectives

- Data Management & Data Integrity
- Senior Management Responsibility in Data Integrity
- Data lifecycle | Data Criticality | Data Risk
- GDocP for paper-based, electronic-based, and hybrid systems
- Original records vs. true records
- Expectations and Potential risks in Data Integrity (Does and Don'ts )
- Remediations for DI failures

2



PHARMACEUTICAL INSPECTION CONVENTION  
PHARMACEUTICAL INSPECTION CO-OPERATION SCHEME

PI 041-1  
1 July 2021

## PIC/S GUIDANCE

### GOOD PRACTICES FOR DATA MANAGEMENT AND INTEGRITY IN REGULATED GMP/GDP ENVIRONMENTS

© PIC/S 2021  
Reproduction prohibited for commercial purposes.  
Reproduction for internal use is authorised,  
provided that the source is acknowledged.

Editor: PIC/S Secretariat  
e-mail: [info@picscheme.org](mailto:info@picscheme.org)  
web site: <https://www.picscheme.org>

## TABLE OF CONTENTS

|   | Page      |
|---|-----------|
| 1 DOCUMENT HISTORY .....  | 3         |
| 2 INTRODUCTION .....  | 3         |
| 3 PURPOSE .....   | 4         |
| 4 SCOPE .....   | 5         |
| <u>5 DATA GOVERNANCE SYSTEM .....</u>   | <u>5</u>  |
| 5.1 What is data governance? .....  | 5         |
| 5.2 Data governance systems .....   | 6         |
| 5.3 Risk management approach to data governance .....                                     | 7         |
| 5.4 Data criticality .....  | 8         |
| 5.5 Data risk .....   | 8         |
| 5.6 Data governance system review .....   | 9         |
| <u>6 ORGANISATIONAL INFLUENCES ON SUCCESSFUL DATA INTEGRITY<br/>MANAGEMENT .....</u>      | <u>10</u> |
| 6.1 General .....   | 10        |
| 6.2 Policies related to organisational values, quality, staff conduct and ethics .....    | 11        |
| 6.3 Quality culture .....   | 12        |
| 6.4 Modernising the Pharmaceutical Quality System .....                                   | 13        |
| 6.5 Regular management review of performance indicators (including quality metrics) ..... | 14        |
| 6.6 Resource allocation .....   | 14        |
| 6.7 Dealing with data integrity issues found internally .....                             | 15        |
| <u>7 GENERAL DATA INTEGRITY PRINCIPLES AND ENABLERS .....</u>                             | <u>15</u> |



|      |   |    |
|------|---|----|
| 8    | <u>SPECIFIC DATA INTEGRITY CONSIDERATIONS FOR PAPER-BASED SYSTEMS</u>                         | 20 |
| 8.1  | Structure of Pharmaceutical Quality System and control of blank forms/templates/records ..... | 20 |
| 8.2  | Importance of controlling records .....   | 21 |
| 8.3  | Generation, distribution and control of template records .....                                | 21 |
| 8.4  | Expectations for the generation, distribution and control of records .....                    | 21 |
| 8.5  | Use and control of records located at the point-of-use .....                                  | 24 |
| 8.6  | Filling out records .....   | 25 |
| 8.7  | Making corrections on records .....   | 26 |
| 8.8  | Verification of records (secondary checks) .....  | 27 |
| 8.9  | Direct print-outs from electronic systems .....   | 29 |
| 8.10 | Document retention (Identifying record retention requirements and archiving records)          | 29 |
| 8.11 | Disposal of original records or true copies .....   | 30 |
| 9    | <u>SPECIFIC DATA INTEGRITY CONSIDERATIONS FOR COMPUTERISED SYSTEMS</u>                        | 31 |
| 9.1  | Structure of the Pharmaceutical Quality System and control of computerised systems            | 31 |
| 9.2  | Qualification and validation of computerised systems .....                                    | 32 |
| 9.3  | Validation and Maintenance .....  | 33 |
| 9.4  | Data Transfer .....   | 38 |
| 9.5  | System security for computerised systems .....  | 40 |
| 9.6  | Audit trails for computerised systems .....   | 45 |
| 9.7  | Data capture/entry for computerised systems .....   | 47 |
| 9.8  | Review of data within computerised systems .....  | 49 |
| 9.9  | Storage, archival and disposal of electronic data .....                                       | 50 |

114TPDA04006-B

5

|      |   |    |
|------|---|----|
| 9.10 | Management of Hybrid Systems .....                                | 52 |
| 10   | <u>DATA INTEGRITY CONSIDERATIONS FOR OUTSOURCED ACTIVITIES</u>    | 54 |
| 10.1 | General supply chain considerations .....                         | 54 |
| 10.2 | Routine document verification .....                               | 54 |
| 10.3 | Strategies for assessing data integrity in the supply chain ..... | 54 |
| 11   | <u>REGULATORY ACTIONS IN RESPONSE TO DATA INTEGRITY FINDINGS</u>  | 56 |
| 11.1 | Deficiency references .....                                       | 56 |
| 11.2 | Classification of deficiencies .....                              | 57 |
| 12   | <u>REMEDICATION OF DATA INTEGRITY FAILURES</u>                    | 59 |
| 12.1 | Responding to Significant Data Integrity issues .....             | 59 |
| 12.2 | Indicators of improvement .....                                   | 60 |
| 13   | Glossary .....  | 61 |
| 14   | REVISION HISTORY .....  | 63 |

114TPDA04006-B

## 1 DOCUMENT HISTORY

|                                   |             |
|-----------------------------------|-------------|
| Adoption by Committee of PI 041-1 | 1 June 2021 |
| Entry into force of PI 041-1      | 1 July 2021 |

6

- 2. INTRODUCTION

- 2.1 PIC/S Participating Authorities regularly undertake inspections of manufacturers and distributors of Active Pharmaceutical Ingredient (API) and medicinal products in order to determine the level of compliance with Good Manufacturing Practice (GMP) and Good Distribution Practice (GDP) principles. These inspections are commonly performed on-site however may be performed through the remote or off-site evaluation of documentary evidence, in which case the limitations of remote review of data should be considered.

- GMP/GDP compliance 稽核

7

- 2.2 The effectiveness of these inspection processes is determined by the reliability of the evidence provided to the inspector and ultimately the integrity of the underlying data. It is critical to the inspection process that inspectors can determine and fully rely on the accuracy and completeness of evidence and records presented to them.

- 稽核過程決定數據資料之準確性及完整性

8



- 2.3 **Data management** refers to **all** those **activities** performed during the **handling of data** including but not limited to **data policy**, **documentation**, **quality** and **security**. **Good data management** practices influence the quality of all **data generated** and **recorded** by a manufacturer. These practices should ensure that data is **attributable**, **legible**, **contemporaneous**, **original**, **accurate**, **complete**, **consistent**, **enduring**, and **available**. While the main focus of this document is in relation to **GMP/GDP expectations**, the principles herein should also be considered in the **wider context** of good data management such as data included in the **registration dossier** based on which **API** and **drug product** control strategies and specifications are set.

- 數據處理的幾個步驟及注意事項 | 查登文件

- 2.4 **Good data management** practices apply to all elements of the **Pharmaceutical Quality System** and the **principles** herein apply equally to data generated by **electronic** and **paper-based** systems.

- 紙本及電子文件都是相同的數據管理要求

- 2.5 Data Integrity is defined as “the degree to which data are complete, consistent, accurate, trustworthy, and reliable and that these characteristics of the data are maintained throughout the data life cycle”.<sup>1</sup> This is a fundamental requirement for an effective Pharmaceutical Quality System which ensures that medicines are of the required quality. Poor data integrity practices and vulnerabilities undermine the quality of records and evidence, and may ultimately undermine the quality of medicinal products.
- <sup>1</sup> ‘GXP’ Data Integrity Guidance and Definitions, MHRA, March 2018

- 數據之可靠性 | PQS說明 | 損害信任度

11

- 2.6 The responsibility for good practices regarding data management and integrity lies with the manufacturer or distributor undergoing inspection. They have full responsibility and a duty to assess their data management systems for potential vulnerabilities and take steps to design and implement good data governance practices to ensure data integrity is maintained.
- DI是製造廠及分銷廠的職責

12

- 3. **PURPOSE**

- 3.1 This document was written with the aim of:

- 3.1.1 Providing guidance for Inspectorates in the interpretation of GMP/GDP requirements in relation to good data management and the conduct of inspections.

- 對data management檢查要求 | GMP/GDP

13

- 3.1.2 Providing consolidated, illustrative guidance on risk-based control strategies which enable the existing requirements for data to be valid, complete and reliable as described in PIC/S Guides for GMP<sup>2</sup> and GDP<sup>3</sup> to be implemented in the context of modern industry practices and globalised supply chains.

- <sup>2</sup> PIC/S PE 009 Guide to Good Manufacturing Practice for Medicinal Products, specifically Part I chapters 4, 5, 6, Part II chapters 5, 6 & Annex 11

- <sup>3</sup> PIC/S PE 011 Guide to Good Distribution Practice for Medicinal Products, specifically sections 3, 4, 5 & 6

- ICH Q9管控策略

14

- 3.1.3 Facilitating the effective **implementation** of good data management elements **into** the **routine** planning and conduct of GMP/GDP **inspections**; to provide a **tool** to **harmonise** GMP/GDP **inspections** and to ensure the **quality** of inspections with regards to **data integrity** expectations.

- DI | GMP/GDP稽核

15

- 3.2 This guidance, together with **Inspectorate resources** such as **aide memoire**, should **enable** the **inspector** to make an optimal use of the **inspection time** and an **optimal evaluation** of data integrity elements during an inspection.
- 3.3 Guidance herein should assist the Inspectorate in **planning** a **risk-based inspection** relating to **good data management practices**.

- 稽核優良數據管理以風險來考量及規劃

16

- 3.4 Good data management has always been considered an **integral** part of **GMP/GDP**. Hence, this guide is **not** intended to impose **additional** regulatory burden upon regulated entities, rather it is intended to provide guidance on the **interpretation** of **existing GMP/GDP requirements** relating to **current** industry data management practices.

- 數據管理是GMP/GDP

17

- 3.5 The **principles** of data management and integrity apply **equally** to **paper-based, computerised** and **hybrid** systems and should **not** place any **restraint** upon the development or adoption of **new concepts** or **technologies**. In accordance with **ICH Q10** principles, this guide should facilitate the **adoption** of **innovative** technologies through **continual** improvement.

- 任何型式數據要求皆相同 | Q10 PQS

18

- 3.6 The term “Pharmaceutical Quality System” is predominantly used throughout this document to denote the quality management system used to manage and achieve quality objectives. While the term “Pharmaceutical Quality System” is used predominantly by GMP regulated entities, for the purposes of this guidance, it should be regarded as interchangeable with the term “Quality System” used by GDP regulated entities.

- PQS | QMS | QS

19

- 3.7 This guide is not mandatory or enforceable under law. It is not intended to be restrictive or to replace national legislation regarding data integrity requirements for manufacturers and distributors of medicinal products and actives substances (i.e. active pharmaceutical ingredients). Data integrity deficiencies should be referenced to national legislation or relevant paragraphs of the PIC/S GMP or GDP guidance.

- DI是GMP/GDP要求

20

- 4. SCOPE

- 4.1 The guidance has been written to apply to on-site inspections of those sites performing manufacturing (GMP) and distribution (GDP) activities. The principles within this guide are applicable for all stages throughout the product lifecycle. The guide should be considered as a non-exhaustive list of areas to be considered during inspection.

- 藥品生命週期都要符合DI要求

21

- 4.2 The guidance also applies to remote (desktop) inspections of sites performing manufacturing (GMP) and distribution (GDP) activities, although this will be limited to an assessment of data governance systems. On-site assessment is normally required for data verification and evidence of operational compliance with procedures.

- 遠端及實體稽核

22

- 4.3 Whilst this document has been written with the above scope, many principles regarding good data management practices described herein have applications for other areas of the regulated pharmaceutical and healthcare industry.
- 4.4 This guide is not intended to provide specific guidance for “for-cause” inspections following detection of significant data integrity vulnerabilities where forensic expertise may be required.

- 優良數據管理

23

## ● 5. DATA GOVERNANCE SYSTEM

### ● 5.1 What is data governance?

- 5.1.1 Data governance is the sum total of arrangements which provide assurance of data integrity. These arrangements ensure that data, irrespective of the process, format or technology in which it is generated, recorded, processed, retained, retrieved and used will ensure an attributable, legible, contemporaneous, original, accurate, complete, consistent, enduring, and available record throughout the data lifecycle. While there may be no legislative requirement to implement a ‘data governance system’, its establishment enables the manufacturer to define, prioritise and communicate their data integrity risk management activities in a coherent manner. Absence of a data governance system may indicate uncoordinated data integrity systems, with potential for gaps in control measures.

- 說明data governance之定義

24



- 5.1.2 The **data lifecycle** refers to how data is generated, processed, reported, checked, used for decision-making, stored and finally discarded at the end of the retention period. Data relating to a product or process may cross various boundaries within the lifecycle. This may include **data transfer** between paper-based and computerised systems, or between different organisational boundaries; both **internal** (e.g. between production, QC and QA) and **external** (e.g. between service providers or contract givers and acceptors).“

- 說明data lifecycle定義 | 橫跨不同界面

25

- 5.2 Data governance systems

- 5.2.1 **Data governance systems** should be **integral** to the Pharmaceutical Quality System described in PIC/S GMP/GDP. It should address **data ownership** throughout the **lifecycle**, and consider the **design, operation and monitoring** of processes and systems in order to **comply with** the principles of **data integrity**, including **control** over **intentional** and **unintentional** changes to, and **deletion** of information.

- 避免蓄意及不小心變更或刪除

26

- 5.2.2 Data governance systems **rely on** the incorporation of **suitably designed systems**, the **use of technologies** and **data security** measures, combined with **specific expertise** to ensure that **data management** and **integrity** is effectively **controlled**. Regulated entities should **take steps** to ensure appropriate **resources** are **available** and applied in the **design, development, operation** and **monitoring** of the **data governance** systems, commensurate with the **complexity** of systems, operations, and data **criticality** and **risk**.
- 設計數據管理系統及其運轉以符合DI

27

- 5.2.3 The **data governance system** should ensure **controls** over the **data lifecycle** which are commensurate with the **principles** of quality risk management. These controls may be:
  - **Organisational**
    - **procedures**, e.g. **instructions** for **completion** of records and **retention** of completed records;
    - **training** of **staff** and documented **authorisation** for **data generation** and **approval**;
    - **data governance system** design, considering how data is **generated, recorded, processed, retained** and **used**, and **risks** or **vulnerabilities** are **controlled** effectively;
    - **routine** (e.g. daily, batch- or activity-related) **data verification**;
    - **periodic surveillance**, e.g. self-inspection processes seek to verify the effectiveness of the data governance system; or
    - the use of personnel with **expertise** in data management and integrity, including expertise in data security measures.

28

- 5.2.3 cont'd

- **Technical**

- computerised system validation, qualification and control;
- automation; or
- the use of technologies that provide greater controls for data management and integrity.

- 數據管理體系

29

- 5.2.4 An effective data governance system will demonstrate Senior management's understanding and commitment to effective data governance practices including the necessity for a combination of appropriate organisational culture and behaviours (section 6) and an understanding of data criticality, data risk and data lifecycle. There should also be evidence of communication of expectations to personnel at all levels within the organisation in a manner which ensures empowerment to report failures and opportunities for improvement. This reduces the incentive to falsify, alter or delete data.

- 高階管理層之承諾 | 鼓勵舉報不符合DI

30

- 5.2.5 The organisation's arrangements for data governance should be documented within their Pharmaceutical Quality System and regularly reviewed.

- 數據管理系統之架構必須文件化

31

- 5.3 Risk management approach to data governance

- 5.3.1 Senior management is responsible for the implementation of systems and procedures to minimise the potential risk to data integrity, and for identifying the residual risk, using the principles of ICH Q9. Contract Givers should perform a review of the contract acceptor's data management policies and control strategies as part of their vendor assurance programme. The frequency of such reviews should be based on the criticality of the services provided by the contract acceptor, using risk management principles (refer to section 10).

- 高階管理層督導 | 委外活動確保數據管理

32

- 5.3.2 The effort and resource assigned to data governance should be commensurate with the risk to product quality, and should also be balanced with other quality resource demands. All entities regulated in accordance with GMP/GDP principles (including manufacturers, analytical laboratories, importers and wholesale distributors) should design and operate a system which provides an acceptable state of control based on the data quality risk, and which is documented with supporting rationale.

- 數據治理管理機制與藥品的品質風險相符合

33

- 5.3.3 Where long term measures are identified in order to achieve the desired state of control, interim measures should be implemented to mitigate risk, and should be monitored for effectiveness. Where interim measures or risk prioritisation are required, residual data integrity risk should be communicated to senior management, and kept under review. Reverting from automated and computerised systems to paper-based systems will not remove the need for data governance. Such retrograde approaches are likely to increase administrative burden and data risk, and prevent the continuous improvement initiatives referred to in paragraph 3.5.

- 短中長期計畫必須符合風險管理

34

- 5.3.4 Not all data or processing steps have the same importance to product quality and patient safety. Risk management should be utilised to determine the importance of each data/processing step. An effective risk management approach to data governance will consider:
  - **Data criticality** (impact to decision making and product quality) and
  - **Data risk** (opportunity for data alteration and deletion, and likelihood of detection / visibility of changes by the manufacturer's routine review processes).
- From this information, risk proportionate control measures can be implemented. Subsequent sections of this guidance that refer to a risk management approach refer to 'risk' as a combination of data risk and data criticality concepts."
- Data criticality, data risk 定義

35

- 5.4 Data criticality
- 5.4.1 The decision that data influences may differ in importance and the impact of the data to a decision may also vary. Points to consider regarding data criticality include:
  - Which decision does the data influence?
  - **For example:** when making a batch release decision, data which determines compliance with critical quality attributes is normally of greater importance than warehouse cleaning records.
  - What is the impact of the data to product quality or safety?
  - **For example:** for an oral tablet, API assay data is of generally greater impact to product quality and safety than tablet friability data.

36

- **5.5 Data risk**

- 5.5.1 Whereas data integrity requirements relate to all GMP/GDP data, the assessment of data criticality will help organisations to prioritise their data governance efforts. The rationale for this prioritisation should be documented in accordance with quality risk management principles.

- DI GMP/GDP

37

- 5.5.2 Data risk assessments should consider the vulnerability of data to involuntary alteration, deletion, loss (either accidental or by security failure) or re-creation or deliberate falsification, and the likelihood of detection of such actions. Consideration should also be given to ensuring complete and timely data recovery in the event of a disaster. Control measures which prevent unauthorised activity, and increase visibility / detectability can be used as risk mitigating actions.

