



데이터 완전성에 대한 지침

(2019 년 10 월)

논평을 위한 초고

2020 년 1 월 15 일까지 모든 논평을 그룹 책임자, 의약품 품질 보증, 기술 표준 및 규범, Sabine Kopp 박사(kopps@who.int)에게 보내고, Claire Vogel 씨(vogelc@who.int)에게 사본을 보내야 한다.

작업 문서는 전자적으로 전송되며 WHO Medicines 웹 사이트

(http://www.who.int/medicines/areas/quality_safety/quality_assurance/guidelines/en/)에

“현재 프로젝트(Current projects)” 링크 아래에 논평을 위해 게시되어 있다. 초고 지침을 받으려면 jonessi@who.int 로 이메일 주소를 보내야 한다. 자신의 이름이 이메일 목록에 추가될 것이다.

© 세계 보건 기구 2019

All rights reserved.

이 초고는 제한된 대상, 즉 이 초고를 받은 개인 및 조직을 위한 것이다. 세계 보건기구의 허가가 없는 경우 이 초고는 이러한 개인과 조직(조직의 관련 직원 및 회원 조직 포함) 외부에 의해 어떤 형태나 수단으로든, 부분적으로나 전체적으로 검토, 요약, 인용, 재생산, 전송, 배포, 번역 또는 조정될 수 없다. 어떤 웹사이트에도 이 초고를 전시해서는 안 된다.

허가 요청은 아래로 보내야 한다.

Dr Sabine Kopp, 스위스 제네바 27 CH-1211 세계 보건기구 이메일: kopps@who.int 의약품 품질 보증, 기술 표준 및 규범, 필수 의약품 및 건강 제품부, 그룹 책임자

이 초고에 사용된 명칭과 자료의 제시는, 그것이 국가, 영토, 도시나 지역 또는 당국의 법적 지위에 관한 것이건, 국경 또는 경계의 한정에 관한 것이건 세계 보건기구 측에서 어떤 의견 표명을 한 것은 아니다. 지도의 점선은 아직 완전히 합의되지 않은 대략적인 경계선을 나타낸다.

특정 회사 또는 특정 제조업체의 제품에 대한 언급이, 언급되지 않은 유사한 특성을 가진 다른 회사보다 세계 보건기구(WHO)가 선호하여 보증하거나 권장하는 것을 암시하지는 않는다. 오류 및 누락을 제외하고 독점 제품의 이름은 첫 글자 대문자로 구별된다.

세계 보건기구는 이 초고에 포함된 정보를 확인하기 위해 모든 합리적인 예방 조치를 취했다.

그러나 본 인쇄물은 명시적이든 묵시적이든 어떠한 종류의 보증 없이 배포되고 있다. 자료의 해석 및 사용에 대한 책임은 독자에게 있다. 세계 보건기구는 어떠한 경우에도 사용으로 인해 발생하는 손해에 대해 책임을 지지 않는다.

이 초고가 불가피하게 세계 보건기구의 결정이나 명시된 정책을 나타내는 것은 아니다.

GUIDELINE ON DATA INTEGRITY

(October 2019)

DRAFT FOR COMMENTS

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

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

© World Health Organization 2019

All rights reserved.

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

Please send any request for permission to:

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

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

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

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

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

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

데이터 완전성(DATA INTEGRITY)에 대한 지침

활동 설명	날짜
제 54 차 WHO 제약 제제 규격 전문가 위원회(ECSP - Expert Committee on Specifications for Pharmaceutical Preparations)의 권고에 따른 문서 준비.	2019 년 10 월
국제약전과 제약 제제의 전문가 자문 패널(Expert Advisory Panel on the International Pharmacopoeia and Pharmaceutical Preparations, EAP)을 포함하여 논평을 요청하는 작업 문서를 우편으로 송부, WHO 웹 사이트에 공개 상담을 위한 작업 문서 게시.	2019 년 11 월 – 2020 년 1 월
접수된 논평의 통합 및 피드백 검토. 토론을 위한 작업 문서 준비.	2019 년 3 월
스크리닝 기술, 실험실 도구 및 약전의 의약품 규격에 관한 비공식 상담 중에 받은 작업 문서와 피드백에 대한 토론.	날짜 추후확정
다중 소스 제품의 규제 지침에 대한 비공식 상담 중 받은 작업 문서와 피드백에 대한 토론.	2020 년 5 월 15-16
공개 상담을 위한 다음 번 작업 문서 준비.	2020 년 5 월
접수된 논평의 통합 및 피드백 검토. 토론을 위한 작업 문서 준비.	2020 년 7 월
건강 제품 제조와 검사를 위한 GXP(Good Practice)에 관한 비공식 상담에서 공개 상담 및 상위 회의에서 받은 작업 문서 및 피드백에 대한 토론.	날짜 추후확정
EAP 를 포함하여 개정된 작업 문서에 대한 논평 요청을 우편으로 송부, WHO 웹 사이트에 2 차 공개 상담을 위한 작업 문서 게시.	2020 년 7 월
접수된 논평의 통합 및 피드백 검토. 토론을 위한 작업 문서 준비.	2020 년 9 월말
제 54 차 ECSP 회의 프레젠테이션.	2020 년 10 월 12-16
필요한 기타 후속 조치.	