- 數據的風險評估

38

- 5.5.3 Examples of **factors** which can increase **risk of data failure** include processes that are **complex**, or **inconsistent**, with **open ended** and **subjective outcomes**. **Simple** processes with tasks which are **consistent**, well defined and objective lead to reduced risk.

- 製程的複雜程度與數據失敗的風險有關

39

- 5.5.4 Risk assessments should focus on a **business process** (e.g. **production, QC**), evaluate **data flows** and the **methods of generating** and **processing** data, and **not** just **consider** information technology (IT) system functionality or complexity. **Factors** to consider include:
- **process complexity** (e.g. **multi-stage** processes, **data transfer** between processes or systems, complex **data processing**);
- **methods of generating, processing, storing** and **archiving** data and the **ability to assure data quality** and **integrity**;

- 了解數據流及數據處理程序

40



- 5.5.4 cont'd

- process consistency (e.g. biological production processes or analytical tests may exhibit a higher degree of variability compared to small molecule chemistry);
- degree of automation / human interaction;
- subjectivity of outcome / result (i.e. is the process open-ended vs well defined);
- outcomes of a comparison between electronic system data and manually recorded events (e.g. apparent discrepancies between analytical reports and raw-data acquisition times); and
- inherent data integrity controls incorporated into the system or software.

41

- 5.5.5 For computerised systems, manual interfaces with IT systems should be considered in the risk assessment process. Computerised system validation in isolation may not result in low data integrity risk, in particular, if the user is able to influence the reporting of data from the validated system, and system validation does not address the basic requirements outlined in section 9 of this document. A fully automated and validated process together with a configuration that does not allow human intervention, or reduces human intervention to a minimum, is preferable as this design lowers the data integrity risk. Appropriate procedural controls should be installed and verified where integrated controls are not possible for technical reasons.

- 人機界面之管控

42

- 5.5.6 Critical thinking skills should be used by inspectors to determine whether control and review procedures effectively achieve their desired outcomes. An indicator of data governance maturity is an organisational understanding and acceptance of residual risk, which prioritises actions. An organisation which believes that there is 'no risk' of data integrity failure is unlikely to have made an adequate assessment of inherent risks in the data lifecycle. The approach to assessment of data lifecycle, criticality and risk should therefore be examined in detail. This may indicate potential failure modes which can be investigated during an inspection.

- GMP/GDP inspector 考量點

43

- 5.6 Data governance system review 重要
- 5.6.1 The effectiveness of data integrity control measures should be assessed periodically as part of self-inspection (internal audit) or other periodic review processes. This should ensure that controls over the data lifecycle are operating as intended.
- 內稽包括：DI管控機制有效性

44

- 5.6.2 In addition to routine data verification checks (e.g. daily, batch- or activity-related), self-inspection activities should be extended to a wider review of control measures, including:
  - A check of continued personnel understanding of good data management practice in the context of protecting of the patient, and ensuring the maintenance of a working environment which is focussed on quality and open reporting of issues (e.g. by review of continued training in good data management principles and expectations).

- 常規數據確認機制 | DI教育訓練

45

- 5.6.2 cont'd
  - A review for consistency of reported data/outcomes against raw entries. This may review data not included during the routine data verification checks (where justified based on risk), and/or a sample of previously verified data to ensure the continued effectiveness of the routine process.
  - A risk-based sample of computerised system logs / audit trails to ensure that information of relevance to GMP/GDP activity is reported accurately. This is relevant to situations where routine computerised system data is reviewed manually or by a validated 'exception report'<sup>4</sup>.
  - <sup>4</sup> An 'exception report' is a validated search tool that identifies and documents predetermined 'abnormal' data or actions, which requires further attention or investigation by the data reviewer.

46

- 5.6.2 cont'd

- A review of quality system metrics (i.e. trending) that may also be indicators of data governance effectiveness.

- PQS 系統趨勢分析 | 不斷進步之用 | 作為其他用途宜謹慎

47

- 5.6.3 An effective review of the data governance system will demonstrate understanding regarding importance of interaction of company behaviours with organisational and technical controls. The outcome of the review should be communicated to senior management, and be used in the assessment of residual data integrity risk.

- 有效性評估結果要向高階管理層報告

48

- 6 ORGANISATIONAL INFLUENCES ON SUCCESSFUL DATA INTEGRITY MANAGEMENT

- 6.1 General

- 6.1.1 It may **not** be appropriate or possible to report an inspection **deficiency** relating to **organisational behaviour**. An **understanding** of **how** behaviour **influences** (i) the **incentive** to **amend**, **delete** or **falsify** data and (ii) the **effectiveness** of **procedural controls** designed to **ensure** data integrity, can **provide** the **inspector** with **useful indicators** of risk which can be **investigated further**.

- 企業文化

49

- 6.1.2 **Inspectors** should be **sensitive** to the **influence of culture** on **organisational behaviour**, and apply the **principles** described in this section of the guidance in an appropriate way. An **effective** 'quality culture' and **data governance** may be **different** in its implementation from **one location** to **another**. However, where it is **apparent** that **cultural approaches** have **led to** data integrity **concerns**; these **concerns** should be **effectively** and **objectively** reported by the **inspector** to the **organisation** for **rectification**.

- 品質文化

50

- 6.1.3 Depending on **culture**, an organisation's **control measures** may be:
  - **'open'** (where **hierarchy** can be **challenged** by subordinates, and **full** reporting of a **systemic** or **individual** failure is a **business expectation**)
  - **'closed'** (where **reporting failure** or **challenging** a hierarchy is culturally more **difficult**)

- 兩種型態企業文化

51

- 6.1.4 **Good** data governance in **'open'** cultures may be facilitated by **employee empowerment** to **identify** and **report** issues **through** the Pharmaceutical Quality System. In **'closed'** cultures, a greater **emphasis** on **oversight** and **secondary review** may be **required** to **achieve** an **equivalent level** of control **due to** the **social barrier** of communicating **undesirable information**. The **availability** of a **confidential escalation process** to **senior** management may also be of **greater importance** in this situation, and these arrangements should clearly **demonstrate** that **reporting** is actively **supported** and **encouraged** by **senior** management.

- 向上報告的企業文化

52

- 6.1.5 The extent of Management's knowledge and understanding of data integrity can influence the organisation's success of data integrity management. Management should know their legal and moral obligation (i.e. duty and power) to prevent data integrity lapses from occurring and to detect them, if they should occur. Management should have sufficient visibility and understanding of data integrity risks for paper and computerised (both hybrid and electronic) workflows.

- 管理層必須深入了解內部DI流程及管控

53

- 6.1.7 Data integrity breaches can occur at any time, by any employee, so management needs to be vigilant in detecting issues and understand reasons behind lapses, when found, to enable investigation of the issue and implementation of corrective and preventive actions.

- 管理層要警覺DI問題

54

- 6.1.8 There are **consequences** of data integrity lapses that **affect** the various **stakeholders** (patients, regulators, customers) including directly impacting **patient safety** and undermining **confidence** in the organisation and its products. **Employee** awareness and understanding of these **consequences** can be helpful in fostering an environment in which **quality is a priority**.

- 全員了解DI過失的後果 | 建立品質優先的認知

55

- 6.1.9 Management should **establish controls** to **prevent, detect, assess** and **correct** data integrity breaches, as well as **verify** those controls are **performing** as intended to **assure** data integrity. Sections **6.2 to 6.7** outline the **key items** that Management should **address** to **achieve success** with **data integrity**.

- 建立DI監督管控機制

56



- 6.1.10 Senior Management should have an appropriate level of understanding and commitment to effective data governance practices including the necessity for a combination of appropriate organisational culture and behaviours (section 6) and an understanding of data criticality, data risk and data lifecycle. There should also be evidence of communication of expectations to personnel at all levels within the organisation in a manner which ensures empowerment to report failures and opportunities for improvement. This reduces the incentive to falsify, alter or delete data.

- 高階管理層應該要做的事情

57

## ● 6.2 Policies related to organisational values, quality, staff conduct and ethics

- 6.2.1 Appropriate expectations for staff conduct, commitment to quality, organisational values and ethics should clearly communicated throughout the organisation and policies should be available to support the implementation and maintenance of an appropriate quality culture. Policies should reflect Management's philosophy on quality, and should be written with the intent of developing an environment of trust, where all individuals are responsible and accountable for ensuring patient safety and product quality.

- 組織價值觀 | 政策導向 | 信賴的環境 | 確保病人安全及產品品質

58

- 6.2.2 Management should make personnel aware of the importance of their role in ensuring data quality and the implication of their activities to assuring product quality and protecting patient safety.

- 讓全員了解DI重要性及對品質及病人的影響

59

- 6.2.3 Policies should clearly define the expectation of ethical behaviour, such as honesty. This should be communicated to and be well understood by all personnel. The communication should not be limited only to knowing the requirements, but also why they were established and the consequences of failing to fulfil the requirements.

- 公司政策 | 倫理行為 | 不符合DI要求之後果

60

- 6.2.4 Unwanted behaviours, such as deliberate data falsification, unauthorised changes, destruction of data, or other conduct that compromises data quality should be addressed promptly. Examples of unwanted behaviours and attitudes should be documented in the company policies. Actions to be taken in response to unwanted behaviours should be documented. However, care should be taken to ensure that actions taken, (such as disciplinary actions) do not impede any subsequent investigation into the data integrity issues identified, e.g. severe retribution may prevent other staff members from disclosing information of value to the investigation.

- 不受歡迎的行為 | 懲罰措施 | 避免嚴重處罰造成禁言

61

- 6.2.5 The display of behaviours that conform to good practices for data management and integrity should be actively encouraged and recognised appropriately.

- 稱讚遵守DI的良好行為

62

- 6.2.6 There should be a **confidential escalation program** supported by company **policies** and **procedures** whereby it encourages personnel to bring instances of **possible breaches** of policies to the attention of **senior management** without consequence for the **informer/employee**. The potential for breaches of the policies by senior management should be **recognised** and a suitable **reporting mechanism** for those cases should be available.

- 向上舉發違反DI機制

63

- 6.2.7 Where possible, management should **implement** systems with **controls** that **by default, uphold** the **intent** and **requirements** of **company policies**.

- 管理層執行公司政策所規定的事項

64

- 6.3 Quality culture

- 6.3.1 Management should aim to **create** a work environment (i.e. **quality culture**) that is **transparent** and **open**, one in which personnel are encouraged to **freely** communicate **failures** and **mistakes**, **including** potential data reliability issues, so that **corrective** and **preventive actions** can be taken. Organisational **reporting structure** should permit the **information flow** between personnel **at all levels**.

- 品質文化 | 透明公開 | 討論報告DI問題

65

- 6.3.2 It is the **collection** of **values**, **beliefs**, **thinking**, and **behaviours demonstrated** consistently **by** management, team leaders, quality personnel and **all personnel** that **contribute to creating** a **quality culture** to **assure** data quality and integrity.

- 集體的價值觀信念行為所呈現之品質文化

66

- 6.3.3 Management can foster quality culture by:
- Ensuring awareness and understanding of expectations (e.g. Code of Values and Ethics and Code of Conduct),
- Leading by example, management should demonstrate the behaviours they expect to see,
- Being accountable for actions and decisions, particularly delegated activities,
- Staying continuously and actively involved in the operations of the business,
- 管理層促進品質文化的重點方向

67

- 6.3.3 cont'd
- Setting realistic expectations, considering the limitations that place pressures on employees,
- Allocating appropriate technical and personnel resources to meet operational requirements and expectations,
- Implementing fair and just consequences and rewards that promote good cultural attitudes towards ensuring data integrity, and
- Being aware of regulatory trends to apply “lessons learned” to the organisation.

68

- 6.4 Modernising the Pharmaceutical Quality System
- 6.4.1 The application of modern quality risk management principles and good data management practices to the current Pharmaceutical Quality System serves to modernize the system to meet the challenges that come with the generation of complex data.

- 現代化的PQS

69

- 6.4.2 The company's Pharmaceutical Quality System should be able to prevent, detect and correct weaknesses in the system or their processes that may lead to data integrity lapses. The company should know their data life cycle and integrate the appropriate controls and procedures such that the data generated will be valid, complete and reliable. Specifically, such control and procedural changes may be in the following areas:

- Quality Risk Management,
- Investigation programs,
- Data review practices (section 9),
- Computerised system validation,
- IT infrastructure, services and security (physical and virtual),

- 推動構面

70

- 6.4.2 cont'd

- **Training program** to include company's **approach** to **data governance** and **data governance SOPs**,
- **Storage, processing, transfer** and **retrieval** of **completed records**, including **decentralised/cloud-based** data storage, **processing** and **transfer** activities,
- Appropriate **oversight** of the **purchase** of **GMP/GDP critical equipment** and **IT infrastructure** that incorporate requirements **designed to meet** data integrity expectations, e.g. **User Requirement Specifications**, (Refer section 9.2)
- **Self-inspection program** to include **data quality** and **integrity**, and
- **Performance indicators** (**quality metrics**) and **reporting** to **senior management**.

71

- 6.5 Regular management review of performance indicators (including quality metrics)

- 6.5.1 There should be **regular** management reviews of **performance indicators**, including those related to **data integrity**, such that **significant issues** are identified, **escalated** and **addressed** in a **timely** manner. **Caution** should be taken when **key performance indicators** are **selected** so as not to inadvertently result in a culture in which **data integrity** is **lower in priority**.

- 定期審查品質指標 | KPI議題

72



- 6.5.2 The **head** of the Quality unit should have **direct** access to **senior management** in order to **directly** communicate risks so that senior management is **aware** and can **allocate** resources to **address** any issues.

- QU主管直接向高層報告DI問題

73

- 6.5.3 Management can have an **independent expert** periodically verify the **effectiveness** of their systems and controls.

- 獨立專家定期評估系統有效性

74

- 6.6 Resource allocation

- 6.6.1 Management should **allocate** appropriate **resources** to **support** and **sustain** good data integrity management such that the **workload** and **pressures** on those responsible for **data generation** and **record keeping** do **not** increase the **likelihood** of **errors** or the **opportunity** to deliberately **compromise** data integrity.

- 足夠資源避免DI問題

75

- 6.6.2 There should be **sufficient** number of **personnel** for **quality** and **management oversight**, **IT support**, conduct of **investigations**, and management of **training programs** that are **commensurate with** the operations of the organisation.

- 足夠人力及相關資源 | 符合公司的運作規模

76

- 6.6.3 There should be provisions to purchase equipment, software and hardware that are appropriate for their needs, based on the criticality of the data in question. Companies should implement technical solutions that improve compliance with ALCOA+<sup>5</sup> principles and thus mitigate weaknesses in relation to data quality and integrity.
- <sup>5</sup> EMA guidance for GCP inspections conducted in the context of the Centralised Procedure
- 相關設備要符合ALCOA+之要求

77

- 6.6.4 Personnel should be qualified and trained for their specific duties, with appropriate segregation of duties, including the importance of good documentation practices (GdocPs). There should be evidence of the effectiveness of training on critical procedures, such as electronic data review. The concept of good data management practices applies to all functional departments that play a role in GMP/GDP, including areas such as IT and engineering.
- 職能分離 | 人員職能訓練 | 包括IT及工程人員

78

- 6.6.5 Data quality and integrity should be familiar to all, but data quality experts from various levels (SMEs, supervisors, team leaders) may be called upon to work together to conduct/support investigations, identify system gaps and drive implementation of improvements.

- 流程或系統有問題 | 全公司調查改善

79

- 6.6.6 Introduction of new roles in an organisation relating to good data management such as a data custodian might be considered.

- 資料保管人

80

- 6.7 Dealing with data integrity issues found internally

- 6.7.1 In the event that data integrity **lapses** are **found**, they should be handled as any **deviation** would be **according to** the Pharmaceutical Quality System. It is important to determine the **extent** of the problem as well as its **root cause**, then **correcting** the issue to **its full extent** and implement **preventive measures**. This may include the use of a **third party** for **additional expertise** or **perspective**, which may involve a **gap assessment** to identify **weaknesses** in the system.

- 發現DI問題啟動偏差及展開調查改善

81

- 6.7.2 When considering the **impact** on **patient safety** and **product quality**, any **conclusions** drawn should be supported by **sound scientific evidence**.

- 結論符合科學證據

82

- 6.7.3 Corrections may include product recall, client notification and reporting to regulatory authorities. Corrections and corrective action plans and their implementation should be recorded and monitored.
- 6.7.4 Further guidance may be found in section 12 of this guide.

- DI問題之矯正措施

83

## ● 7 GENERAL DATA INTEGRITY PRINCIPLES AND ENABLERS

- 7.1 The Pharmaceutical Quality System should be implemented throughout the different stages of the life cycle of the APIs and medicinal products and should encourage the use of science and risk-based approaches.

- PQS | 科學及風險基礎

84

- 7.2 To ensure that **decision making** is well **informed** and to **verify** that the **information** is **reliable**, the **events** or **actions** that informed those decisions should be well **documented**. As such, **Good Documentation Practices** are **key** to ensuring **data integrity**, and a **fundamental part** of a **well-designed** Pharmaceutical Quality System (discussed in section 6).

- DI問題之結論 | 文件化

85

- 7.3 The application of **GdocPs** may **vary** depending on the **medium** used to **record** the data (i.e. **physical** vs. **electronic** records), but the **principles** are **applicable** to both. This section will introduce those **key principles** and following sections (8 & 9) will explore these principles relative to **documentation** in both **paper-based** and **electronic-based** recordkeeping.