데이터 완전성(DATA INTEGRITY)에 대한 지침

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

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

데이터 완전성에 대한 지침

1. 소개 및 배경
2. 범위
3. 용어
4. 데이터 완전성 및 GDP(Good Documentation Practice)의 원칙
5. 품질 리스크 관리
6. 관리 검토
7. 아웃소싱
8. 훈련
9. 데이터
10. 데이터 완전성
11. Good Documentation Practice
12. 컴퓨터화된 시스템
13. 시정 및 예방 조치

참고 문헌 및 추가 자료

부록 1: 데이터 완전성 관리의 예

GUIDELINE ON DATA INTEGRITY

1. Introduction and background
2. Scope
3. Glossary
4. Principles of data integrity and good documentation practices
5. Quality risk management
6. Management review
7. Outsourcing
8. Training
9. Data
10. Data integrity
11. Good documentation practices
12. Computerized systems
13. Corrective and preventive actions

References and further reading

Annex 1: Examples of data integrity management

1. 소개 및 배경

1.1 데이터 거버넌스 및 데이터 완전성(Data Integrity)은 제약 제품의 생산 및 관리에서 얻은 데이터와 정보의 신뢰성을 보장하는 데 중요한 요소이다. 데이터와 정보는 일반적으로 "ALCOA" 원칙을 충족한다고 말하는 귀속성(attributable), 가독성(legible), 동시성(contemporaneous), 원본성(original), 정확성(accurate)을 갖추어야 하며, 그에 못지 않게 완전해야 한다.

1.2 최근 몇 년, GMP(Good Manufacturing Practice), GCP(Good Clinical Practice) 및 GLP(Good Laboratory Practice)를 실시하는 동안 데이터, 문서 및 기록 관리 시행의 완전성에 대한 관찰이 증가하고 있다. 이에 대한 가능한 원인에는 다음이 포함된다: (i) 인간의 관습에 너무 의존 (ii) 적절하게 관리되고 검증되지 않은 컴퓨터 시스템의 사용 및 (iii) 원본 데이터와 기록을 적절히 검토 및 관리하지 못하는 경우.

1.3 이러한 위험을 완화하기 위해서는 품질 위험 관리(QRM - Quality Risk Management), 제어 전략 및 건전한 과학적 원칙이 필요하다. 제어 방식의 예로 다음이 포함되지만 이에 국한되지는 않는다.

- 데이터 완전성 정책의 수립 및 시행
- 데이터 완전성 요건과 기대를 용이하게 준수하도록 하는 절차의 수립 및 실행
- 보고 메커니즘을 포함하여 직원이 실패에 투명하도록 장려하는 회사 내 품질 배양 문화 채택
- 데이터 완전성 위험 평가(DIRA - Data Integrity Risk Assessment)를 통해 데이터 완전성에 대한 모든 위험 영역을 식별하여 QRM을 적용, 데이터 생애주기 동안 위험을 수용 가능한 수준으로 제거하거나 줄일 수 있는 적절한 제어 방식 실행
- 데이터 완전성 정책, 절차 및 프로세스 준수를 모니터링하고 지속적인 개선을 촉진시키기에 충분한 자원 확보

1. INTRODUCTION AND BACKGROUND

- 1.1. Data governance and data integrity (DI) are important elements in ensuring the reliability of data and information obtained in production and control of pharmaceutical products. The data and information should be complete as well as being attributable, legible, contemporaneous, original and accurate, commonly referred to as meeting “ALCOA” principles.
- 1.2. In recent years, the number of observations made regarding the integrity of data, documentation and record management practices during inspections of good manufacturing practice (GMP), good clinical practice (GCP) and good laboratory practice (GLP) has been increasing. Possible causes for this may include (i) too much reliance on human practices; (ii) the use of computerized systems that are not appropriately managed and validated; and (iii) failure to adequately review and manage original data and records.
- 1.3. Quality risk management (QRM), control strategies and sound scientific principles are required to mitigate such risks. Examples of controls may include, but are not limited to:
 - the establishment and implementation of a DI policy;
 - the establishment and implementation of procedures that will facilitate compliance with DI requirements and expectations;
 - adoption of a quality culture within the company that encourages personnel to be transparent about failures which includes a reporting mechanism;
 - application of QRM with identification of all areas of risk to DI through data integrity risk assessment (DIRA) and implementation of appropriate controls to eliminate or reduce risks to an acceptable level throughout the life cycle of the data;
 - ensuring sufficient resources to monitor compliance with DI policies and procedures and processes, and facilitate continuous improvement;

- 인력에 필요한 훈련 제공; 예를 들어 컴퓨터화 시스템 및 데이터 완전성 등을 위한 GXP(Good Practices).
- 의도된 용도에 적합한 컴퓨터 시스템 실현 및 검증
- 계약 제시자와 계약 수용자가 체결한 품질 협약 및 계약에 대한 적절한 역할 및 책임 정의 및 관리

2. 범위

2.1 이 지침은 문서와 기록 유지 요구 사항에 데이터 완전성, GXP 를 손쉽게 준수할 수 있도록 정보, 지침 및 권장 사항을 제공한다.