- 記錄數據的工具型式

86

- 7.4 Some key concepts of GdocPs are summarised by the acronym **ALCOA**: **A**ttributable, **L**egible, **C**ontemporaneous, **O**riginal, and **A**ccurate. The following attributes can be added to the list: **C**omplete, **C**onsistent, **E**nduring and **A**vailable (**ALCOA+**<sup>6</sup>). Together, these expectations ensure that events are properly documented and the data can be used to support informed decisions.
- <sup>6</sup> EMA guidance for GCP inspections conducted in the context of the Centralised Procedure
- ALCOA+

- 7.5 Basic data integrity principles applicable to both paper and electronic systems (i.e. ALCOA +):

| Data Integrity Attribute | Requirement   |
|--------------------------|---|
| Attributable             | It should be possible to identify the individual or computerised system that performed a recorded task and when the task was performed. This also applies to any changes made to records, such as corrections, deletions, and changes where it is important to know who made a change, when, and why. |



| Data Integrity Attribute | Requirement  |
|--------------------------|--|
| Legible                  | All records should be legible – the information should be readable and unambiguous in order for it to be understandable and of use. This applies to all information that would be required to be considered Complete, including all Original records or entries. Where the 'dynamic' nature of electronic data (the ability to search, query, trend, etc.) is important to the content and meaning of the record, the ability to interact with the data using a suitable application is important to the 'availability' of the record. |

| Data Integrity Attribute | Requirement   |
|--------------------------|---|
| Contemporaneous          | The evidence of actions, events or decisions should be recorded as they take place. This documentation should serve as an accurate attestation of what was done, or what was decided and why, i.e. what influenced the decision at that time. |

| Data Integrity Attribute | Requirement   |
|--------------------------|---|
| Original                 | The original record can be described as the <u>first-capture</u> of information, whether recorded on paper (static) or electronically (usually dynamic, depending on the complexity of the system). Information that is originally captured in a dynamic state should remain available in that state. |

| Data Integrity Attribute | Requirement   |
|--------------------------|---|
| Accurate                 | <p>Records need to be a truthful representation of facts to be accurate. Ensuring records are accurate is achieved through many elements of a robust Pharmaceutical Quality System. This can be comprised of:</p> <ul style="list-style-type: none"> <li>equipment related factors such as qualification, calibration, maintenance and computer validation.</li> <li>policies and procedures to control actions and behaviours, including data review procedures to verify adherence to procedural requirements</li> <li>deviation management including root cause analysis, impact assessments and CAPA</li> </ul> |

| Data Integrity Attribute | Requirement  |
|--------------------------|--|
| Accurate                 | <ul style="list-style-type: none"> <li>trained and qualified personnel who understand the importance of following established procedures and documenting their actions and decisions.</li> </ul> <p>Together, these elements aim to ensure the accuracy of information, including scientific data that is used to make critical decisions about the quality of products.</p> |

| Data Integrity Attribute | Requirement  |
|--------------------------|--|
| Complete                 | <p>All information that would be critical to recreating an event is important when trying to understand the event. It is important that information is <u>not lost or deleted</u>. The level of detail required for an information set to be considered complete would depend on the criticality of the information (see section 5.4 Data criticality). A complete record of data generated electronically includes relevant metadata (see section 9).</p> |

| Data Integrity Attribute | Requirement  |
|--------------------------|--|
| Consistent               | Information should be created, processed, and stored in a logical manner that <u>has a defined consistency</u> . This includes policies or procedures that help control or standardize data (e.g. chronological sequencing, date formats, units of measurement, approaches to rounding, significant digits, etc.). |

| Data Integrity Attribute | Requirement   |
|--------------------------|---|
| Enduring                 | Records should be kept in a manner such that they exist for the entire period during which they might be needed. This means they need to <u>remain intact and accessible</u> as an indelible/durable record throughout the record retention period. |

| Data Integrity Attribute | Requirement   |
|--------------------------|---|
| Available                | Records should be available for review at any time during the required retention period, accessible in a readable format to all applicable personnel who are responsible for their review whether for routine release decisions, investigations, trending, annual reports, audits or inspections. |

- 7.6 If these elements are appropriately applied to all applicable areas of GMP and GDP related activities, along with other supporting elements of a Pharmaceutical Quality System, the reliability of the information used to make critical decisions regarding drug products should be adequately assured.

- ALCOA+各要素以確保關鍵決定之可靠性



## ● 7.7 True copies

- 7.7.1 Copies of original paper records (e.g. analytical summary reports, validation reports, etc.) are generally very useful for communication purposes, e.g. between companies operating at different locations. These records should be controlled during their life cycle to ensure that the data received from another site (sister company, contractor, etc.) are maintained as “true copies” where appropriate, or used as a “summary report” where the requirements of a “true copy” are not met (e.g. summary of complex analytical data).

- 溝通的文件

99

- 7.7.2 It is conceivable for raw data generated by electronic means to be retained in an acceptable paper or pdf format, where it can be justified that a static record maintains the integrity of the original data. However, the data retention process should record all data, (including metadata) for all activities which directly or indirectly impact on all aspects of the quality of medicinal products, (e.g. for records of analysis this may include: raw data, metadata, relevant audit trail and result files, software / system configuration settings specific to each analytical run, and all data processing runs (including methods and audit trails) necessary for reconstruction of a given raw data set). It would also require a documented means to verify that the printed records were an accurate representation. This approach is likely to be onerous in its administration to enable a GMP/GDP compliant record.

- 重要 | 數據流 | 資料處理

100

- 7.7.3 Many **electronic records** are important to **retain** in their **dynamic format**, to enable **interaction** with the **data**. Data should be **retained** in a **dynamic form** where this is **critical** to its **integrity** or later **verification**. Risk management **principles** should be **utilised** to **support** and **justify** whether and **how long data** should be **stored** in a **dynamic format**.
- 電子紀錄之管理

101

- 7.7.4 At the **receiving site**, these **records** (**true copies**) may either be managed in a **paper** or **electronic format** (e.g., **PDF**) and should be **controlled** according to an **approved QA procedure**.
- True copy

102

- 7.7.5 Care should be taken to ensure that documents are appropriately authenticated as “true copies” in a manner that allows the authenticity of the document to be readily verified, e.g. through the use of handwritten or electronic signatures or generated following a validated process for creating true copies.

- 被定義true copy的程序

| Item | How should the “true copy” be issued and controlled?  |
|------|---|
| 1.   | <p><b><u>Creating a “true copy” of a paper document.</u></b></p> <p>At the company who issues the true copy:</p> <ul style="list-style-type: none"> <li>- Obtain the original of the document to be copied</li> <li>- Photocopy the original document ensuring that no information from the original copy is lost;</li> <li>- Verify the authenticity of the copied document and sign and date the new hardcopy as a “true copy”;</li> </ul> <p>The “True Copy” may now be sent to the intended recipient.</p> <p><b><u>Creating a “true copy” of a electronic document.</u></b></p> <p>A ‘true copy’ of an electronic record should be created by electronic means (electronic file copy), including all required metadata. Creating pdf versions of electronic data should be prohibited, where there is the potential for loss of metadata.</p> <p>The “True Copy” may now be sent to the intended recipient.</p> <p>A distribution list of all issued “true copies” (soft/hard) should be maintained.</p> |



### Specific elements that should be checked when reviewing records:

- Verify the procedure for the generation of true copies, and ensure that the generation method is controlled appropriately.
- Check that true copies issued are identical (complete and accurate) to original records. Copied records should be checked against the original document records to make sure there is no tampering of the scanned image.
- Check that scanned or saved records are protected to ensure data integrity.
- After scanning paper records and verifying creation of a 'true copy':
  - Where true copies are generated for distribution purposes, e.g. to be sent to a client, the original documents from which the Where true copies are generated for distribution purposes, e.g. to be sent to a client, the original documents from which the scanned images have been created should be retained for the respective retention periods by the record owner.
  - Where true copies are generated to aid document retention, it may be possible to retain the copy in place of the original records documents from which the scanned images have been created.

105

2.

At the company who receives the true copy:

- The paper version, scanned copy or electronic file should be reviewed and filed according to good document management practices.

The document should clearly indicate that it is a true copy and not an original record.

### Specific elements that should be checked when reviewing records:

- Check that received records are checked and retained appropriately.
- A system should be in place to verify the authenticity of "true copies" e.g. through verification of the correct signatories.

106

- 7.7.6 A quality agreement should be in place to address the responsibilities for the generation and transfer of “true copies” and data integrity controls. The system for the issuance and control of “true copies” should be audited by the contract giver and receiver to ensure the process is robust and meets data integrity principles.

- 品質協議列入true copies的流程

107

- 7.8 Limitations of remote review of summary reports

- 7.8.1 The remote review of data within summary reports is a common necessity; however, the limitations of remote data review should be fully understood to enable adequate control of data integrity.

- 摘要報告需確保其DI議題

108

- 7.8.2 Summary reports of data are often **supplied** between **physically remote manufacturing sites**, **Market Authorisation Holders** and other **interested parties**. However, it should be acknowledged that summary reports are essentially limited in their nature, in that **critical supporting data** and **metadata** is often **not included** and therefore **original data** cannot be **reviewed**.

- Summary report 之議題

109

- 7.8.3 It is therefore **essential** that **summary reports** are **viewed** as but **one element** of the **process** for the **transfer of data** and that interested parties and **inspectorates** do **not** place **sole reliance** on **summary report data**.

- 著重於數據移轉之過程

110

- 7.8.4 Prior to acceptance of summary data, an evaluation of the supplier's quality system and compliance with data integrity principles should be established. It is not normally acceptable nor possible to determine compliance with data integrity principles through the use of a desk-top or similar assessment.

- 確認彙整數據之真實性

111

- 7.8.4.1 For external entities, this should be determined through on-site audit when considered important in the context of quality risk management. The audit should assure the veracity of data generated by the company, and include a review of the mechanisms used to generate and distribute summary data and reports.

- 匯整數據給外部公司 | Supplier audit 項目

112

- 7.8.4.2 Where **summary data** is distributed between **different sites** of the **same organisation**, the evaluation of the **supplying site's compliance** may be determined through **alternative** means (e.g. **evidence of compliance** with **corporate procedures**, **internal audit reports**, etc.).

- 匯整數據給不同分公司 | 不同確認方法

113

- 7.8.5 **Summary data** should be **prepared** in accordance with **agreed procedures** and **reviewed** and **approved** by **authorised staff** at the **original site**. **Summaries** should be accompanied with a **declaration** signed by the **Authorised Person** stating the **authenticity** and **accuracy** of the **summary**. The **arrangements** for the **generation**, **transfer** and **verification** of **summary reports** should be addressed within **quality/technical agreements**.

- **Summary data** 準備過程及核准程序

114

- 8 SPECIFIC DATA INTEGRITY CONSIDERATIONS FOR PAPER-BASED SYSTEMS

- 8.1 Structure of Pharmaceutical Quality System and control of blank forms/templates/records

- 8.1.1 The effective management of paper based documents is a key element of GMP/GDP. Accordingly the documentation system should be designed to meet GMP/GDP requirements and ensure that documents and records are effectively controlled to maintain their integrity.

- 紙本型式是GMP/GDP文件管理要點

115

- 8.1.2 Paper records should be controlled and should remain attributable, legible, contemporaneous, original and accurate, complete, consistent enduring (indelible/durable), and available (ALCOA+) throughout the data lifecycle.

- 紙本紀錄符合ALCOA+

116

- 8.1.3 Procedures outlining good documentation practices and arrangements for document control should be available within the Pharmaceutical Quality System. These procedures should specify how data integrity is maintained throughout the lifecycle of the data, including:
  - creation, review, and approval of master documents and procedures;
  - generation, distribution and control of templates used to record data (master, logs, etc.);
  - retrieval and disaster recovery processes regarding records;
- 紙本文件管理要點

117

- 8.1.3 cont'd
  - generation of working copies of documents for routine use, with specific emphasis on ensuring copies of documents, e.g. SOPs and blank forms are issued and reconciled for use in a controlled and traceable manner;
  - completion of paper based documents, specifying how individual operators are identified, data entry formats, recording amendments, and routine review for accuracy, authenticity and completeness; and filing, retrieval, retention, archival and disposal of records.

118

## ● 8.2 Importance of controlling records

- 8.2.1 Records are critical to GMP/GDP operations and thus control is necessary to ensure:
  - evidence of activities performed;
  - evidence of compliance with GMP/GDP requirements and company policies, procedures and work instructions;
  - effectiveness of Pharmaceutical Quality System;
  - traceability;
- 紙本紀錄之重要性

119

## ● 8.2 Importance of controlling records

- 8.2.1 cont'd
  - process authenticity and consistency;
  - evidence of the good quality attributes of the medicinal products manufactured;
  - in case of complaints or recalls, records could be used for investigational purposes; and
  - in case of deviations or test failures, records are critical to completing an effective investigation.

120



- 8.3 Generation, distribution and control of template records
- 8.3.1 Managing and controlling master documents is necessary to ensure that the risk of someone inappropriately using and/or falsifying a record 'by ordinary means' (i.e. not requiring the use of specialist fraud skills) is reduced to an acceptable level. The following expectations should be implemented using a quality risk management approach, considering the risk and criticality of data recorded (see section 5.4, 5.5).
- Master document

121

- 8.4 Expectations for the generation, distribution and control of records

| Item | Generation   |
|------|--|
| 1.   | <p><b>Expectation</b></p> <p>All documents should have a unique identifier (including the version number) and should be checked, approved, signed and dated.</p> <p>The use of uncontrolled documents should be prohibited by local procedures. The use of temporary recording practices, e.g. scraps of paper should be prohibited.</p> |

122

### Potential risk of not meeting expectations/items to be checked

- Uncontrolled documents increase the potential for omission or loss of critical data as these documents may be discarded or destroyed without traceability. In addition, uncontrolled records may not be designed to correctly record critical data.
- It might be easier to falsify uncontrolled records.
- Use of temporary recording practices may lead to data omission, and these temporary original records are not specified for retention.
- If records can be created and accessed without control, it is possible that the records may not have been recorded at the time the event occurred.
- There is a risk of using superseded forms if there is no version control or controls for issuance.

123

2.

### Expectation

The document design should provide sufficient space for manual data entries.

### Potential risk of not meeting expectations/items to be checked

- Handwritten data may not be clear and legible if the spaces provided for data entry are not sufficiently sized.
- Documents should be designed to provide sufficient space for comments, e.g. in case of a transcription error, there should be sufficient space for the operator to cross out, initial and date the error, and record any explanation required.
- If additional pages of the documents are added to allow complete documentation, the number of, and reference to any pages added should be clearly documented on the main record page and signed.
- Sufficient space should be provided in the document format to add all necessary data, and data should not be recorded haphazardly on the document, for example to avoid recording on the reverse of printed recording on the reverse of printed pages which are not intended for this purpose.

114TPDA04006-B

124

### 3. **Expectation**

The document design should make it clear what data is to be provided in entries.

#### **Potential risks of not meeting expectations/items to be checked**

- Ambiguous instructions may lead to inconsistent/incorrect recording of data.
- Good design ensures all critical data is recorded and ensures clear, contemporaneous and enduring (indelible/durable) completion of entries.
- The document should also be structured in such a way as to record information in the same order as the operational process and related SOP, to minimize the risk of inadvertently omitting critical data.

125

### 4. **Expectation**

Documents should be stored in a manner which ensures appropriate version control.

Master documents should contain distinctive marking so to distinguish the master from a copy, e.g. use of coloured papers or inks so as to prevent inadvertent use.

Master documents (in electronic form) should be prevented from unauthorised or inadvertent changes.

E.g.: For the template records stored electronically, the following precautions should be in place:

- access to master templates should be controlled;
- process controls for creating and updating versions should be clear and practically applied/verified; and
- master documents should be stored in a manner which prevents unauthorised changes.

126



### Potential risk of not meeting expectations/items to be checked

- Inappropriate storage conditions can allow unauthorised modification, use of expired and/or draft documents or cause the loss of master documents.
- The processes of implementation and the effective communication, by way of appropriate training prior to implementation when applicable, are just as important as the document.

| Item | Distribution and Control   | 114TPDA04006-B |
|------|--|----------------|
| 1.   | <p><b>Expectations</b></p> <p>Updated versions should be distributed in a timely manner.</p> <p>Obsolete master documents and files should be archived and their access restricted.</p> <p>Any issued and unused physical documents should be retrieved and reconciled.</p> <p>Where authorised by Quality, recovered copies of documents may be destroyed. However, master copies of authorised documents should be preserved.</p> <p><b>Potential risk of not meeting expectations/items to be checked</b></p> <ul style="list-style-type: none"> <li>• There may be a risk that obsolete versions can be used by mistake if available for use.</li> </ul> | 128            |

## 2. Expectation

Document issuance should be controlled by written procedures that include the following controls:

- details of who issued the copies and when they were issued;
- clear means of differentiating approved copies of documents, e.g. by use of a secure stamp, or paper colour code not available in the working areas or another appropriate system;
- ensuring that only the current approved version is available for use;
- allocating a unique identifier to each blank document issued and recording the issue of each document in a register;
- numbering every distributed copy (e.g.: copy 2 of 2) and sequential numbering of issued pages in bound books;
- where the re-issue of additional copies of the blank template is necessary, a controlled process regarding re-issue should be followed with all distributed copies maintained and a justification and approval for the need of an extra copy recorded, e.g.: "the original template record was damaged";

129

- critical GMP/GDP blank forms (e.g.: worksheets, laboratory notebooks, batch records, control records) should be reconciled following use to ensure the accuracy and completeness of records; and
- where copies of documents other than records, (e.g. procedures), are printed for reference only, reconciliation may not be required, providing the documents are time-stamped on generation, and their short-term validity marked on the document.

114TPDA04006-B

### Potential risk of not meeting expectations/items to be checked

- Without the use of security measures, there is a risk that rewriting or falsification of data may be made after photocopying or scanning the template record (which gives the user another template copy to use).
- Obsolete versions can be used intentionally or by error.
- A filled record with an anomalous data entry could be replaced by a new rewritten template.
- All unused forms should be accounted for, and either defaced and destroyed, or returned for secure filing.
- Check that (where used) reference copies of documents are clearly marked with the date of generation, period of validity and clear indication that they are for reference only and not an official copy, e.g. marked 'uncontrolled when printed'.

130

- 8.4.1 An **index** of all authorised **master documents**, (**SOP's**, **forms**, **templates** and **records**) should be **maintained** within the Pharmaceutical Quality System. This index should mention for **each type of template record** at least the following **information**: **title**, **identifier** including **version** number, **location** (e.g. **documentation database**, **effective date**, **next review date**, etc.).
- Master document (SOP, form, template, records)

131

- 8.5 Use and control of records located at the point-of-use
- 8.5.1 **Records** should be available to operators at the **point-of-use** and appropriate **controls** should be in place to **manage** these records. These controls should be carried out to **minimize** the risk of **damage** or **loss** of the records and **ensure** data integrity. Where necessary, **measures** should be taken to **protect** records from being **soiled** (e.g. **getting wet** or **stained** by materials, etc.).
- 紀錄表單及紀錄文件

132

- 8.5.2 **Records** should be appropriately controlled in these **areas** by **designated persons** or **processes** in accordance with **written procedures**.

- 規範紀錄文件儲存程序

133

- 8.6 Filling out records

- 8.6.1 The items listed in the **table below** should be **controlled** to assure that a **record** is properly **filled out**.

- 填記表格

134

| Item | Completion of records   |
|------|---|
| 1.   | <p><b>Expectations</b></p> <p>Handwritten entries should be made by the person who executed the task<sup>7</sup>.</p> <p>Unused, blank fields within documents should be voided (e.g. crossed-out), dated and signed.</p> <p>Handwritten entries should be made in clear and legible writing.</p> <p>The completion of date fields should be done in an unambiguous format defined for the site. E.g. dd/mm/yyyy or mm/dd/yyyy.</p> |

- 7 Scribes may only be used in exceptional circumstances, refer footnote 8.