2.2 이 지침의 범위는 'GXP'로 지정된다. 그러나 의료 기구에는 적용되지 않는다.

2.3 가능한 경우 이 지침은 출판된 다른 문서에 맞게 조율되었다. 본 지침은 다른 WHO GXP 지침 및 출판물과 함께 읽어야 한다.

2.4 GMP 의 현재 접근 방식에 따라 데이터 생애주기 동안 위험 기반 접근 방식을 권장한다. 위험 영역을 식별하고 평가하기 위해 DIRA 를 수행해야 한다.

2.5 이 지침의 원칙은 계약 제시자 및 계약 수용자에게 적용된다. 계약 제시자는 궁극적으로 계약 수용자가 그들에게 제공한 데이터 완전성에 대한 책임이 있다. 따라서 계약 제시자는 계약 수용자가 이 지침에 포함된 원칙을 준수하도록 해야 한다.

2.6 효율적인 위험 기반 제어 방식과 데이터 및 문서 검토가 식별 및 실현되어야 한다. 제어 방식의 효율성은 검증되어야 한다.

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

2. SCOPE

- 2.1. This guideline provides information, guidance and recommendations to facilitate compliance with DI, GXP in documentation and record keeping requirements.
- 2.2. The scope of this guideline is designated as 'GXP'. It does not, however, cover medical devices.
- 2.3. Where possible, this guideline has been harmonised with other published documents. The guideline should be read with other WHO GXP guidelines and publications.
- 2.4. In line with the current approach in GMP, it recommends a risk-based approach over the life cycle of data. DIRA should be carried out in order to identify and assess areas of risk.
- 2.5. The principles of this guideline apply to contract givers and contract acceptors. Contract givers are ultimately responsible for the integrity of data provided to them by contract acceptors. Contract givers should therefore ensure that contract acceptors comply with the principles contained in this guideline.
- 2.6. Efficient risk-based controls and review of data and documents should be identified and implemented. The effectiveness of the controls should be verified.

3. 용어 사전

(참고: 이 섹션은 업데이트될 예정입니다)

아래의 정의는 이 지침에서 사용된 용어에 적용된다. 맥락에 따라 다른 의미를 가질 수 있다.

ALCOA

"귀속성(attributable), 가독성(legible), 동시성(contemporaneous), 원본성(original), 정확성(accurate)"의 약어로 보통 사용된다.

ALCOA +

"귀속성(attributable), 가독성(legible), 동시성(contemporaneous), 원본성(original), 정확성(accurate)"의 약어로 보통 사용된다. 여기에 완전성, 일관성, 영구성, 그리고 가용성을 추가적으로 강조한 것이다. ALCOA 원칙에 기본적으로 암시되어 있다.

보관/아카이빙 (archiving, archival)

보관/아카이빙은 필요한 보존 기간 동안 독립적인 데이터 관리 담당자의 제어 하에 기록에 액세스하고 추가로 변경하거나 삭제할 수 없도록 기록을 저장하고 보호하는 프로세스이다. 보관된 기록에는 예를 들어 관련 메타 데이터 및 전자 서명이 포함되어야 한다.

보관 관리인 (archivist)

GLP 에 지정된 독립적인 개인으로서 경영진이 보관소 관리에 대한 책임을, 즉 보관 작업 및 절차를 담당할 권한을 부여하였다.

점검기록 (audit trail)

점검기록은 GXP 기록의 생성, 수정 또는 삭제와 관련한 작업과 그에 관련된 정보가 포함된 메타 데이터 형식이다. 점검기록은 원본 기록을 가리거나 덮어쓰지 않고, 종이 또는 전자 기록으로 기록 내의 정보 생성, 추가, 삭제 또는 변경과 같은 생애주기 세부 사항을 안전하게 기록한다.

3. GLOSSARY

(Note: This section will be updated)

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

ALCOA.

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

ALCOA+.

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

archiving, archival.

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

archivist.

An independent individual designated in GLP who has been authorized by management to be responsible for the management of the archive, i.e. for the operations and procedures for archiving.

audit trail.

The audit trail is a form of metadata containing information associated with actions that relate to the creation, modification or deletion of GXP records. An audit trail provides for secure recording of life cycle details such as creation, additions, deletions or alterations of information in a record, either paper or electronic, without obscuring or overwriting the original record. An

점검기록은 작업의 "누가, 무엇을, 언제, 왜"를 포함하여, 매체와 상관없이 기록과 관련된 이러한 이벤트 히스토리를 재구성하기 쉽게 한다.