#### Potential risk of not meeting expectations/items to be checked

- Check that handwriting is consistent for entries made by the same person.
- Check the entry is legible and clear (i.e. unambiguous; and does not include the use of unknown symbols or abbreviations, e.g. use of ditto (") marks.
- Check for completeness of data recorded.
- Check correct pagination of the records and are all pages present.



## 2. Expectation

Records relating to operations should be completed contemporaneously<sup>8</sup>.

- <sup>8</sup> The use of scribes (second person) to record activity on behalf of another operator should be considered 'exceptional', and only take place where:
  - The act of recording places the product or activity at risk e.g. documenting line interventions by sterile operators.
  - To accommodate cultural or staff literacy / language limitations, for instance where an activity is performed by an operator, but witnessed and recorded by a scribe. In these cases, bilingual or controlled translations of documents into local languages and dialect are advised.
  - In both situations, the scribe 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 a scribe to complete documentation should be described in an approved procedure, which should; specify the activities to which the process applies and assesses the risks associated.

137

### Potential risk of not meeting expectations/items to be checked

- Verify that records are available within the immediate areas in which they are used, i.e. Inspectors should expect that sequential recording can be performed at the site of operations. If the form is not available at the point of use, this will not allow operators to fill in records at the time of occurrence.

138

### 3. Expectation

Records should be enduring (indelible).

#### Potential risk of not meeting expectations/items to be checked

- Check that written entries are in ink, which is not erasable, and/or will not smudge or fade (during the retention period).
- Check that the records were not filled out using pencil prior to use of pen (overwriting).
- Note that some paper printouts from systems may fade over time, e.g. thermal paper. Indelible signed and dated true copies of these should be produced and kept.

● 領料記錄 | 製造記錄 | 分包裝記錄之設計

139

### 4. Expectation

Records should be signed and dated using a unique identifier that is attributable to the author.

#### Potential risk of not meeting expectations/items to be checked

- Check that there are signature and initials logs, that are controlled and current and that demonstrate the use of unique examples, not just standardized printed letters.
- Ensure that all key entries are signed & dated, particularly if steps occur over time, i.e. not just signed at the end of the page and/or process.
- The use of personal seals is generally not encouraged; however, where used, seals should be controlled for access. There should be a log which clearly shows traceability between an individual and their personal seal. Use of personal seals should be dated (by the owner), to be deemed acceptable.

140

- **8.7 Making corrections on records**
- Corrections to the records should be made in such way that full traceability is maintained.

| Item | How should records be corrected?   |
|------|--|
| 1    | <p><b>Expectation</b></p> <p>Cross out what is to be changed with a single line.</p> |

Where appropriate, the reason for the correction should be clearly recorded and verified if critical.

Initial and date the change made.

**Specific elements that should be checked when reviewing records:**

- Check that the original data is readable not obscured (e.g. not obscured by use of liquid paper; overwriting is not permitted).
- If changes have been made to critical data entries, verify that a valid reason for the change has been recorded and that supporting evidence for the change is available.
- Check for unexplained symbols or entries in records.

## 2. Expectation

Corrections should be made in **indelible ink**.

### **Specific elements that should be checked when reviewing records:**

- Check that written entries are **in ink**, which is **not erasable**, and/or will not **smudge** or **fade** (during the retention period).
- Check that the records were **not filled out** using **pencil** prior to use of pen (**overwriting**).

143

## 8.8 Verification of records (secondary checks)

114TPDA04006-B

| Item | When and who should verify the records?   |
|------|---|
| 1.   | <p><b>Expectation</b></p> <p>Records of <b>critical process steps</b>, e.g. <b>critical steps</b> within <b>batch records</b>, should be:</p> <ul style="list-style-type: none"> <li>- <b>reviewed/witnessed</b> by <b>independent</b> and <b>designated personnel</b> at the time of operations occurring; and</li> <li>- reviewed by an <b>approved person</b> within the <b>production department</b> before sending them to the Quality unit ; and</li> <li>- reviewed and approved by the <b>Quality Unit</b> (e.g. <b>Authorised Person / Qualified Person</b>) before release or distribution of the batch produced.</li> </ul> <p><b>Batch production records</b> of <b>non-critical process steps</b> is generally <b>reviewed</b> by <b>production personnel</b> according to an approved procedure.</p> <p><b>Laboratory records</b> for <b>testing steps</b> should also be <b>reviewed</b> by <b>designated personnel</b> (e.g.: <b>second analysts</b>) following <b>completion</b> of testing. <b>Reviewers</b> are expected to <b>check all entries</b>, <b>critical calculations</b>, and undertake appropriate <b>assessment</b> of the <b>reliability of test results</b> in accordance with <b>data-integrity principles</b>.</p> |

144



Additional controls should be considered when critical test interpretations are made by a single individual (e.g. recording of microbial colonies on agar

plates). A secondary review may be required in accordance with risk management principles. In some cases this review may need to be performed in real-time. Suitable electronic means of verifying critical data may be an acceptable alternative, e.g. taking photograph images of the data for retention.

This verification should be conducted after performing production-related tasks and activities and be signed or initialled and dated by the appropriate persons.

Local SOPs should be in place to describe the process for review of written documents.

### **Specific elements that should be checked when reviewing records:**

- Verify the process for the handling of production records within processing areas to ensure they are readily available to the correct personnel at the time of performing the activity to which the record relates.
- Verify that any secondary checks performed during processing were performed by appropriately qualified and independent personnel, e.g. production supervisor or QA.
- Check that documents were reviewed by production personnel and then quality assurance personnel following completion of operational activities.

| Item | How should records be verified?   |
|------|---|
| 2.   | <p><b>Expectation</b></p> <p>Check that all the fields have been completed correctly using the current (approved) templates, and that the data was critically compared to the acceptance criteria.</p> <p>Check items 1, 2, 3, and 4 of section 8.6 and Items 1 and 2 of section 8.7</p> <p><b>Specific elements that should be checked when reviewing records:</b></p> <ul style="list-style-type: none"> <li>Inspectors should review company procedures for the review of manual data to determine the adequacy of processes.</li> <li>The need for, and extent of a secondary check should be based on quality risk management principles, based on the criticality of the data generated.</li> <li>Check that the secondary reviews of data include a verification of any calculations used.</li> <li>View original data (where possible) to confirm that the correct data was transcribed for the calculation.</li> </ul> |

## ● 8.9 Direct print-outs from electronic systems

- 8.9.1 Some very simple electronic systems, e.g. balances, pH meters or simple processing equipment which do not store data, generate directly-printed paper records. These types of systems and records provide limited opportunity to influence the presentation of data by (re-)processing, changing of electronic date/time stamps. In these circumstances, the original record should be signed and dated by the person generating the record and information to ensure traceability, such as sample ID, batch number, etc. should be recorded on the record. These original records should be attached to batch processing or testing records.

- 8.9.2 **Consideration** should be given to ensuring these **records** are **enduring** (see section 8.6.1).

- 8.10 Document retention (Identifying record retention requirements and archiving records)
- 8.10.1 The **retention period** of each type of records should (at a **minimum**) meet those periods specified **by GMP/GDP** requirements. Consideration should be given to **other local** or **national** legislation that may stipulate **longer** storage periods.
- 文件保存期限

- 8.10.2 The records can be retained **internally** or by using an **outside** storage service subject to **quality agreements**. In this case, the data **centre's locations** should be **identified**. A **risk assessment** should be available to demonstrate **retention systems/facilities/services** are suitable and that the residual risks are understood.

- 保存地點

| Item | Where and how should records be archived?   |
|------|---|
| 1.   | <p><b>Expectation</b></p> <p>A system should be in place describing the different steps for archiving records (identification of archive boxes, list of records by box, retention period, archiving location, etc.).</p> <p>Instructions regarding the controls for storage, as well as access and recovery of records should be in place.</p> <p>Systems should ensure that all GMP/GDP relevant records are stored for periods that meet GMP/GDP requirements<sup>9</sup>.</p> <p><b>Specific elements that should be checked when reviewing records:</b></p> <ul style="list-style-type: none"> <li>• Check that the system implemented for retrieving archived records is effective and traceable.</li> <li>• Check if the records are stored in an orderly manner and are easily identifiable.</li> <li>• Check that records are in the defined location and appropriately secured.</li> </ul> |



- Check that **access** to archived documents is **restricted** to **authorised** personnel ensuring integrity of the stored records.
- Check for the **presence** of **records** of **accessing** and **returning** of records.
- The **storage** methods used should permit **efficient** **retrieval** of documents when required.

## 2. Expectation

All **hardcopy** quality records should be **archived** in:

- **secure** **locations** to prevent **damage** or **loss**,
- such a manner that it is easily **traceable** and **retrievable**, and
- a manner that ensures that records are **durable** for their archived life.

### **Specific elements that should be checked when reviewing records:**

- Check for the **outsourced** archived operations if there is a **quality agreement** in place and if the **storage location** was **audited**.
- Ensure there is some assessment of ensuring that **documents** will still be **legible/available** for the entire archival period.
- In case of printouts which are **not permanent** (e.g. **thermal transfer paper**) a verified ('true') copy should be **retained**.
- Verify whether the **storage methods** used permit **efficient** retrieval of documents when required.

### 3. Expectation

All records should be protected from damage or destruction by:

- fire;
- liquids (e.g. water, solvents and buffer solution);
- rodents;
- humidity etc; and.
- unauthorised personnel access, who may attempt to amend, destroy or replace records.

**Specific elements that should be checked when reviewing records:**

- Check if there are systems in place to protect records (e.g. pest control and sprinklers).
- Note: Sprinkler systems should be implemented according to local safety requirements; however, they should be designed to prevent damage to documents, e.g. documents are protected from water.
- Check for appropriate access controls for records.

#### ● 8.11 Disposal of original records or true copies

- 8.11.1 A documented process for the disposal of records should be in place to ensure that the correct original records or true copies are disposed of after the defined retention period. The system should ensure that current records are not destroyed by accident and that historical records do not inadvertently make their way back into the current record stream (e.g. historical records confused/mixed with existing records.)

- 銷毀程序

- 8.11.2 A **record/register** should be available to demonstrate appropriate and timely **archiving** or **destruction** of **retired** records in accordance with local policies.

- 銷毀紀錄

157

- 8.11.3 Measures should be in place to **reduce** the risk of **deleting** the **wrong documents**. The **access rights** allowing **disposal** of records should be **controlled** and **limited** to **few persons**.

- 銷毀文件之職責人員

158

## ● 9 SPECIFIC DATA INTEGRITY CONSIDERATIONS FOR COMPUTERISED SYSTEMS

### ● 9.1 Structure of the Pharmaceutical Quality System and control of computerised systems

- 9.1.1 A large variety of computerised systems are used by companies to assist in a significant number of operational activities. These range from the simple standalone to large integrated and complex systems, many of which have an impact on the quality of products manufactured. It is the responsibility of each regulated entity to fully evaluate and control all computerised systems and manage them in accordance with GMP<sup>10</sup> and GDP<sup>11</sup> requirements.

- <sup>10</sup> PIC/S PE 009 Guide to Good Manufacturing Practice for Medicinal Products, specifically Part I chapters 4, Part II chapters 5, & Annex 11
- <sup>11</sup> PIC/S PE 011 GDP Guide to Good Distribution Practice for Medicinal Products, specifically section 3.5

159

- 9.1.2 Organisations should be fully aware of the nature and extent of computerised systems utilised, and assessments should be in place that describe each system, its intended use and function, and any data integrity risks or vulnerabilities that may be susceptible to manipulation. Particular emphasis should be placed on determining the criticality of computerised systems and any associated data, in respect of product quality.

- 電腦化系統之風險等級

160

- 9.1.3 All computerised systems with potential for impact on product quality should be effectively managed under a Pharmaceutical Quality System which is designed to ensure that systems are protected from acts of accidental or deliberate manipulation, modification or any other activity that may impact on data quality and integrity.

- 管控每個電腦化系統之管理策略

161

- 9.1.4 The processes for the design, evaluation, and selection of computerised systems should include appropriate consideration of the data management and integrity aspects of the system. Regulated users should ensure that vendors of systems have an adequate understanding of GMP/GDP and data integrity requirements, and that new systems include appropriate controls to ensure effective data management. Legacy systems are expected to meet the same basic requirements; however, full compliance may necessitate the use of additional controls, e.g. supporting administrative procedures or supplementary security hardware/software.

- Legacy system 仍需要符合相同的DI要求

162

- 9.1.5 Regulated users should fully understand the **extent** and **nature** of **data** generated by computerised systems, and a **risk based approach** should be taken to **determining** the **data risk** and **criticality** of data (including **metadata**) and the **subsequent controls** required to manage the data generated. For example:

- 管控機制

163

- 9.1.5.1 In dealing with raw data, the **complete capture** and **retention** of raw data would normally be **required** in order to **reconstruct** the manufacturing **event** or **analysis**.

- 電腦化系統資訊保存

164

- 9.1.5.2 In dealing with **metadata**, some metadata is **critical** in **reconstruction** of events, (e.g. **user identification**, **times**, critical **process parameters**, **units** of measure), and would be considered as '**relevant metadata**' that should be **fully captured** and **managed**. However, **non-critical** meta-data such as **system error logs** or **non-critical system checks** may **not** require full capture and management where **justified** using **risk management**.

- Metadata 的分類

165

- 9.1.6 When determining data **vulnerability** and **risk**, it is important that the computerised system is considered in the **context** of its **use** within the business process. For example, the integrity of **results** generated by an analytical method utilising an **integrated computer interface** are affected by **sample preparation**, **entry** of sample **weights** into the system, use of the system to **generate data**, and **processing / recording** of the **final result** using that data. The **creation** and **assessment** of a **data flow map** may be **useful** in **understanding** the **risks** and **vulnerabilities** of computerised systems, particularly **interfaced** systems.

- 資訊流單元系統的各界面

166

- 9.1.7 Consideration should be given to the **inherent** data integrity controls incorporated into the system and/or software, especially those that may be **more vulnerable** to **exploits** than **more modern** systems that have been designed to meet **contemporary** data management requirements. Examples of systems that may have **vulnerabilities** include: **manual** recording systems, **older** electronic systems with **obsolete** security measures, **non-networked** electronic systems and those that require **additional** network **security protection** e.g. using **firewalls** and **intrusion detection** or **prevention** systems.

- 列出電腦化系統需注意之弱點

167

- 9.1.8 During **inspection** of computerised systems, inspectors are recommended to **utilise** the **company's expertise** during assessment. **Asking** and **instructing** the company's representatives to facilitate **access** and **navigation** can aid in the inspection of the system.

- 稽核方式

168



- 9.1.9 The guidance herein is intended to provide specific considerations for data integrity in the **context of computerised systems**. Further guidance regarding **good practices** for computerised systems may be **found** in the PIC/S Good Practices for Computerised Systems in Regulated “GxP” Environments (**PI 011**).

- 電腦化系統DI相關的參考文件

169

- 9.1.10 The principles herein apply **equally** to circumstances where the **provision** of computerised systems is **outsourced**. In these cases, the regulated entity **retains** the **responsibility** to ensure that outsourced services are managed and assessed in accordance with GMP/GDP requirements, and that appropriate data management and integrity controls are understood **by both parties** and effectively **implemented**.

- 委託者及受託者皆需了解DI的規範

170

- 9.2 Qualification and validation of computerised systems

- 9.2.1 The **qualification** and **validation** of **computerised systems** should be performed in accordance with the relevant GMP/GDP guidelines; the **tables** below provide **clarification** regarding specific expectations for ensuring **good data governance practices** for computerised systems.

171

- 9.2.2 **Validation** alone does **not** necessarily **guarantee** that **records** generated are necessarily adequately **protected** and **validated systems** may be **vulnerable** to loss and alteration **by accidental** or **malicious means**. Thus, validation should be **supplemented by** appropriate **administrative** and **physical controls**, as well as **training** of users.

- 系統只經過確效無法確保DI

172

|              |  |
|--------------|--|
| <b>Item:</b> | <b>System Validation &amp; Maintenance</b>   |
| <b>1.</b>    | <p><b>Expectation</b></p> <p>Regulated companies should document and implement appropriate controls to ensure that data management and integrity requirements are considered in the initial stages of system procurement and throughout system and data lifecycle. For regulated users, Functional Specifications (FS) and/or User Requirement Specifications (URS) should adequately address data management and integrity requirements.</p> <p>Specific attention should be paid to the purchase of GMP/GDP critical equipment to ensure that systems are appropriately evaluated for data integrity controls prior to purchase.</p> <p>Legacy systems (existing systems in use) should be evaluated to determine whether existing system configuration and functionality permits the appropriate control of data in accordance with good data management and integrity practices. Where system functionality or design of these systems does not provide an appropriate level of control, additional controls should be considered and implemented.</p> |

### **Potential risk of not meeting expectations/items to be checked**

- Inadequate consideration of DI requirements may result in the purchase of software systems that do not include the basic functionality required to meet data management and integrity expectations.
- Inspectors should verify that the implementation of new systems followed a process that gave adequate consideration to DI principles.
- Some legacy systems may not include appropriate controls for data management, which may allow the manipulation of data with a low probability of detection.
- Assessments of existing systems should be available and provide an overview of any vulnerabilities and list any additional controls implemented to assure data integrity. Additional controls should be appropriately validated and may include:

- Assessments of existing systems should be available and provide an overview of any vulnerabilities and list any additional controls implemented to assure data integrity. Additional controls should be appropriately validated and may include:
  - Using operating system functionality (e.g. Windows Active Directory groups) to assign users and their access privileges where system software does not include administrative controls to control user privileges;
  - Configuring operating system file/folder permissions to prevent modification/deletion of files when the modification/deletion of data files cannot be controlled by system software; or
  - Implementation of hybrid or manual systems to provide control of data generated.

## 2. Expectation

Regulated users should have an inventory of all computerised systems in use. The list should include reference to:

- The name, location and primary function of each computerised system;
- Assessments of the function and criticality of the system and associated data; (e.g. direct GMP/GDP impact, indirect impact, none)
- The current validation status of each system and reference to existing validation documents.

Risk assessments should be in place for each system, specifically assessing the necessary controls to ensure data integrity. The level and extent of validation of controls for data integrity should be determined based on the criticality of the system and process and potential risk to product quality, e.g. processes or systems that generate or control batch release data would generally require greater control than those systems managing less critical data or processes.



Consideration should also be given to those systems with higher potential for disaster, malfunction or situations in which the system becomes inoperative.

Assessments should also review the vulnerability of the system to inadvertent or unauthorised changes to critical configuration settings or manipulation of data. All controls should be documented and their effectiveness verified.

#### Potential risk of not meeting expectations/items to be checked

- Companies that do not have adequate visibility of all computerised systems in place may overlook the criticality of systems and may thus create vulnerabilities within the data lifecycle.
- An inventory list serves to clearly communicate all systems in place and their criticality, ensuring that any changes or modifications to these systems are controlled.
- Verify that risk assessments are in place for critical processing equipment and data acquisition systems. A lack of thorough assessment of system impact may lead to a lack of appropriate validation and system control. Examples of critical systems to review include:

- Verify that risk assessments are in place for critical processing equipment and data acquisition systems. A lack of thorough assessment of system impact may lead to a lack of appropriate validation and system control. Examples of critical systems to review include:

- systems used to control the purchasing and status of products and materials;
- systems for the control and data acquisition for critical manufacturing processes;
- systems that generate, store or process data that is used to determine batch quality;
- systems that generate data that is included in the batch processing or packaging records; and
- systems used in the decision process for the release of products.

### 3. Expectation

For new systems, a Validation Summary Report for each computerised system (written and approved in accordance with Annex 15 requirements) should be in place and state (or provide reference to) at least the following items:

- Critical system configuration details and controls for restricting access to configuration and any changes (change management).
- A list of all currently approved normal and administrative users specifying the username and the role of the user.
- Frequency of review of audit trails and system logs.
- Procedures for:
  - creating new system user;
  - modifying or changing privileges for an existing user;
  - defining the combination or format of passwords for each system
  - reviewing and deleting users;
  - back-up processes and frequency;
  - disaster recovery;
  - data archiving (processes and responsibilities), including procedures for accessing and reading archived data;
  - approving locations for data storage.

- data archiving (processes and responsibilities), including procedures for accessing and reading archived data;
- approving locations for data storage.
- The report should explain how the original data are retained with relevant metadata in a form that permits the reconstruction of the manufacturing process or the analytical activity.

For existing systems, documents specifying the above requirements should be available; however, need not be compiled into the Validation Summary report. These documents should be maintained and updated as necessary by the regulated user.

#### Potential risk of not meeting expectations/items to be checked

- Check that validation systems and reports specifically address data integrity requirements following GMP/GDP requirements and considering ALCOA principles.
- System configuration and segregation of duties (e.g. authorisation to generate data should be separate to authorisation to verify data) should be defined prior to validation, and verified as effective during testing.
- Check the procedures for system access to ensure modifications or changes to systems are restricted and subject to change control management.
- Ensure that system administrator access is restricted to authorised persons and is not used for routine operations.
- Check the procedures for granting, modifying and removing access to computerised systems to ensure these activities are controlled. Check the currency of user access logs and privilege levels, there should be no unauthorised users to the system and access accounts should be kept up to date.



- There should also be restrictions to prevent users from amending audit trail functions and from changing any pre-defined directory paths where data files are to be stored.

#### 4. Expectation

Companies should have a Validation Master Plan in place that includes specific policies and validation requirements for computerised systems and the integrity of such systems and associated data.

The extent of validation for computerised systems should be determined based on risk. Further guidance regarding assessing validation requirements for computerised systems may be found in PI 011.

Before a system is put into routine use, it should be challenged with defined tests for conformance with the acceptance criteria.

It would be expected that a prospective validation for computerised systems is conducted. Appropriate validation data should be available for systems already in-use.

Computerised system validation should be designed according to GMP Annex 15 with URS, DQ, FAT, SAT, IQ, OQ and PQ tests as necessary.





PHARMACEUTICAL INSPECTION CONVENTION  
PHARMACEUTICAL INSPECTION CO-OPERATION SCHEME

114TPDA04006-B

PI 011-3  
25 September 2007

PIC/S GUIDANCE

**GOOD PRACTICES FOR COMPUTERISED  
SYSTEMS IN REGULATED  
“GXP” ENVIRONMENTS**

© PIC/S September 2007  
Reproduction prohibited for commercial purposes.  
Reproduction for internal use is authorised,  
provided that the source is acknowledged.

185

The qualification testing approach should be tailored for the specific system under validation, and should be justified by the regulated user. Qualification may include Design Qualification (DQ); Installation qualification (IQ); Operational Qualification (OQ); and Performance Qualification (PQ). In particular, specific tests should be designed in order to challenge those areas where data quality or integrity is at risk.

Companies should ensure that computerised systems are qualified for their intended use. Companies should therefore not place sole reliance on vendor qualification packages; validation exercises should include specific tests to ensure data integrity is maintained during operations that reflect normal and intended use.

The number of tests should be guided by a risk assessment but the critical functionalities should be at least identified and tested, e.g., certain PLCs and systems based on basic algorithms or logic sets, the functional testing may provide adequate assurance of reliability of the computerised system. For critical and/or more complex systems, detailed verification testing is required during IQ, OQ & PQ stages.

186

### Potential risk of not meeting expectations/items to be checked

- Check that validation documents include specific provisions for data integrity; validation reports should specifically address data integrity principles and demonstrate through design and testing that adequate controls are in place.
  - Unvalidated systems may present a significant vulnerability regarding data integrity as user access and system configuration may allow data amendment.
- 
- Check that end-user testing includes test-scripts designed to demonstrate that software not only meets the requirements of the vendor, but is fit for its intended use.

## 5. Expectation

### Periodic System Evaluation

Computerised systems should be evaluated periodically in order to ensure continued compliance with respect to data integrity controls. The evaluation should include deviations, changes (including any cumulative effect of changes), upgrade history, performance and maintenance, and assess whether these changes have had any detrimental effect on data management and integrity controls.

The frequency of the re-evaluation should be based on a risk assessment depending on the criticality of the computerised systems considering the cumulative effect of changes to the system since last review. The assessment performed should be documented.

### Potential risk of not meeting expectations/items to be checked

- Check that re-validation reviews for computerised systems are outlined within validation schedules.
- Verify that systems have been subject to periodic review, particularly with respect to any potential vulnerabilities regarding data integrity.
- Any issues identified, such as limitations of current software/hardware should be addressed in a timely manner and corrective and preventive actions, and interim controls should be available and implemented to manage any identified risks.

189

## 6. Expectation

Operating systems and network components (including hardware) should be updated in a timely manner according to vendor recommendations and migration of applications from older to newer platforms should be planned and conducted in advance of the time before the platforms reach an unsupported state which may affect the management and integrity of data generated by the system.

Security patches for operating systems and network components should be applied in a controlled and timely manner according to vendor recommendations in order to maintain data security. The application of security patches should be performed in accordance with change management principles.

Where unsupported operating systems are maintained, i.e. old operating systems are used even after they run out of support by the vendor or supported versions are not security patched, the systems (servers) should be isolated as much as possible from the rest of the network. Remaining interfaces and data transfer to/from other equipment should be carefully designed, configured and qualified to prevent exploitation of the vulnerabilities caused by the unsupported operating system.

114TPDA04006-B

190



Remote access to unsupported systems should be carefully evaluated due to inherent vulnerability risks.

**Potential risk of not meeting expectations/items to be checked**

- Verify that system updates are performed in a controlled and timely manner. Older systems should be reviewed critically to determine whether appropriate data integrity controls are integrated, or, (where integrated controls are not possible) that appropriate administrative controls have been implemented and are effective.

#### 9.4 Data Transfer

| Item: | Data transfer and migration   |
|-------|---|
| 1.    | <p><b>Expectation</b></p> <p>Interfaces should be assessed and addressed during validation to ensure the correct and complete transfer of data.</p> <p>Interfaces should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimise data integrity risks. Verification methods may include the use of:</p> <ul style="list-style-type: none"> <li>○ Secure transfer</li> <li>○ Encryption</li> <li>○ Checksums</li> </ul> <p>Where applicable, interfaces between systems should be designed and qualified to include an automated transfer of GMP/GDP data.</p> |

### Potential risk of not meeting expectations/items to be checked

- Interfaces between computerised systems present a risk whereby data may be inadvertently lost, amended or transcribed incorrectly during the transfer process.
- Ensure data is transferred directly to the secure location/database and not simply copied from the local drive (where it may have the potential to be altered).
- Temporary data storage on local computerised systems (e.g. instrument computer) before transfer to final storage or data processing location creates an opportunity for data to be deleted or manipulated. This is a particular risk in the case of 'standalone' (non-networked) systems. Ensure the environment that initially stores the data has appropriate DI controls in place.
- Well designed and qualified automated data transfer is much more reliable than any manual data transfer conducted by humans.

## 2. Expectation

Where system software (including operating system) is installed or updated, the user should ensure that existing and archived data can be

read by the new software. Where necessary this may require conversion of existing archived data to the new format.

Where conversion to the new data format of the new software is not possible, the old software should be maintained, e.g. installed in one computer or other technical solution, and also available as a backup media in order to have the opportunity to read the archived data in case of an investigation.

### Potential risk of not meeting expectations/items to be checked

- It is important that data is **readable** in its **original form** throughout the data lifecycle, and therefore users should maintain the readability of data, which may require maintaining **access** to **superseded** software.
- The **migration** of data from one system to another should be performed in a **controlled manner**, in accordance with documented **protocols**, and should include appropriate **verification** of the **complete** migration of data.

### 3. Expectation

When **legacy** systems software can **no longer** be supported, consideration should be given to **maintaining** the software for **data accessibility purposes** (for as long possible depending upon the specific **retention requirements**). This may be achieved by maintaining **software in a virtual environment**.

**Migration** to an alternative file **format** that **retains** as much as possible of the 'true copy' attributes of the data may be necessary with increasing age of the **legacy data**.

Where **migration** with full original data functionality is **not** technically possible, **options** should be assessed based on **risk** and the **importance** of the data over time. The migration file format should be selected considering the balance of **risk** between **long-term** accessibility versus the **possibility** of **reduced** dynamic data functionality (e.g. **data interrogation**, **trending**, **re-processing**, etc.) The risk assessment should also review the **vulnerability** of the system to inadvertent or unauthorised changes to critical configuration settings or manipulation of data. **All controls** to mitigate risk should be **documented** and their **effectiveness** verified. It is recognised that the need to maintain accessibility may require migration to a file format that **loses** some attributes and/or dynamic data functionality.



### Potential risk of not meeting expectations/items to be checked

- When the software is maintained in a virtual environment, check that appropriate measures to control the software (e.g. validation status, access control by authorised persons, etc.) are in place. All controls should be documented and their effectiveness verified.

## 9.5 System security for computerised systems

| Item: | System security  |
|-------|--|
| 1.    | <p><b>Expectation</b></p> <p>User access controls shall be configured and enforced to prohibit unauthorised access to, changes to and deletion of data. The extent of security controls is dependent on the criticality of the computerised system. For example:</p> <ul style="list-style-type: none"> <li>Individual Login IDs and passwords should be set up and assigned for all staff needing to access and utilise the specific electronic system. Shared login credentials do not allow for traceability to the individual who performed the activity. For this reason, shared passwords, even for reasons of financial savings, should be prohibited. Login parameters should be verified during validation of the electronic system to ensure that login profiles, configuration and password format are clearly defined and function as intended.</li> </ul> |

- Input of data and changes to computerised records should be made only by authorised personnel. Companies should maintain a list of authorised individuals and their access privileges for each electronic system in use.
- Appropriate controls should be in place regarding the format and use of passwords, to ensure that systems are effectively secured.
- Upon initially having been granted system access, a system should allow the user to create a new password, following the normal password rules.
- Systems should support different user access roles (levels) and assignment of a role should follow the least-privilege rule, i.e. assigning the minimum necessary access level for any job function. As a minimum, simple systems should have normal and admin users, but complex systems will typically require more levels of users (e.g. a hierarchy) to effectively support access control.

- Granting of administrator access rights to computerised systems and infrastructure used to run GMP/GDP critical applications should be strictly controlled. Administrator access rights should not be given to normal users on the system (i.e. segregation of duties).
- Normal users should not have access to critical aspects of the computerised system, e.g. system clocks, file deletion functions, etc.
- Systems should be able to generate a list of users with actual access to the system, including user identification and roles. User lists should include the names or unique identifiers that permit identification of specific individuals. The list should be used during periodic user reviews.



- Systems should be able to generate a list of successful and unsuccessful login attempts, including:
  - User identification
  - User access role
  - Date and time of the attempted login, either in local time or traceable to local time
  - Session length, in the case of successful logins
- User access controls should ensure strict segregation of duties (i.e. that all users on a system who are conducting normal work tasks should have only normal access rights). Normally, users with elevated access rights (e.g. admin) should not conduct normal work tasks on the system.

- System administrators should normally be independent from users performing the task, and have no involvement or interest in the outcome of the data generated or available in the electronic system. For example, QC supervisors and managers should not be assigned as the system administrators for electronic systems in their laboratories (e.g. HPLC, GC, UV-Vis). Typically, individuals outside of the quality and production organisations (e.g. Information Technology administrators) should serve as the system administrators and have enhanced permission levels.

- For smaller organisations, it may be permissible for a nominated person in the quality unit or production department to hold access as the system administrator; however, in these cases the administrator access should not be used for performing routine operations and the user should hold a second and restricted access for performing routine operations. In these cases all administrator activities conducted should be recorded and approved within the quality system.

- Any request for new users, new privileges of users should be authorised by appropriate personnel (e.g. line manager and system owner) and forwarded to the system administrator in a traceable way in accordance with a standard procedure.
- Computerised systems giving access to GMP/GDP critical data or operations should have an inactivity logout, which, either at the application or the operating system level, logs out a user who has been inactive longer than a predefined time. The time should be shorter, rather than longer and should typically be set to prevent unauthorised access to systems. Upon activation of the inactivity logout, the system should require the user to go through the normal authentication procedure to login again.

### Potential risk of not meeting expectations/items to be checked

- Check that the company has taken all reasonable steps to ensure that the computerised system in use is secured, and protected from deliberate or inadvertent changes.
- Systems that are not physically and administratively secured are vulnerable to data integrity issues. Inspectorates should confirm that verified procedures exist that manage system security, ensuring that computerised systems are maintained in their validated state and protected from manipulation.
- Check that individual user log-in IDs are in use. Where the system configuration allows the use of individual user log-in IDs, these should be used.
- It is acknowledged that some legacy computerised systems support only a single user login or limited numbers of user logins. Where no suitable alternative computerised system is available, equivalent control may be provided by third party software, or a paper based method of providing traceability (with version control). The suitability

205

of alternative systems should be justified and documented. Increased data review is likely to be required for hybrid systems.

- Inspectors should verify that a password policy is in place to ensure that systems enforce good password rules and require strong passwords. Consideration should be made to using stronger passwords for systems generating or processing critical data.
- Systems where a new password cannot be changed by the user, but can only be created by the admin, are incompatible with data integrity, as the confidentiality of passwords cannot be maintained.
- Check that user access levels are appropriately defined, documented and controlled. The use of a single user access level on a system and assigning all users this role, which per definition will be the admin role, is not acceptable.
- Verify that the system uses authority checks to ensure that only authorised individuals can use the system, electronically sign a record, access the operation or computerised system input or output device, alter a record, or perform the operation at hand.

206



## 2. Expectation

Computerised systems should be protected from accidental changes or deliberate manipulation. Companies should assess systems and their design to prevent unauthorised changes to validated settings that may ultimately affect data integrity. Consideration should be given to:

- The physical security of computerised system hardware:
  - Location of and access to servers;
  - Restricting access to PLC modules, e.g. by locking access panels.
  - Physical access to computers, servers and media should be restricted to authorised individuals. Users on a system should not normally have access to servers and media.
- Vulnerability of networked systems from local and external attack;
- Remote network updates, e.g. automated updating of networked systems by the vendor.

207

- Security of system settings, configurations and key data. Access to critical data/operating parameters of systems should be appropriately restricted and any changes to settings/configuration controlled through change management processes by authorised personnel.
- The operating system clock should be synchronized with the clock of connected systems and access to all clocks restricted to authorised personnel.
- Appropriate network security measures should be applied, including intrusion prevention and detection systems.
- Firewalls should be setup to protect critical data and operations. Port openings (firewall rules) should be based on the least privilege policy, making the firewall rules as tight as possible and thereby allowing only permitting traffic.

208

Regulated users should conduct periodic reviews of the continued appropriateness and effectiveness of network security measures, (e.g. by the use of network vulnerability scans of the IT infrastructure to identify potential security weaknesses) and ensure operating systems are maintained with current security measures.

#### Potential risk of not meeting expectations/items to be checked

- Check that access to hardware and software is appropriately secured, and restricted to authorised personnel.
- Verify that suitable authentication methods are implemented. These methods should include user IDs and passwords but other methods are possible and may be required. However, it is essential that users are positively identifiable.
- For remote authentication to systems containing critical data available via the internet; verify that additional authentication techniques are employed such as the use of pass code tokens or biometrics.
- Verify that access to key operational parameters for systems is appropriately controlled and that, where appropriate, systems enforce the correct order of events and parameters in critical sequences of GMP/GDP steps.

### 3. Expectation

#### Network protection

Network system security should include appropriate methods to detect and prevent potential threats to data.

The level of network protection implemented should be based on an assessment of data risk.

Firewalls should be used to prevent unauthorised access, and their rules should be subject to periodic reviews against specifications in order to ensure that they are set as restrictive as necessary, allowing only permitted traffic. The reviews should be documented.

Firewalls should be supplemented with appropriate virus-protection or intrusion prevention/detection systems to protect data and computerised systems from attempted attacks and malware.

211

#### **Potential risk of not meeting expectations/items to be checked**

- Inadequate network security presents risks associated with vulnerability of systems from unauthorised access, misuse or modification.
- Check that appropriate measures to control network access are in place. Processes should be in place for the authorisation, monitoring and removal of access.
- Systems should be designed to prevent threats and detect attempted intrusions to the network and these measures should be installed, monitored and maintained.
- Firewall rules are typically subject to changes over time, e.g. temporary opening of ports due to maintenance on servers etc. If never reviewed, firewall rules may become obsolete permitting unwanted traffic or intrusions.

212



4. Electronic signatures used in the place of handwritten signatures should have appropriate controls to ensure their authenticity and traceability to the specific person who electronically signed the record(s).

Electronic signatures should be permanently linked to their respective record, i.e. if a later change is made to a signed record; the record should indicate the amendment and appear as unsigned.

Where used, electronic signature functionality should automatically log the date and time when a signature was applied.

The use of advanced forms of electronic signatures is becoming more common (e.g. the use of biometrics is becoming more prevalent by firms). The use of advanced forms of electronic signatures should be encouraged.

#### Potential risk of not meeting expectations/items to be checked

- Check that electronic signatures are appropriately validated, their issue to staff is controlled and that at all times, electronic signatures are readily attributable to an individual.
- Any changes to data after an electronic signature has been assigned should invalidate the signature until the data has been reviewed again and re-signed.