데이터 거버넌스 (data governance)

데이터가 생성된 형식에 관계없이 데이터가 기록, 프로세스, 유지 및 사용되어 데이터 생애주기 내내 그 기록을 보장하도록 정리하는 것

데이터 생애주기 (data life cycle)

데이터가 폐기될 때까지 생성, 기록, 처리, 수정, 전송, 검토, 보고, 사용, 승인, 보관 및 복구되는 프로세스의 모든 단계

전자 서명 (electronic signatures)

서명인을 나타내는 디지털 형식(바이오메트릭 또는 비-바이오메트릭)의 서명. 이것은 법적인 측면에서 서명인의 자필 서명과 동일하다.

GXP (Good Practices)

GLP, GCP, GMP, GPP(Good Pharmacovigilance Practice) 및 GDP(Good Distribution Practice)와 같은 규제관리 대상 의약품, 생물학적 제제 및 의료기기에 대한 전임상, 임상, 제조, 시험, 저장, 유통 및 사후 시장 활동을 지배하는, GXP(Good Practice) 지침 집합을 통칭하는 약어.

메타 데이터 (metadata)

메타 데이터는 다른 데이터의 속성을 설명하고 맥락과 의미를 제공하며 원본 기록의 필수 부분을 구성하는 데이터이다. 점검기록 기록은 메타 데이터의 한 예이다.

원본데이터(소스 데이터) raw data (source data)

종이나 전자적으로 기록된 정보의 첫 번째 캡처라고 설명할 수 있는 원본 기록(데이터)

일상적 데이터 검토 (routine data review)

audit trail facilitates the reconstruction of the history of such events relating to the record regardless of its medium, including the “who, what, when and why” of the action.

data governance.

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

data life cycle.

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

electronic signatures.

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

good practices (GXP).

Acronym for the group of good practice guides governing the preclinical, clinical, manufacturing, testing, storage, distribution and post-market activities for regulated pharmaceuticals, biologicals and medical devices, such as GLP, GCP, GMP, good pharmacovigilance practices (GPP) and good distribution practices (GDP).

metadata.

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

raw data (source data).

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

routine data review.

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

일상적 데이터 검토는 개별 데이터 세트의 완전성을 위해 원본데이터 및 메타 데이터를 검토하는 프로세스이다.

정기적 데이터 검토 (periodic data review)

정기적 데이터 검토는 생성된 데이터의 감사가 주기적으로(예: 월간) 수행되는 프로세서이며, 기존 제어 조치의 효과 및 모든 인터페이스상의 무단 활동 가능성 확인을 검증하기 위해 무작위로 데이터가 선택되는 프로세스이다.

4. 데이터 완전성 및 GDP(GOOD DOCUMENTATION PRACTICE)의 원칙

4.1 서면으로 된 데이터 완전성 정책이 있어야 한다.

4.2 고위 경영진은 효과적인 품질 시스템과 데이터 거버넌스 시스템의 구축 및 실행을 책임진다. 이것은 종이 및 전자 생성 데이터에 적용된다.

4.3 데이터는 귀속성, 가독성, 동시성, 원본성, 정확성의 ALCOA 이 있어야 하며, 완전성, 일관성, 지속성, 가용성(available)(+) 또한 있어야 한다. 이를 일반적으로 ALCOA +라고 한다(어떤 약어가 사용되는지에 관계없이 기대치에는 차이가 없다).

4.4 품질 시스템은 데이터 기록 절차 및 형식과 같은 문서를 포함하며, 기록과 데이터가 이 지침에 포함된 원칙을 충족하도록 보장하기 위해 적절하게 설계 및 실행되어야 한다.

4.5 데이터 거버넌스는 생애주기 내내 데이터 소유권 및 책임을 다루고, 의도하거나 의도하지 않은 데이터 변화에 대한 제어방식을 포함하여 데이터 완전성 원리를 준수하기 위한 프로세스/시스템의 설계, 운영 및 모니터링을 고려해야 한다.

4.6 데이터 거버넌스 시스템에는 다음이 포함되어야 한다.

- 데이터 완전성 원칙의 중요성에 대한 훈련

periodic data review.

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

4. PRINCIPLES OF DATA INTEGRITY AND GOOD DOCUMENTATION PRACTICES

- 4.1. There should be a written DI policy.
- 4.2. Senior management is responsible for the establishment and implementation of an effective quality system and a data governance system. This applies to paper and electronic generated data.
- 4.3. Data should be Attributable, Legible, Contemporaneous, Original, and Accurate (ALCOA) and be Complete, Consistent, Enduring, and Available (+). This is generally referred to as ALCOA+. (There is no difference in expectations regardless of which acronym is used).
- 4.4. The quality system, including documentation such as procedures and formats for recording data, should be appropriately designed and implemented to provide assurance that records and data meet the principles contained in this guideline.
- 4.5. Data governance should address data ownership and accountability throughout the life cycle and consider the design, operation and monitoring of processes/systems to comply with the principles of DI, including control over intentional and unintentional changes to data.
- 4.6. Data governance systems should include:
 - training in the importance of DI principles;

- 적절한 작업 환경 조성
- 오류, 누락 및 바람직하지 않은 결과에 대한 보고를 적극적으로 장려한다.