## 5. Restrictions on use of USB devices

For reasons of system security, computerised systems should be configured to prevent vulnerabilities from the use of USB memory sticks and storage devices on computer clients and servers hosting GMP/GDP critical data. If necessary, ports should only be opened for approved purposes and all USB devices should be properly scanned before use.

The use of private USB devices (flash drives, cameras, smartphones, keyboards, etc.) on company computer clients and servers hosting GMP/GDP data, or the use of company USB devices on private computers, should be controlled in order to prevent security breaches.

215

### **Potential risk of not meeting expectations/items to be checked**

- This is especially important where operating system vulnerabilities are known that allow USB devices to trick the computer, by pretending to be another external device, e.g. keyboard, and can contain and start executable code.
- Controls should be in place to restrict the use of such devices to authorised users and measures to screen USB devices before use should be in place.

216

## 9.6 Audit trails for computerised systems

|              |  |
|--------------|--|
| <b>Item:</b> | <b>Audit Trails</b>  |
| <b>1.</b>    | <p><b>Expectation</b></p> <p>Consideration should be given to data management and integrity requirements when purchasing and implementing computerised systems. Companies should select software that includes appropriate electronic audit trail functionality.</p> <p>Companies should endeavour to purchase and upgrade older systems to implement software that includes electronic audit trail functionality.</p> <p>It is acknowledged that some very simple systems lack appropriate audit trails; however, alternative arrangements to verify the veracity of data should be implemented, e.g. administrative procedures, secondary checks and controls. Additional guidance may be found under section 9.10 regarding hybrid systems.</p> |

217

Audit trail functionality should be verified during validation of the system to ensure that all changes and deletions of critical data associated with each manual activity are recorded and meet ALCOA+ principles.

Regulated users should understand the nature and function of audit trails within systems, and should perform an assessment of the different audit trails during qualification to determine the GMP/GDP relevance of each audit trail, and to ensure the correct management and configuration of audit trails for critical and GMP/GDP relevant data. This exercise is important in determining which specific trails and which entries within trails are of significance for review with a defined frequency established. For example, following such an assessment audit trail reviews may focus on:

218

- Identifying and reviewing entries/data that relate to changes or modification of data.
- Review by exception – focusing on anomalous or unauthorized activities.
- Systems with limitations that allow change of parameters/data or where activities are left open to modification
- Note: Well-designed systems with permission settings that prevent change of parameters/data or have access restrictions that prevent changes to configuration settings may negate the need to examine related audit trails in detail

Audit trail functionalities should be enabled and locked at all times and it should not be possible to deactivate, delete or modify the functionality. If it is possible for administrative users to deactivate, delete or modify the audit trail functionality, an automatic entry should be made in the audit trail indicating that this has occurred.

Companies should implement procedures that outline their policy and processes to determine the data that is required in audit trails, and the review of audit trails in accordance with risk management principles. Critical



audit trails related to each operation should be independently reviewed with all other records related to the operation and prior to the review of the completion of the operation (e.g. prior to batch release) so as to ensure that critical data and changes to it are acceptable. This review should be performed by the originating department, and where necessary verified by the quality unit, e.g. during self-inspection or investigative activities.

Non-critical audit trails reviews can be conducted during system reviews at a pre-defined frequency. This review should be performed by the originating department, and where necessary verified by the quality unit (e.g. during batch release, self-inspection or investigative activities).

#### Potential risk of not meeting expectations/items to be checked

- Validation documentation should demonstrate that audit trails are functional, and that all activities, changes and other transactions within the systems are recorded, together with all relevant metadata.
- Verify that audit trails are regularly reviewed (in accordance with quality risk management principles) and that discrepancies are investigated.
- If no electronic audit trail system exists a paper based record to demonstrate changes to data may be acceptable until a fully audit trailed (integrated system or independent audit software using a validated interface) system becomes available. These hybrid systems are permitted, where they achieve equivalence to integrated audit trail, such as described in Annex 11 of the PIC/S GMP Guide.
- Failure to adequately review audit trails may allow manipulated or erroneous data to be inadvertently accepted by the Quality Unit and/or Authorised Person.
- Clear details of which data are critical, and which changes and deletions should be recorded (audit trail) should be documented.

## 2.

**Expectation**

Where available, **audit trail** functionalities for electronic-based systems should be assessed and configured properly to **capture any critical activities** relating to the **acquisition, deletion, overwriting** of and **changes** to data for audit purposes.

**Audit trails** should be configured to record all **manually initiated** processes related to critical data.

The system should provide a **secure, computer generated, time stamped** audit trail to independently **record the date and time** of entries and actions that **create, modify, or delete** electronic records.

The **audit trail** should include the following parameters:

- details of the **user** that undertook the action;
- **what action** occurred, was changed, incl. old and new values;
- **when** the action was taken, incl. date and time ;
- **why** the action was taken (reason); and

223

- in the case of **changes or modifications** to data, the **name** of any person authorising the change.

The audit trail should allow for **reconstruction** of the **course** of events relating to the creation, modification, or deletion of an electronic record.

The system should be able to **print** and provide an **electronic copy** of the **audit trail**, and whether **viewing** in the system **online** or in a **hardcopy**, the audit trail should be available in a meaningful format.

If possible, the **audit trail** should **retain** the **dynamic** functionalities found in the computerised system, (e.g. **search** functionality and ability to **export** data such as to a spreadsheet).

Note: An **audit trail** should not be confused with a **change control system** where changes may needed to appropriately controlled and approved under a PQS.

224

### Potential risk of not meeting expectations/items to be checked

- Verify the **format** of audit trails to ensure that all critical and relevant information is captured.
- The audit trail should include all **previous values** and **record changes** should **not overwrite** or **obscure** previously recorded information.
- Audit trail entries should be recorded in **true time** and **reflect** the actual time of activities. Systems recording the same time for a number of **sequential** interactions, or which only make an **entry** in the audit trail, once **all interactions** have been **completed**, may **not** be in **compliance** with expectations to data integrity, particularly where each discrete interaction or sequence is critical, e.g. for the electronic recording of addition of 4 raw materials to a mixing vessel. If the **order** of addition is a critical process parameter (CPP), then each addition should be recorded **individually**, with **time stamps**. If the **order** of addition is **not** a CPP then the addition of **all 4** materials could be recorded as a **single** timestamped activity.

## 9.7 Data capture/entry for computerised systems

|              |  |
|--------------|--|
| <b>Item:</b> | <b>Data capture/entry</b>  |
| <b>1.</b>    | <p><b>Expectation</b></p> <p>Systems should be designed for the <b>correct capture</b> of data whether acquired through <b>manual</b> or <b>automated</b> means.</p> <p>For <b>manual entry</b>:</p> <ul style="list-style-type: none"> <li>- The entry of <b>critical data</b> should only be made by <b>authorised individuals</b> and the system should record details of the <b>entry</b>, the <b>individual</b> making the entry and <b>when</b> the entry was made.</li> </ul> |



- Data should be entered in a specified format that is controlled by the software, validation activities should verify that invalid data formats are not accepted by the system.
- All manual data entries of critical data should be verified, either by a second operator, or by a validated computerised means.
- Changes to entries should be captured in the audit trail and reviewed by an appropriately authorised and independent person.

For automated data capture: (refer also to table 9.3)

- The interface between the originating system, data acquisition and recording systems should be validated to ensure the accuracy of data.
- Data captured by the system should be saved into memory in a format that is not vulnerable to manipulation, loss or change.
- The system software should incorporate validated checks to ensure the completeness of data acquired, as well as any relevant metadata associated with the data.

#### Potential risk of not meeting expectations/items to be checked

- Ensure that manual entries of critical data made into computerised systems are subject to an appropriate secondary check.
- Validation records should be reviewed for systems using automated data capture to ensure that data verification and integrity measures are implemented and effective, e.g. verify whether an auto save function was validated and, therefore, users have no ability to disable it and potentially generate unreported data.



## 2. Expectation

Any necessary changes to data should be authorised and controlled in accordance with approved procedures.

For example, manual integrations and reprocessing of laboratory results should be performed in an approved and controlled manner. The firm's quality unit should establish measures to ensure that changes to data are performed only when necessary and by designated individuals. Original (unchanged) data should be retained in its original context.

Any and all changes and modifications to raw data should be fully documented and should be reviewed and approved by at least one appropriately trained and qualified individual.

229

### Potential risk of not meeting expectations/items to be checked

- Verify that appropriate procedures exist to control any amendments or re-processing of data. Evidence should demonstrate an appropriate process of formal approval for the proposed change, controlled/restricted/defined changes and formal review of the changes made.

230

## 9.8 Review of data within computerised systems

|              |   |
|--------------|---|
| <b>Item:</b> | <b>Review of electronic data</b>  |
| <b>1.</b>    | <p><b>Expectation</b></p> <p>The regulated user should perform a risk assessment in order to identify all the GMP/GDP relevant <b>electronic data</b> generated by the computerised systems, and the <b>criticality</b> of the data. Once identified, <b>critical data</b> should be <b>audited</b> by the regulated user and verified to determine that <b>operations</b> were performed correctly and whether any <b>change</b> (<b>modification</b>, <b>deletion</b> or <b>overwriting</b>) have been made to original information in electronic records, or whether any relevant <b>unreported data</b> was <b>generated</b>. All <b>changes</b> should be duly authorised.</p> <p>An <b>SOP</b> should describe the process by <b>which data is checked</b> by a <b>second operator</b>. These SOPs should outline the critical raw data that is reviewed, a review of <b>data summaries</b>, review of any associated <b>log-books</b> and <b>hard-copy records</b>, and explain <b>how</b> the review is performed, recorded and authorised.</p> |

231

The review of **audit trails** should be part of the **routine data review** within the approval process.

The **frequency**, roles and responsibilities of **audit trail review** should be based on a **risk assessment** according to the GMP/GDP relevant value of the data recorded in the computerised system. For example, for **changes** of electronic data that can have a direct impact on the quality of the medicinal products, it would be **expected to review** audit trails prior to the point that the data is relied upon to **make a critical decision**, e.g. batch release.

232

The regulated user should establish an SOP that describes in detail how to review audit trails, what to look for and how to perform searches etc. The procedure should determine in detail the process that the person in charge of the audit trail review should follow. The audit trail review activity should be documented and recorded.

Any significant variation from the expected outcome found during the audit trail review should be fully investigated and recorded. A procedure should describe the actions to be taken if a review of audit trails identifies serious issues that can impact the quality of the medicinal products or the integrity of data.

#### **Potential risk of not meeting expectations/items to be checked**

- Check local procedures to ensure that electronic data is reviewed based on its criticality (impact to product quality and/or decision making). Evidence of each review should be recorded and available to the inspector.
- Where data summaries are used for internal or external reporting, evidence should be available to demonstrate that such summaries have been verified in accordance with raw data.



- Check that the regulated party has a detailed SOP outlining the steps on how to perform secondary reviews and audit trail reviews and what steps to take if issues are found during the course of the review.
- Where global systems are used, it may be necessary for date and time records to include a record of the time zone to demonstrate contemporaneous recording.
- Check that known changes, modifications or deletions of data are actually recorded by the audit trail functionality.

2. The company's quality unit should establish a program and schedule to conduct ongoing reviews of audit trails based upon their criticality and the system's complexity in order to verify the effective implementation of current controls and to detect potential non-compliance issues. These reviews should be incorporated into the company's self-inspection programme.

Procedures should be in place to address and investigate any audit trail discrepancies, including escalation processes for the notification of senior management and national authorities where necessary.

**Potential risk of not meeting expectations/items to be checked**

- Verify that self-inspection programs incorporate checks of audit trails, with the intent to verify the effectiveness of existing controls and compliance with internal procedures regarding the review of data.
- Audit trail reviews should be both random (selected based on chance) and targeted (selected based on criticality or risk).

|              |  |
|--------------|--|
| <b>Item:</b> | <b>Storage, archival and disposal of electronic data</b>   |
| <b>1.</b>    | <p><b>Expectation</b></p> <p>Storage of data should include the entire original data and all relevant metadata, including audit trails, using a secure and validated process.</p> <p>If the data is backed up, or copies of it are made, then the backup and copies should also have the same appropriate levels of controls so as to prohibit unauthorised access to, changes to and deletion of data or their alteration. For example, a firm that backs up data onto portable hard drives should prohibit the ability to delete data from the hard drive. Some additional considerations for the storage and backup of data include:</p> <ul style="list-style-type: none"> <li>- True copies of dynamic electronic records can be made, with the expectation that the entire content (i.e. all data and all relevant metadata is included) and meaning of the original records are preserved.</li> <li>- Stored data should be accessible in a fully readable format. Companies may need to maintain suitable software and hardware</li> </ul> |

to access electronically stored data backups or copies during the retention period

- Routine backup copies should be stored in a remote location (physically separated) in the event of disasters.
- Back-up data should be readable for all the period of the defined regulatory retention period, even if a new version of the software has been updated or substituted for one with better performance.
- Systems should allow backup and restoration of all data, including meta-data and audit trails.

#### **Potential risk of not meeting expectations/items to be checked**

- Check that data storage, back-up and archival systems are designed to capture all data and relevant metadata. There should be documented evidence that these systems have been validated and verified.
- The extent of metadata captured should be based on risk management principles, and users should ensure that all metadata critical in the reconstruction of activities or processes are captured.
- Check that data associated with superseded or upgraded systems is managed appropriately and is accessible.



## 2. Expectation

The record retention procedures should include provisions for retaining the metadata. This allows for future queries or investigations to reconstruct the activities that occurred related to a batch.

## 3. Expectation

Data should be backed-up periodically and archived in accordance with written procedures. Archive copies should be physically (or virtually, where relevant) secured in a separate and remote location from where back up and original data are stored.

The data should be accessible and readable and its integrity maintained for all the period of archiving.

There should be in place a procedure for restoring archived data in case an investigation is needed. The procedure in place for restoring archived data should be regularly tested.

If a facility is needed for the archiving process then specific environmental controls and only authorised personnel access should be implemented in order to ensure the protection of records from deliberate or inadvertent alteration or loss. When a system in the facility has to be retired because problems with long term access to data are envisaged, procedures should assure the continued readability of the data archived. For example, it could be established to transfer the data to another system.

### Potential risk of not meeting expectations/items to be checked

- There is a risk with archived data that access and readability of the data may be lost due to software application updates or superseded equipment. Verify that the company has access to archived data,

and that they maintain access to the necessary software to enable review of the archived data.

- Where external or third party facilities are utilised for the archiving of data, these service providers should be subject to assessment, and all responsibilities recorded in a quality technical agreement. Check agreements and assessment records to verify that due consideration has been given to ensuring the integrity of archived records.

241

## 4. Expectation

It should be possible to print out a legible and meaningful record of all the data generated by a computerised system (including metadata).

If a change is performed to records, it should be possible to also print out the change of the record, indicating when and how the original data was changed.

### Potential risk of not meeting expectations/items to be checked

- Check validation documentation for systems to ensure that systems have been validated for the generation of legible and complete records.
- Samples of print-outs may be verified.

242



5.

**Expectation**

Procedures should be in place that describe the process for the disposal of electronically stored data. These procedures should provide guidance for the assessment of data and allocation of retention periods, and describe the disposal of data that is no longer required.

**Potential risk of not meeting expectations/items to be checked**

- Check that the procedures clearly stipulate the conditions for the disposal of data, and that care is taken to avoid the inadvertent disposal of required data during its lifecycle.

243

## 9.10 Management of Hybrid Systems

| Item: | <b>Management of Hybrid Systems</b>  |
|-------|--|
| 1.    | <p>Hybrid systems require specific and additional controls in reflection of their complexity and potential increased vulnerability to manipulation of data. For this reason, the use of hybrid systems is discouraged and such systems should be replaced whenever possible.</p> <p>Each element of the hybrid system should be qualified and controlled in accordance with the guidance relating to manual and computerised systems as specified above.</p> |

244

Appropriate quality risk management principles should be followed when assessing, defining, and demonstrating the effectiveness of control measures applied to the system.

A detailed system description of the entire system should be available that outlines all major components of the system, the function of each component, controls for data management and integrity, and the manner in which system components interact.

Procedures and records should be available to manage and appropriately control the interface between manual and automated systems, particularly steps associated with:

- manual input of manually generated data into computerised systems;
- transcription (including manual) of data generated by automated systems onto paper records; and
- automated detection and transcription of printed data into computerised systems.

#### Potential risk of not meeting expectations/items to be checked

- Check that hybrid systems are clearly defined and identified, and that each contributing element of the system is validated.
- Attention should be paid to the interface between the manual and computerised system. Inspectors should verify that adequate controls and secondary checks are in place where manual transcription between systems takes place.
- Original data should be retained following transcription and processing.
- Hybrid systems commonly consist of a combination of computerised and manual systems. Particular attention should be paid to verifying:
  - The extent of qualification and/or validation of the computerised system; and,
  - The robustness of controls applied to the management of the manual element of the hybrid system due to the difficulties in consistent application of a manual process.

2. Procedures should be in place to manage the review of data generated by hybrid systems which clearly outline the process for the evaluation and approval of electronic and paper-based data. Procedures should outline:
- Instructions for how electronic data and paper-based data is correlated to form a complete record.
  - Expectations for approval of data outputs for each system.
  - Risks identified with hybrid systems, with a focus on verification of the effective application of controls

**Potential risk of not meeting expectations/items to be checked**

- Verify that instructions for the review of hybrid system data is in place.

● **10 DATA INTEGRITY CONSIDERATIONS FOR OUTSOURCED ACTIVITIES**

● **10.1 General supply chain considerations**

- 10.1.1 Modern supply chains often consist of multiple partner companies working together to ensure safe and continued supply of medicinal products. Typical supply chains require the involvement of API producers, dosage form manufacturers, analytical laboratories, wholesale and distribution organisations, often from differing organisations and locations. These supply chains are often supported by additional organisations, providing outsourced services, IT services and infrastructure, expertise or consulting services.

- 供應鏈|委外項目

- 10.1.2 **Data integrity** plays a key part in ensuring the **security** and **integrity** of supply chains. **Data governance** measures **by** a **contract giver** may be significantly weakened **by** unreliable or falsified data or materials provided **by** supply chain partners. This principle **applies** to **all** outsourced activities, including **suppliers** of **raw materials**, **contract manufacturers**, **analytical services**, **wholesalers**, **contracted** service providers and consultants.
- DI的數據管控與所有供應鏈的廠商有關

- 10.1.3 **Initial** and **periodic re-qualification** of supply chain **partners** and **outsourced** activities should include **consideration** of **data integrity** risks and appropriate **control measures**.
- 供應商評估應包括DI assessment

- 10.1.4 It is important for an organisation to understand the **data integrity limitations** of information obtained from the **supply chain** (e.g. summary records and copies / printouts) and **the challenges of remote** supervision. These **limitations** are similar to those discussed in section **8.11** of this guidance. This will help to focus resources towards **data integrity verification** and **supervision** using a **quality risk management approach**.

- DI的弱點及挑戰 | 著重於確認其系統 | 使用Q9的精神來進行確認

251

- **10.2 Routine document verification**

- 10.2.1 The **supply chain** relies upon the use of **documentation** and **data** passed from one organisation to another. It is often **not** practical for the **contract giver** to review **all** raw data relating to reported results. **Emphasis** should be placed upon a **robust qualification process** for **outsourced** supplier and contractor, using quality risk management **principles**.

- 所有數據都是關鍵

252



### ● 10.3 Strategies for assessing data integrity in the supply chain

- 10.3.1 Companies should conduct regular risk reviews of supply chains and outsourced activity that evaluate the extent of data integrity controls required. The frequency of such reviews should be based on the criticality of the services provided by the contract acceptor, using risk management principles, Information considered during risk reviews may include:
  - The outcome of site audits, with focus on data governance measures
  - Demonstrated compliance with international standards or guidelines related to data integrity and security
  - Review of data submitted in routine reports, for example:
    - 外來數據之基本要求

253

| Area for review  | Rationale  |
|--|--|
| Comparison of analytical data reported by the contractor or supplier vs in-house data from analysis of the same material | To look for discrepant data which may be an indicator of falsification |

254

- 10.3.2 **Quality agreements** (or equivalent) should be in place **between** manufacturers and suppliers of materials, service providers, contract manufacturing organisations (CMOs) **and** (in the case of distribution) suppliers of medicinal products, **with** specific provisions for ensuring **data integrity** across the supply chain. This may be achieved by setting out **expectations** for **data governance**, and **transparent error/deviation reporting** by the **contract acceptor** to the contract giver. There should also be a requirement to **notify** the contract giver of any data integrity **failures** identified at the contract acceptor site.

- 報告任何DI的議題

255

- 10.3.3 **Audits** of suppliers and manufacturers of **APIs**, critical **intermediate** suppliers, primary and printed **packaging materials** suppliers, contract **manufacturers** and service providers conducted **by** the **manufacturer** (or by a third party on their behalf) should include a **verification** of **data integrity** measures at the contract organisation. **Contract acceptors** are expected to provide **reasonable access** to data generated on behalf of the contract giver **during audits**, so that compliance with **data integrity** and **management** principles can be assessed and demonstrated.

- 供應商稽核重點之一：DI

256

- 10.3.4 Audits and routine surveillance should include adequate verification of the source electronic data and metadata by the Quality Unit of the contract giver using a quality risk management approach. This may be achieved by measures such as:

- 稽核及定期審閱

257

|                         |  |
|-------------------------|--|
| Site audit              | Review the contract acceptors organisational behaviour, and understanding of data governance, data lifecycle, risk and criticality.  |
| Material testing vs CoA | Compare the results of analytical testing vs suppliers reported CoA. Examine discrepancies in accuracy, precision or purity results. This may be performed on a routine basis, periodically, or unannounced, depending on material and supplier risks. Periodic proficiency testing of samples may be considered where relevant.   |
| Remote data review      | <p>The contract giver may consider offering the Contracted Facility/Supplier use of their own hardware and software system (deployed over a Wide Area Network) to use in batch manufacture and testing. The contract giver may monitor the quality and integrity of the data generated by the Contracted Facility personnel in real time.</p> <p>In this situation, there should be segregation of duties to ensure that contract giver monitoring of data does not give provision for amendment of data generated by the contract acceptor.</p> |

114TPDA04006-B

|                    |   |
|--------------------|---|
| Quality monitoring | Quality and performance monitoring may indicate incentive for data falsification (e.g. raw materials which marginally comply with specification on a frequent basis). |
|--------------------|---|

- 10.3.5 Contract givers may work with the contract acceptor to ensure that all client-confidential information is encoded to de-identify clients. This would facilitate review of source electronic data and metadata at the contract giver's site, without breaking confidentiality obligations to other clients. By reviewing a larger data set, this enables a more robust assessment of the contract acceptors data governance measures. It also permits a search for indicators of data integrity failure, such as repeated data sets or data which does not demonstrate the expected variability.

- 客戶去識別化之命名

- 10.3.6 Care should be taken to ensure the authenticity and accuracy of supplied documentation (refer section 8.11). The difference in data integrity and traceability risks between 'true copy' and 'summary report' data should be considered when making contractor and supply chain qualification decisions.

- 供應商稽核重點

261

## ● 11 REGULATORY ACTIONS IN RESPONSE TO DATA INTEGRITY FINDINGS

### ● 11.1 Deficiency references

- 11.1.1 The integrity of data is fundamental to good manufacturing practice and the requirements for good data management are embedded in the current PIC/S Guides to GMP/GDP for Medicinal products. The following table provides a reference point highlighting some of these existing requirements.

- DI不是新的GMP/GDP要求

262



| <b>ALCOA principle</b> | <b>PIC/S Guide to Good Manufacturing Practice for Medicinal products, PE 009 (Part I):</b> | <b>PIC/S Guide to Good Manufacturing Practice for Medicinal products, PE 009 (Part II):</b> | <b>Annex 11 (Computerised Systems)</b>      | <b>PIC/S Guide to Good Distribution Practice for Medicinal products, PE 011:</b> |
|------------------------|--|---|---|--|
| <b>Attributable</b>    | [4.20, c & f], [4.21, c & i], [4.29 point 5]   | [5.43], [6.14], [6.18], [6.52]  | [2], [12.1], [12.4], [15]                   | [4.2.4], [4.2.5]   |
| <b>Legible</b>         | [4.1], [4.2], [4.7], [4.8], [4.9], [4.10]  | [6.11], [6.14], [6.15], [6.50]  | [4.8], [7.1], [7.2], [8.1], [9], [10], [17] | [4.2.3], [4.2.9]   |
| <b>Contemporaneous</b> | [4.8]  | [6.14]  | [12.4], [14]                                | [4.1], [4.2.9]   |
| <b>Original</b>        | [4.9], [4.27], [Paragraph "Record"]  | [6.14], [6.15], [6.16]  | [8.2], [9]                                  | [4.2.5]  |

|                   |                                |   |   |                  |
|-------------------|--------------------------------|---|---|------------------|
| <b>Accurate</b>   | [4.1], [6.17]                  | [5.40], [5.42], [5.45], [5.46], [5.47], [6.6] | [Paragraph "Principles"] [4.8], [5], [6], [7.2], [10], [11] | [4.2.3]          |
| <b>Complete</b>   | [4.8]                          | [6.16], [6.50], [6.60], [6.61]                | [4.8], [7.1], [7.2], [9]                                    | [4.2.3], [4.2.5] |
| <b>Consistent</b> | [4.2]                          | [6.15], [6.50]                                | [4.8], [5]  | [4.2.3]          |
| <b>Enduring</b>   | [4.1], [4.10]                  | [6.11], [6.12], [6.14]                        | [7.1], [17]   | [4.2.6]          |
| <b>Available</b>  | [Paragraph "Principle"], [4.1] | [6.12], [6.15], [6.16]                        | [3.4], [7.1], [16], [17]                                    | [4.2.1]          |

- 11.2 Classification of deficiencies

- Note: The following guidance is intended to aid consistency in reporting and classification of data integrity deficiencies, and is not intended to affect the inspecting authority's ability to act according to its internal policies or national regulatory frameworks.

- 缺失程度分類

265

- 11.2.1 Deficiencies relating to data integrity failure may have varying impact to product quality. Prevalence of the failure may also vary between the actions of a single employee to an endemic failure throughout the inspected organisation.

- 缺失程度取決於對品質的影響 | 單一事件或普遍事件

266

- 11.2.2 The PIC/S guidance<sup>12</sup> on **classification** of deficiencies states:
- “A **critical** deficiency is a practice or process that has produced, or leads to a **significant risk** of producing either a **product** which is harmful to the human or veterinary patient or a **product** which could result in a harmful residue in a food producing animal. A **critical** deficiency also occurs when it is observed that the manufacturer has engaged in **fraud**, **misrepresentation** or **falsification** of products or data”.
- <sup>12</sup> PI 040 PIC/S Guidance on Classification of GMP Deficiencies
- 嚴重DI缺失

267

- 11.2.3 Notwithstanding the “**critical**” classification of deficiencies relating to fraud, misrepresentation or falsification, it is understood that data integrity deficiencies can also **relate to**:
- Data integrity failure resulting from **bad practice**,
- Opportunity for failure (without evidence of actual failure) due to **absence** of the required **data control measures**.
- DI來自不良行為| 缺乏數據管控機制

268

- 11.2.4 In these cases, it may be appropriate to assign **classification of deficiencies** by taking into account the following (indicative list only):
- **Impact to product with actual or potential risk to patient health: Critical deficiency:**
  - Product failing to **meet** Marketing Authorisation **specification** at **release** or within **shelf life**.
  - Reporting of a '**desired**' result rather than an actual **out of specification** result when reporting of QC tests, critical product or process parameters.
  - **Wide-ranging** misrepresentation or falsification of data, with or without the knowledge and assistance of **senior management**, the extent of which critically **undermines** the **reliability** of the Pharmaceutical Quality System and **erodes** all confidence in the quality and safety of medicines manufactured or handled by the site.

269

- **Impact to product with no risk to patient health: Major deficiency:**
- Data being misreported, e.g. original results '**in specification**', but altered to give a **more favourable** trend.
- Reporting of a '**desired**' result rather than an actual out of specification result when reporting of data which **does not** relate to **QC tests, critical product or process parameters**.
- Failures arising from **poorly designed** data capture systems (e.g. using **scraps of paper** to record info for **later transcription**).

270

- **No impact to product; evidence of moderate failure: Major deficiency:**
- Bad practices and poorly designed systems which may result in opportunities for data integrity issues or loss of traceability across a limited number of functional areas (QA, production, QC etc.). Each in its own right has no direct impact to product quality.

271

- **No impact to product; limited evidence of failure: Other deficiency:**
- Bad practice or poorly designed system which result in opportunities for data integrity issues or loss of traceability in a discrete area.
- Limited failure in an otherwise acceptable system, e.g. manipulation of non-critical data by an individual.

272



- 11.2.5 It is important to build an **overall** picture of the adequacy of the **key elements** (**data governance** process, **design** of systems to facilitate **compliant** data recording, use and verification of **audit trails** and **IT user access** etc.) to make a robust assessment as to **whether** there is a **company-wide** failure, or a deficiency of **limited** scope/ impact.

273

- 11.2.6 **Individual** circumstances (**exacerbating / mitigating factors**) may also **affect** final classification or regulatory action. Further guidance on the **classification of deficiencies** and intra-authority reporting of compliance issues will be available in the *PIC/S Guidance on the classification of deficiencies* **PI 040**.

274



PHARMACEUTICAL INSPECTION CONVENTION  
PHARMACEUTICAL INSPECTION CO-OPERATION SCHEME

PI 040-1  
3 Appendices  
1 January 2019

## PIC/S GUIDANCE ON CLASSIFICATION OF GMP DEFICIENCIES

© PIC/S January 2019  
Reproduction prohibited for commercial purposes.  
Reproduction for internal use is authorised,  
provided that the source is acknowledged.

275

## ● 12 REMEDIATION OF DATA INTEGRITY FAILURES

### ● 12.1 Responding to Significant Data Integrity issues

- 12.1.1 Consideration should be primarily given to **resolving** the **immediate issues** identified and **assessing the risks** associated with the data integrity issues. The **response** by the company in question should outline the **actions** taken as part of a remediation plan. **Responses** from implicated manufacturers should include:

- DI問題修復之考量點

276

- 12.1.1.1 A comprehensive investigation into the extent of the inaccuracies in data records and reporting, to include:
  - A detailed investigation protocol and methodology; a summary of all laboratories, manufacturing operations, products and systems to be covered by the assessment; and a justification for any part of the operation that the regulated user proposes to exclude<sup>13</sup>;
  - Interviews of current and where possible and appropriate, former employees to identify the nature, scope, and root cause of data inaccuracies. These interviews may be conducted by a qualified third party;
  - <sup>13</sup> The scope of the investigation should include an assessment of the extent of data integrity at the corporate level, including all facilities, sites and departments that could potentially be affected.

277

- 12.1.1.1 (cont'd)
  - An assessment of the extent of data integrity deficiencies at the facility. Identify omissions, alterations, deletions, record destruction, non-contemporaneous record completion, and other deficiencies;
  - Determination of the scope (data, products, processes and specific batches) and timeframe for the incident, with justification for the time-boundaries applied;
  - A description of all parts of the operations in which data integrity lapses occurred, additional consideration should be given to global corrective actions for multinational companies or those that operate across multiple sites;

278

- 12.1.1.1 (cont'd)

- A comprehensive **retrospective** evaluation of the **nature** of the data integrity deficiencies, and the identification of **root cause(s)** or most **likely** root cause that will form the **basis** of corrective and preventative actions, as defined in the **investigation protocol**. The services of a qualified **third-party consultant** with specific expertise in the areas where potential **breaches** were identified may be required;

279

- 12.1.1.1 (cont'd)

- A risk assessment of the **potential effects** of the observed failures on the **quality** of the substances, medicines, and products involved. The **assessment** should include **analyses** of the potential **risks** to patients **caused by** the release/distribution of **products** affected by a lapse of **data integrity**, risks posed by **ongoing operations**, and any **impact** on the integrity of data **submitted** to regulatory agencies, including data related to product registration dossiers.

280

- 12.1.1.2 Corrective and preventive actions taken to address the data integrity vulnerabilities and timeframe for implementation, and including:
  - Interim measures describing the actions to protect patients and to ensure the quality of the medicinal products, such as notifying customers, recalling product, conducting additional testing, adding lots to the stability program to assure stability, drug application actions, and enhanced complaint monitoring. Interim measures should be monitored for effectiveness and residual risks should be communicated to senior management, and kept under review.

281

- 12.1.1.2 (cont'd)
  - Long-term measures describing any remediation efforts and enhancements to procedures, processes, methods, controls, systems, management oversight, and human resources (e.g. training, staffing improvements) designed to ensure the data integrity. Where long term measures are identified interim measures should be implemented to mitigate risks.

282



- 12.1.1.3 CAPA effectiveness checks implemented to monitor if the actions taken has eliminated the issue.

283

- 12.1.2 Whenever possible, Inspectorates should meet with senior representatives from the implicated companies to convey the nature of the deficiencies identified and seek written confirmation that the company commits to a comprehensive investigation and a full disclosure of issues and their prompt resolution. A management strategy should be submitted to the regulatory authority that includes the details of the global corrective action and preventive action plan. The strategy should include:

284

- 12.1.2 (cont'd)
- A **comprehensive description** of the **root causes** of the data integrity lapses, including **evidence** that the **scope** and **depth** of the current **action plan** is commensurate with the **findings** of the investigation and **risk assessment**. This should indicate if **individuals** responsible for data integrity lapses remain able to **influence** GMP/GDP-related or drug application data.

285

- 12.1.2 (cont'd)
- A detailed **corrective action plan** that describes **how** the regulated user intends to **ensure** the '**ALOCA+**' attributes (see section 7.4) of all of the data generated, including **analytical data**, **manufacturing records**, and all **data** submitted or presented to the Competent Authority.

286

- 12.1.3 **Inspectorates** should implement **policies** for the **management** of significant data integrity issues identified at inspection in order to **manage** and **contain** risks associated with the data integrity **breach**.

287

- 12.2 Indicators of improvement
- 12.2.1 An **on-site inspection** is recommended to verify the **effectiveness** of actions taken to address serious data integrity issues. Alternative approaches to verify effective **remediation** may be considered in accordance with risk management principles. Some indicators of improvement are:

288

- 12.2.1.1 Evidence of a thorough and open evaluation of the identified issue and timely implementation of effective corrective and preventive actions, including appropriate implementation of corrective and preventive actions at an organisational level;

289

- 12.2.1.2 Evidence of open communication of issues with clients and other regulators. Transparent communication should be maintained throughout the investigation and remediation stages. Regulators should be aware that further data integrity failures may be reported as a result of the detailed investigation. Any additional reaction to these notifications should be proportionate to public health risks, to encourage continued reporting;

290

- 12.2.1.3 **Evidence** of communication of data integrity expectations across the organisation, incorporating and encouraging processes for **open** reporting of potential issues and opportunities **for improvement**;

291

- 12.2.1.4 The regulated user should ensure that an appropriate **evaluation** of the **vulnerability** of electronic systems to data manipulation takes place to ensure that **follow-up actions** have fully resolved all the violations. For this evaluation the services of qualified **third party consultant** with the relevant expertise may be **required**;

292

- 12.2.1.5 Implementation of **data integrity policies** in line with the principles of this guide;
- 12.2.1.6 Implementation of **routine data verification** practices.

## 13 Glossary

### ● Archiving

- Long term, **permanent retention** of completed data and relevant metadata in its **final form** for the purposes of **reconstruction** of the **process** or **activity**.

### ● Audit Trail

- GMP/GDP audit trails are **metadata** that are a **record** of **GMP/GDP critical** information (for example the **creation**, **modification**, or **deletion** of GMP/GDP relevant data), which permit the **reconstruction** of GMP/GDP activities.

### ● Back-up

- A **copy** of **current** (editable) data, **metadata** and **system configuration settings** (e.g. **variable** settings which relate to an **analytical run**) maintained for the purpose of **disaster recovery**.

### ● Computerised system

- A system including the **input** of data, electronic processing and the output of information to be used either for **reporting** or **automatic** control.



- **Data**

- Facts, figures and statistics collected together for **reference** or **analysis**.

- **Data Flow Map**

- A **graphical representation** of the "**flow**" of data through an information system

- **Data Governance**

- The **sum total** of arrangements to **ensure** that data, irrespective of the format in which it is **generated, recorded, processed, retained** and **used** to **ensure** a complete, consistent and accurate record throughout the data lifecycle.

295

- **Data Integrity**

- The degree to which data are complete, consistent, accurate, trustworthy, reliable and that these characteristics of the data are **maintained** throughout the **data life cycle**.
- The data should be **collected** and **maintained** in a secure manner, so that they are attributable, legible, contemporaneously recorded, original (or a true copy) and accurate. Assuring data integrity requires appropriate quality and risk management systems, including adherence to **sound scientific principles** and **good documentation** practices. The data should comply with **ALCOA+** principles.

296

### ● Data Lifecycle

- All phases in the life of the data (including raw data) from initial generation and recording through processing (including transformation or migration), use, data retention, archive / retrieval and destruction.