4.7 고위 경영진은 데이터 완전성에 대한 잠재적 위험을 최소화하고, 국제의약품규제조화위원회 (ICH - International Conference on Harmonization) Q9 의 원칙과 같은 위험 관리 기술을 사용하여 잔류 위험을 식별하기 위해, 시스템과 절차의 실현에 대해 책임을 져야 한다.

4.8 데이터 거버넌스 프로그램에는 데이터 관리를 다루는 정책 및 절차가 포함되어야 한다. 효과적인 관리 거버넌스 요소에는 다음이 포함되어야 한다.

- 관리 감독 및 헌신
- QRM의 적용
- 바른 데이터 관리 원칙
- 품질 지표 및 성과 지표
- 밸리데이션
- 변경 관리
- 보안 및 액세스 제어
- 구성 제어
- 상업적, 정치적, 재정적 및 기타 조직적 압력 방지
- 업무의 질과 완전성에 악영향을 줄 수 있는 인센티브 예방
- 적절한 자원, 시스템
- 데이터 완전성과 효과적인 제어 방식을 지원하기에 맞는 환경을 원활하게 하는
작업량 및 시설
- 모니터링
- 기록 아카이빙
- 훈련
- 데이터 완전성, 제품 품질 및 환자 안전의 중요성에 대한 인식

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

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

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

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

4.9 데이터 완전성 오류를 식별하기 위해 문서와 데이터를 정기적으로 검토할 수 있는 시스템이 있어야 한다. 여기에는 일상 업무에서 나온 종이 기록과 전자 기록, 시스템과 시설 감사 및 자체 검사를 포함된다.

4.10 데이터의 완전성을 보장하기 위해 적용되는 노력과 자원은 데이터 완전성 오류의 위험과 영향에 상응해야 한다.

4.11 데이터 완전성 약점을 식별한 경우 적절한 시정 및 예방 조치(CAPA - Corrective And Preventive Action)를 관련 활동 및 시스템, 그리고 별개로 있지 않은 모든 사항에 걸쳐 실현해야 한다.

4.12 확인된 중요한 데이터 완전성 과실은 국가 의약 규제 당국에 보고해야 한다.

4.13 자동화 또는 컴퓨터화된 시스템에서 종이 기반 수동 시스템으로 또는 그 반대로 변경해도 자체적으로 적절한 데이터 완전성 제어 방식에 대한 요구를 삭제하는 것은 아니다.

4.14 모든 기록이 완료되도록 GDP(Good Documentation Practice)를 따라야 한다.

4.15 이 지침의 원칙을 준수할 수 있도록 기록(종이 및 전자)을 보관해야 한다. 여기에는 다음이 포함되지만 이에 국한되지는 않는다.

- 이벤트 기록을 위한 날짜 및 시간 변경 기능을 제한
- GXP 데이터의 기록용으로 제작된 문서 및 양식을 사용
- GXP 활동의 데이터 기록시에 백지 견본 발행을 제어하고 회수하는 것
- 자동화 시스템에 대한 액세스 및 특권을 정의
- 점검기록 활성화
- 가능한 경우 생산 및 품질 관리에서 장비 및 기기에 연결된 자동화 데이터 캡처 시스템 및 프린터 구비
- 관련 활동 장소에 프린터를 가까이 배치

- 4.9. There should be a system for the regular review of documents and data to identify any DI failures. This includes paper records and electronic records in day-to-day work, system and facility audits and self-inspections.
- 4.10. The effort and resources applied to assure the integrity of the data should be commensurate with the risk and impact of a DI failure.
- 4.11. Where DI weaknesses are identified, appropriate corrective and preventive actions (CAPA) should be implemented across all relevant activities and systems and not in isolation.
- 4.12. Significant DI lapses identified should be reported to the national medicine regulatory authority.
- 4.13. Changing from automated or computerised systems to paper-based manual systems or vice-versa will not in itself remove the need for appropriate DI controls.
- 4.14. Good documentation practices should be followed to ensure that all records are complete.
- 4.15. Records (paper and electronic) should be kept in a manner that ensures compliance with the principles of this guideline. These include, but are not limited to:
- restricting the ability to change dates and times for recording events;
 - using controlled documents and forms for recording GXP data;
 - controlling the issuance of blank paper templates for data recording of GXP activities, with reconciliation;
 - defining access and privilege rights to automated systems;
 - enabling audit trails;
 - having automated data capture systems and printers connected to equipment and instruments in production and quality control where possible;
 - ensuring proximity of printers to sites of relevant activities; and

- 데이터 검토 및 확인을 담당하는 직원이 원본 전자 데이터에 액세스할 수 있도록 한다.

4.16 데이터와 기록 매체는 내구성이 있어야 한다. 잉크는 지워지지 않아야 한다. 온도에 민감하거나 감광성 잉크 및 기타 지울 수 있는 잉크를 사용하지 않아야 하며, 생애주기 동안 데이터의 추적성을 보장하기 위한 방법을 확인해야 한다.

4.17 용지는 온도에 민감하거나 감광성이 있거나 쉽게 산화되지 않아야 한다. 이것이 가능하지 않거나 제한적인 경우, 진본 또는 인증된 사본을 사용할 수 있어야 한다.

4.18 데이터를 기록하고 저장하는 데 사용되는 시스템, 절차 및 방법론을 정기적으로 검토하여 효율성을 확인하고, 필요에 따라 새로운 기술과 관련하여 업데이트해야 한다.

5. 품질 리스크 관리

5.1 DIRA 를 문서화해야 한다. DIRA 는 데이터를 생성하거나 획득한 경우, 데이터 중요도 및 내재된 위험이 포함된 시스템 및 프로세스를 관장해야 한다.

5.2 위험 평가에는 컴퓨터 시스템, 지원 인력, 훈련 및 품질 시스템 등이 포함되어야 한다.

5.3 문서 및 데이터의 생애주기 동안 기록과 데이터 완전성의 위험을 평가, 완화, 전달 및 검토해야 한다.

5.4 DIRA 의 교정 (remediation) 부분에서는 조치의 우선 순위(적절한 수준의 잔여 위험 수용 포함)와 제어 방식을 문서화하고 전달하는 과정이 강조되어 있어야 한다. 장기적인 교정 조치가 확인되는 경우, 위험을 줄이는 단기 조치를 실행하여 중간에 수용 가능한 데이터 거버넌스를 제공해야 한다.

- ensuring access to original electronic data for personnel responsible for reviewing and checking data.
- 4.16. Data and recorded media should be durable. Ink should be indelible. Temperature-sensitive or photosensitive inks and other erasable inks should not be used, or other means should be identified to ensure traceability of the data over their life cycle.
- 4.17. Paper should not be temperature-sensitive, photosensitive or easily oxidizable. If this is not feasible or limited, then true or certified copies should be available.
- 4.18. Systems, procedures and methodology used to record and store data should be periodically reviewed for effectiveness and updated, as necessary, in relation to new technology.

5. QUALITY RISK MANAGEMENT

- 5.1. The DIRA should be documented. This should cover systems and processes that produce data or, where data are obtained, data criticality and inherent risks.
- 5.2. The risk assessment should include, for example, computerised systems, supporting personnel, training and quality systems.
- 5.3. Record and DI risks should be assessed, mitigated, communicated and reviewed throughout the document and data life cycle.
- 5.4. Where the DIRA has highlighted areas for remediation, prioritisation of actions (including acceptance of an appropriate level of residual risk) and controls should be documented and communicated. Where long-term remediation actions are identified, risk-reducing short-term measures should be implemented to provide acceptable data governance in the interim.

5.5 확인된 제어 방식에는 절차, 프로세스, 장비, 도구 및 기타 시스템과 같은 조직 및 기능 제어 방식이 포함되어 데이터 완전성에 영향을 줄 수 있는 상황을 방지하고 탐지할 수 있다(예를 들면 적절한 내용과 절차 설계, 기록 형식, 액세스 제어, 컴퓨터 시스템 사용 및 기타 수단이 포함된다).

5.6 제어 방식은 데이터에 대한 위험을 망라하여야 한다.. 위험에는 활동 및 이벤트에 대한 서면 승인 및 탐지 없이 데이터 및 데이터 세트의 결과를 삭제, 변경 및 제외하는 것이 포함된다.

6. 관리 검토

6.1 데이터 완전성 정책 및 절차의 준수는 정기적인 경영 검토 회의에서 보고되어야 한다.

6.2 실현된 제어 방식의 효과는 품질 지표 및 성과 지표와 비교하여 측정되어야 한다. 예를 들면 다음과 같다.

- 데이터의 추적 및 추세
- 데이터 완전성 발생율의 결손 발생
- 생산, 품질 관리, GLP, 사례 보고서 양식 및 데이터 처리 등의 업무에 시행된 점검 기록결과에 대한 검토
- 데이터 완전성 및 컴퓨터 시스템을 포함한 부분에서의 정기 감사 그리고/또는 자체 감사
- 외주 시설(계약 수용자)에서 발생한 데이터 완전성의 결손

7. 아웃소싱

7.1 각 당사자(계약 제시자 및 계약 수용자)의 활동 및 책임 아웃소싱은 서면 계약으로 명확하게 기술되어야 한다. 데이터 완전성 요구 사항을 준수할 수 있도록 특별한 주의를 기울여야 한다.