### ● Data Quality

- The assurance that data produced is exactly what was intended to be produced and fit for its intended purpose. This incorporates ALCOA + principles.<sup>14</sup>
- <sup>14</sup> 'GXP' Data Integrity Guidance and Definitions, MHRA, March 2018

297

### ● Data Ownership

- The allocation of responsibilities for control of data to a specific process owner. Companies should implement systems to ensure that responsibilities for systems and their data are appropriately allocated and responsibilities undertaken.

### ● Dynamic Record

- Records, such as electronic records, that allow an interactive relationship between the user and the record content.<sup>13</sup>

### ● Exception Report

- A validated search tool that identifies and documents predetermined 'abnormal' data or actions, which require further attention or investigation by the data reviewer.

298

- **Good Documentation Practices (GdocP)**

- Those measures that collectively and individually ensure documentation, whether **paper** or **electronic**, meet **data management** and **integrity** principles, e.g. ALCOA+.

- **Hybrid Systems**

- A system for the management and control of data that typically consists of an **electronic system** generating electronic data, supplemented by a defined **manual system** that typically generate a paper-based record. The complete data set from a hybrid system therefore consists of both **electronic** and **paper** data together. Hybrid systems rely on the effective management of both sub-systems for correct operation.

- **Master Document**

- An **original** approved document from which controlled copies for distribution or use can be made.

299

- **Metadata**

- In-file data that describes the **attributes** of other data, and provides context and meaning.
- Typically, these are data that describe the structure, data elements, inter-relationships and other characteristics of data e.g. **audit trails**. Metadata also permit data to be attributable to an **individual** (or if automatically generated, to the original data source). Metadata form an **integral part** of the original record. **Without** the **context** provided by metadata the data has no meaning.

- **Quality Unit**

- The department within the regulated entity responsible for **oversight** of quality including in particular the design, effective implementation, monitoring and maintenance of the **Pharmaceutical Quality System**.

300

### ● Raw Data

- Raw data is defined as the **original record** (data) which can be described as **the first-capture** of information, whether recorded on **paper** or **electronically**. Information that is originally captured in a **dynamic** state should remain **available** in that state.<sup>14</sup>

### ● Static Record

- A record format, such as a paper or electronic record, that is **fixed** and allows little or **no interaction** between the user and the record content.<sup>14</sup>

301

### ● Supply Chain

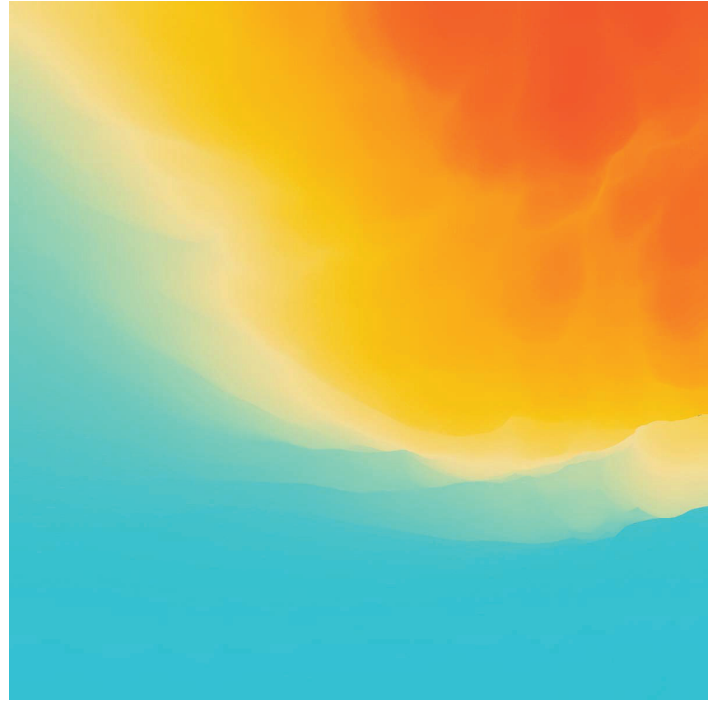
- The **sum total** of arrangements between manufacturing sites, **wholesale** and **distribution** sites that ensure that the quality of medicines is ensured throughout production and distribution to the point of sale or use.

### ● System Administrator

- A person who manages the **operation** of a computerised system or particular electronic communication service.

302

Take a Break



# US FDA Data Integrity 483

2025/4/1, 2025/4/8

Eileen Changchien

1

114TPDA04006-C

## # 1

- a. The validation of your internally developed electronic Quality System "...", which includes the modules of "Material Receiving and Quality Control System" used for material management and "Production and Quality Control System" used for electronic batch record data entry during production, failed to include record retention, audit trial verification, authority check, employee accountability/responsibility policy, and system document control to ensure that data is trustworthy, reliable and generally equivalent to paper records.

2



## # 1

- b. You failed to perform a **change control** to evaluate the **overall impact** of your electronic Quality System ... **from** paper record and recordkeeping.
- c. You lack **data integrity** procedures to assure raw data are original, **unmodifiable**, and **undeletable** for finished pharmaceutical products.

3

## # 2

- Specifically, your firm failed to exercise appropriate controls over your **computers and related system** to assure that **changes** in the records are instituted **only by** authorized personnel. Following are the examples for the **lack of control** on the electronic system, but are not limited to:
- a. You firm utilize a ... **pH meter** (pH meter ..., assessment ID #...) for pH analysis. I observed that analyst can **log into** the system **without** entering a **password**. All usernames created for this instrument are **without a password**. This instrument is capable for **storing** test data and **print** test results. Your firm **neither** review the electronic data generated **nor** print test results for review. Instead, your firm **record** the test result in copies of form Document ... which is **not** controlled **by** the quality department. The **accuracy** of data record on these forms were **not reviewed** by your quality unit.

4

## # 2

- b. During the walkthrough, I observed that your firm utilizes a common username and password to login to a computer system in packaging area. Your Packaging Manager stated that the computer system is utilized to login to ... to print copies of the production records. At that time, a username and password written on a white paper and taped to computer rack.

5

## # 3

- Specifically, computerized systems in your Quality Control laboratory do not have sufficient controls to prevent unauthorized access to, changes to, or omission of data. Electronic data can be deleted from computerized systems connected to your ... instruments with no audit trail to document such an event. Additionally, one general account and password for QC managers and analysts is used for the operating systems installed on these systems, and no computer lock mechanism has been configured to prevent unauthorized access to data.

6

## # 4

- Specifically, power outages and instrument errors hindered testing of ... on Instrument .... Moreover, such a situation rendered data for ... -... deleted and not retrievable. There are no investigations into these events.

7

## # 5

- Specifically, your firm's review of laboratory data does not include a review of an audit trail or revision history of your ... used in the analysis of your ... and ... OTC Drug products to determine if unapproved changes have been made. You do not have procedures on your quality unit reviewing ... audit trails before product disposition and periodic system audit trail review. Your Quality Manager stated that you do not review Audit trails before ... OTC Drug product disposition.

8

## # 6

- Specifically, you provide open access to the Nuclear Magnetic Resonance (NMR) spectroscopy computer to qualified students and staff who have been granted keycard access to the laboratory. You also lack a means to validate or otherwise ensure that electronic data is copied accurately and completely between acquisition, processing, and storage systems.
- a. You lack access controls over NMR spectroscopy computers, which fails to prevent data loss and manipulation. You currently perform NMR testing of .... The instrument computers used for this testing are accessible to any individual with access to the laboratories. A single user ID is used to access the NMR computer. Therefore, user access is not controlled in order to link source data to a specific user. In addition, original source NMR data is stored in a common location without access controls or other protection to prevent potential data deletion or manipulation.

9

## # 6

- b. You do not demonstrate that the source NMR data that undergoes processing and storage is completely and accurately transferred. When NMR source data is collected, the data is saved locally on the NMR computer and then copied to a networked UIC-controlled computer via ... using ... The source data is ... by the staff scientist on the UIC-controlled computer using ... software. Then, both the source NMR data and the ... data are uploaded to a ... folder for storage. None of these data copying/transfer steps are validated to ensure data is not lost or altered. The original source data is deleted from its original acquisition and storage location on the NMR computer by the staff scientist.

10

## # 7

- a. Your firm has ... bottle packaging lines (e.g., ...), which are used for the commercial packaging of OTC drug products which are distributed to U.S. market. There is no access control for each user of the associated software for ... within these packaging lines. All supervisors use same password to access the software and change product recipes, and all operators uses same password to access the software to run the packaging lines.
- b. Your firm has ... blister packaging lines which are used for commercial packaging of OTC drug products which are distributed to U.S. market. There is no access control system for each user of the associated software of blister packaging lines (SOFTWARE: ...) All supervisors use the same password to access the software and change drug product recipes, and all operators uses same password to run packaging lines.

11

## # 8

- a. There is no system in place to ensure data from the Gas Chromatography (GC) and High Performance Liquid Chromatography (HPLC) systems used to test raw materials, in process, and finished products are complete, accurate, reported and reviewed by your quality assurance department.
- b. The System Administrators for your Gas Chromatography (GC) and High Performance Liquid Chromatography (HPLC) systems perform analyses logged in with their system administrator credentials. Data can be altered or deleted under the system administrator logins.

12

## # 8

- c. Your Quality Control Supervisor stated it is part of his normal laboratory procedure to run a standard with a sample to ensure the sample preparation is correct prior to running the assay.
- d. You have not validated the ... software which is used to generate and store data on your Gas Chromatography (GC) and High Performance Liquid Chromatography (HPLC) systems.

13

## # 9

- The audit trails produced by the HPLC and FT-IR instruments used in analysis of finished packaged drug products lots and incoming bulk drug product lots are not reviewed in a way that would reveal improper retesting of samples. When an analyst submits a completed HPLC sequence or FT-IR spectrum for review, a hard copy of the audit trail data specific to that sequence or spectrum only is submitted along with the test data and results for review by your Chief Scientific Officer (CSO). Your CSO does not verify within the data collection software used in these analyses that all of the audit trail data relating to the testing of a particular sample has been submitted for review along with the final results.

14



## # 10

- Specifically, your firm uses an Excel spreadsheet to track a material inventory.
- a. There are no controls to prevent users from retroactively editing information in the spreadsheet.
- b. There are no audit trails to capture changes in the spreadsheet.
- c. There are no controls to prevent users from deleting information within the spreadsheet or deleting the spreadsheet itself.

15

## # 11

- Specifically, prior to the current inspection, your firm did not perform audit trail reviews of the ... System. SOP ..., "... Site", indicates the ... System is the process historian used to collect and archive data generated from electronic systems in manufacturing.

16

## # 12

- Specifically, laboratory analysts have the ability to delete ... data. The ... computerized system is used to test and release incoming drug components. For example, the ... was used to test and release active pharmaceutical ingredient ..., lot # ..., for the production of..., lot #... Moreover, there is no audit trail control to detect the deletion of data.

17

## # 13

- HPLC machines ... are used in the testing of pharmaceutical drug product. The following were observed:
- a. No access controls for the computer systems HPLC machine (1) and (2) do not have individual assigned sign-on for each analytical chemistry technician or manager using the specified instrument to complete an HPLC run. Within the last (2) years ... tests were conducted on pharmaceutical drug using HPLC (1) or (2). Unique individuals cannot be identified through the login. In addition, several HPLC runs are completed under employees that are no longer with the firm.

18

## # 13

- b. No audit trail for the software used to acquire data used to test pharmaceutical drug product on both HPLC machines.
- c. Data stored on local computer drive using the software: Windows... can be deleted. Additionally, Windows software has a ... user login on both HPLC machines.
- d. No backup of electronic data generated in pharmaceutical drug products.

19

## # 14

- Specifically, the computer systems used to locally store sterility sample results for the firm's ... Instruments allows the addition and deletion of files in the directory used for storage of ... data while logged in under the Windows operating system's shared general laboratory user login.

20

## # 15

- Specifically, the delete functions are enabled for all users assigned to your FTIR Spectroscopy system ... Your firm utilizes FTIR for the identification of ... For example, FTIR spectroscopy was utilized in the release testing of ... Lot #..., that was used in the exhibit batch manufacturing of ....

21

## # 16

- Specifically, your firm utilizes a common user login, that is not password protected for your ..., used to determine ... We also observed that the 21 CFR Part 11 was disabled for the instrument. For example, the ... was utilized in the release testing of ... Lot #..., that was used in the exhibit batch manufacturing of ....

22

## # 17

- Specifically, we observed a quality control employee who performs data review access the ..... software, and noted the user role was defined as an administrator in the system. The firm was unable to provide clarification on his or other user abilities within the software.

23

## # 18

- Specifically, the Quality Assurance Director stated you do not have access to your archived raw data, know what has been backed up or how long the data has been backed up, and if anything is missing.

24

## # 19

- Specifically, the ..... system allows for the deletion of the audit trail on the computers. The audit trail for one of the ..... computers was deleted from one of ..... computer systems. The system has been in use since .....

25

## # 20

- According to the firm's Chief Technology Officer, sterility testing data is supposed to be backed up .....; however, data file backup did not occur for one of the firm's ..... computer systems for a 4-month period. During the time period the backup stopped, approximately ..... sample runs were conducted on the instrument.

26



## # 21

- Specifically, the Quality Assurance Director states that the analyst user role has the capability of creating new methods in the electronic system, and there is no documented review by the quality unit of the methods after they are input into the .... software. These methods are used for raw material, finished product and stability testing for your OTC drug products.

27

## # 22

- Specifically, your firm does not have procedures or protocols in place to validate software used as part of your quality system, and these software systems have not been validated for their intended use. Examples include .... (used for document storage and tracking), .... (used for design control and risk management), .... (used for software development and ticketing), and .... (used for training courses and completion tracking).

28

## # 23

- a. None of the computerized systems in the QC laboratory are tied to a remote server, and data is stored on a local PC associated with each piece of equipment. One single log-in and password for the operating system (OS) of each PC is shared by ..... laboratory employees. Data files are accessible through the OS, where they can be deleted. This includes ..... PCs running ..... chromatographic software for HPLC, ..... PC running ..... chromatographic software for HPLC, and ..... PC running ..... Version ..... for FT-IR. These systems are used for assay and impurity tests of finished OTC drug product and stability samples, as well as raw material identification tests.

29

## # 23

- b. The administrator role for ..... and ..... chromatographic software is not assigned to a specific person but is identified under ..... usernames. Any activities performed under these user accounts are not attributable to any specific person at the firm, and there is no assurance that the passwords are not shared, including among personnel in Quality Assurance or the Quality Control laboratory.
- The failure to exercise appropriate controls over computerized systems is a repeat observation from the previous inspection.

30

## # 24

- a. The Gas Chromatograph used to test your OTC drug products is not programmed where your users are required to have passwords which are specific to them when conducting analysis on these OTC drug products. In addition, there is no audit trail available for tests conducted on your OTC drug products. For example, the copies of the Chromatographs generated for your testing includes the “User” name as ..... and does specify what analyst performed the test.

31

## # 24

- b. The data contained on the Gas Chromatograph is not secured and can be manipulated and deleted.
- c. You do not maintain a backup file of data entered into your Gas Chromatograph, which is used to test your OTC drug products, including raw materials, in-process, finished products and stability testing.

32

## # 25

- Specifically, data collected by ..... and ..... chromatographic software from ..... HPLC units, and from the ..... version ..... software from FT-IR instrument, are all stored on ..... PCs associated with each piece of equipment. The data from each is backed up on a ..... basis, even though the equipment may be used on a ..... or ..... basis. The data stored is susceptible to loss until the ..... backup is created.

33

## # 26

- Specifically, no documentation was available defining the ..... software user roles and their functions for the HPLC system. The Quality Assurance Director stated you rely on a third-party company to set the roles in the ..... system. The Quality Assurance Director, who is also the system Administrator for ....., was unable to log into the system, was unsure how to navigate the software, and had no knowledge of assigned responsibilities of each user role.

34

## # 27

- Electronic documents used by laboratory personnel are not attributable, contemporaneous, or original. Specifically, excel worksheets that are used for calculation and reporting of analytical data have no documentation of who performed or reviewed the calculations. Furthermore, your firm's excel worksheets do not include a date and time stamp to indicate when the data was generated or if any changes occurred to the document after the initial review.

35

## # 28

- a. The firm's HPLC test methods on ..... software allows the users to perform manual integrations on the analyzed data. Several chromatographic peaks from analysis performed on ..... were observed in the system audit trail as being deleted.
- b. A single/trial injection data was observed on the chromatographic software database. A single/trial injection chromatogram was found to have been performed on HPLC Instrument ..... and saved to the "TEST" folder.

36

## # 28

- c. There are no controls in place to restrict the locations on the saved data file. Multiple, non-product specific file folders are available to save analytical data on the .... database, including folders named “TEST” and “R&D.” Each of these folders contained unknown chromatographic data files.

37

## # 29

- Specifically, your firm does not have a procedure for electronic audit trail review of the laboratory instrument software which generates and stores raw analytical data, and there is no documented evidence that electronic audit trail reviews are performed by the Quality Control unit. Additionally, your firm’s Quality Assurance does not perform periodic audit trail reviews of the electronic data generated.

38



## # 30

- Specifically, there are no controls in place to prevent the deletion of raw data from ..... software connected to any workstations (for example HPLC .....). Analysts have administrative privileges within the ..... operating system, and have the capability to delete raw data and manipulate the operating system date and time. Furthermore, a review of audit trails for accuracy is not performed nor documented on a regular basis.

39

## # 31

- Specifically, you do not document the review of electronic data and audit trails stored on HPLC systems or on the UV spectrometer prior to release and reporting of results. While reviewing the HPLC assay of ....., lot ....., in the analytical laboratory, we inquired about whether the audit trail is reviewed. You were unable to provide documentation at that time showing that the audit trail is reviewed.

40

## # 32

- Specifically, the ..... computer system currently in use had not been validated. The computer system is responsible for inventory and product status.

41

## # 33

- Specifically, the warehouse management systems used for the receiving and distribution of raw materials, components and finished drug products, such as ....., and the ..... were not validated for its intended use. There is no assurance that information inputted into the systems are reliable or prevented from deletion or alteration.

42

## # 34

- Specifically, the software validation for the ..... software, Version 3, was inadequate as it only included high level functional testing and did not include documented code reviews, unit testing, or regression testing. Additionally, there are no documented software verifications or validations for the 5 software updates for the ..... released since Version 3. In addition, procedures have not been established for performing code reviews, unit testing, integration testing, or regression testing. The software for the ..... is developed by the firm.

43

## # 35

- Specifically, your firm's main computer system ..... used to monitor inventory, create packing slip orders, transportation documentation records, and document quality related functions is not a validated system. Your main computer system ..... used by all personnel does not have sufficient controls to prevent changes, omissions, and deletion of inventory data. There is also no audit trail functionality when entering data into the system. Furthermore, there are no written procedures available for the use and maintenance for your firm's ..... system.

44

# Questions?