- 5.5. Controls identified may include organizational and functional controls such as procedures, processes, equipment, instruments and other systems to both prevent and detect situations that may impact on DI. (Examples include appropriate content and design of procedures, formats for recording, access control, the use of computerized systems and other means).
- 5.6. Controls should cover risks to data. Risks include deletion of, changes to, and excluding data and results from data sets without written authorisation and detection of those activities and events.

6. MANAGEMENT REVIEW

- 6.1. Compliance with DI policy and procedures should be reported in the periodic management review meetings.
- 6.2. The effectiveness of the controls implemented should be measured against the quality metrics and performance indicators. These should include for example:
- The tracking and trending of data;
 - lapse in DI rates;
 - review of audit trails in, for example, production, quality control, GLP, case report forms and data processing;
 - routine audits and/or self-inspections including DI and computerized systems; and
 - DI lapses at outsourced facilities (contract acceptors).

7. OUTSOURCING

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

7.2 정기적인 현장 감사 기간 동안 원칙과 책임의 준수 여부를 확인해야 한다. 여기에는 계약 제시자의 제품 또는 서비스와 관련되어 계약된 조직이 보유한 절차 및 데이터(원본데이터 및 메타 데이터, 종이 기록, 전자 데이터, 점검기록 및 기타 관련 데이터 포함)에 대한 검토가 포함되어야 한다.

7.3 데이터 및 문서 보존이 제 3 자와 계약되는 경우, 해당 계약에 따라 보존된 데이터의 소유권 및 검색을 이해하는 데 특별한 주의를 기울여야 한다. 그 뿐 아니라 생애주기 동안 데이터의 완전성을 보장하기 위한 제어 방식에도 특별한 주의를 기울여야 한다.

7.4 계약 제시자의 사전 승인 없이 아웃소싱 데이터베이스를 포함한 어떠한 활동도 제 3 자와 하청 계약해서는 안 된다.

7.5 모든 계약 당사자는 데이터 거버넌스, 데이터 완전성 및 데이터 관리와 관련된 요구 사항을 알고 있어야 한다.

8. 훈련

8.1 직원은 데이터 완전성 정책 및 절차에 대한 훈련을 받아야 한다.

8.2 직원은 데이터 완전성 원칙을 준수하기로 동의해야 하며, 위반 시 발생할 수 있는 결과에 대해 알고 있어야 한다.

8.3 데이터 완전성 문제를 예방하고 탐지하기 위한 GDP 및 조치에 대해 직원을 훈련해야 한다. 이를 위해서는 데이터 생성, 처리 및 보고에 사용되는 개별 컴퓨터 시스템에 대한 구성 설정을 평가하고, 점검기록과 같은 전자 데이터 및 메타 데이터를 검토하는 것에 대한 특정한 훈련이 필요할 수 있다.

9. 데이터

- 7.2. Compliance with the principles and responsibilities should be verified during periodic site audits. This should include the review of procedures and data (including raw data and metadata, paper records, electronic data, audit trails and other related data) held by the contracted organization that are relevant to the contract giver's product or services.
- 7.3. Where data and document retention are contracted to a third party, particular attention should be paid to understanding the ownership and retrieval of data held under that agreement, as well as controls to ensure the integrity of data over their life cycle.
- 7.4. No activity, including outsourcing databases, should be sub-contracted to a third party without the prior approval of the contract giver.
- 7.5. All contracted parties should be aware of the requirements relating to data governance, DI and data management.

8. TRAINING

- 8.1. Personnel should be trained in DI policies and procedures.
- 8.2. Personnel should agree to abide by DI principles and should be made aware of the potential consequences in cases of non-compliance.
- 8.3. Personnel should be trained in good documentation practices and measures to prevent and detect DI issues. This may require specific training in evaluating the configuration settings and reviewing electronic data and metadata, such as audit trails, for individual computerized systems used in the generation, processing and reporting of data.

9. DATA

- 9.1. Data may be presented by manually recording an observation, result or other data and information on paper, or electronically recording thereof, by using equipment and

9.1 데이터는 컴퓨터화된 시스템에 링크된 것을 포함하는 장비 및 기구를 사용하여, 관찰, 결과 또는 다른 데이터 및 정보를 종이에 수동으로 기록하거나 전자적으로 기록함으로써 나올 수 있다. 또는 수동과 전자 시스템의 조합이 사용될 수도 있다.

9.2 데이터 완전성은 사진, 비디오, DVD, 이미지 및 크로마토그래피 판과 같은 종류의 데이터에도 동일하게 적용된다. 이와 함께 복사, 사진 또는 디지털화와 같은 해당 형식에 필요한 추가 제어 방식에 적용된다. 그러한 방법의 선택에 대한 문서화된 근거가 있어야 한다.

9.3 가능한 경우, 위험 축소 감독 조치를 실행해야 한다.

9.4 DIRA 또는 다른 요구 사항에서 필요하다고 판단되는 경우 결과 및 데이터 세트에 대하여 독립적인 검증이 필요하다.

10. 데이터 완전성

10.1 데이터 완전성(DI)은 데이터가 완전하고 일관성 있고 정확하며 신뢰할 수 있고 확실한 수준을 말한다.

10.2 위험 기반 시스템 설계 및 제어 방식은 데이터 생애주기 동안 결과 및 데이터의 오류, 과실 및 누락을 탐지할 수 있어야 한다. 제어 방식에는 절차적 제어, 조직적 제어 및 기능적 제어가 포함될 수 있다.

10.3 데이터 완전성 정책은 원본데이터, 소스 데이터, 메타 데이터 및 "완전한 데이터 세트"를 구성하는 요소를 명확하게 정의해야 한다.

10.4 데이터는 동시에 안전한 방식으로 기록, 수집 및 유지되어야 한다. 제어 방식은 귀속성, 가독성, 원본성 (또는 실제 사본), 정확성을 갖고 있는지 확인해야 한다. 데이터 완전성을 보장하려면 건전한 과학적 원칙 준수 및 GDP(Good Documentation Practice)를 포함한 적절한 QRM 시스템이 필요하다.

instruments including those linked to computerised systems. A combination of manual and electronic systems may also be used.

- 9.2. The same considerations for DI apply for other data sets (such as photographs, videos, DVD, imagery and chromatography plates) as for the other data sets, together with any additional controls required for that format such as copying, photography or digitisation. There should be a documented rationale for the selection of such a method.
- 9.3. Where possible, risk-reducing supervisory measures should be implemented.
- 9.4. Results and data sets require independent verification if deemed necessary from the DIRA or by another requirement.

10. DATA INTEGRITY

- 10.1. Data integrity (DI) is the degree to which data are complete, consistent, accurate, trustworthy and reliable.
- 10.2. Risk-based system design and controls should enable the detection of errors, lapses and omissions of results and data during the data life cycle. Controls may include procedural controls, organizational controls and functional controls.
- 10.3. The DI policy should clearly define what constitutes raw data, source data, metadata and a “complete data set”.
- 10.4. Data should be contemporaneously recorded, collected and maintained in a secure manner. Controls should ensure that they are attributable, legible, original (or a true copy) and accurate. Assuring DI requires appropriate QRM systems, including adherence to sound scientific principles and good documentation practices.

10.5 수집, 처리 및 보고된 모든 데이터가 이 지침의 원칙을 준수하도록 시스템을 구축하고 실현해야 한다. 데이터는 다음과 같아야 한다.

- A = 데이터를 생성 한 사람에게 귀속됨
- L = 읽기 쉽고 영구적임
- C = 동시적임
- O = 원본성 (또는 인증된 실제 사본)
- A = 정확함

10.6 데이터 거버넌스 조치는 생애주기 내내 데이터가 완전하고 일관되며 지속적이며 사용 가능해야 한다.

- 완전성 = 데이터가 총체적이어야 한다. 즉 완전한 세트
- 일관성 = 데이터는 자체적 일관성이 있어야 한다.
- 지속성 = 지속적. 데이터 생애주기에 걸쳐 지속된다.
- 가용성 = 검토 또는 검사 목적으로 즉시 사용 가능하다.

10.7 기록 보존 기간 동안 원본 데이터를 검토, 유지, 완료, 지속할 수 있으며 쉽게 복구하고 읽을 수 있어야 한다.

11. GDP(GOOD DOCUMENTATION PRACTICE)

11.1 이 지침에 포함된 원칙은 종이 및 전자 데이터에 적용된다.

11.2 종이에 기록된 데이터 및 결과의 완전성을 보장하기 위해 DIRA 를 통한 특정 제어 방식이 확인되어야 한다. 여기에는 다음이 포함되지만 이에 국한되지는 않는다.

- 영구적이고 지워지지 않는 잉크 사용
- 연필이나 지우개를 사용하지 않음

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

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

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

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

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

11. GOOD DOCUMENTATION PRACTICES

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

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

- the use of permanent, indelible ink;
- no use of pencil or erasers;
- the use of single-line cross-outs to record changes with name, date and reason recorded (i.e. the paper equivalent to the audit trail);

- 이름, 날짜 및 기록된 이유(즉, 점검기록과 동등한 논문)에 대한 변경 사항을 기록하기 위해 한 줄 줄긋기 사용
- 수정액을 사용하지 않거나 기록이 모호하지 않아야 함
- 바인딩된 페이지 매김 노트북의 통제된 발행
- 순차적으로 번호가 매겨진 빈 양식 사본의 통제된 발행
- 안전하고 통제된 기록 보관소에서 독립적이고 지정된 직원이 종이 기록을 보관

12. 컴퓨터화된 시스템

(참고: 이 섹션에서는 컴퓨터 시스템 사용과 관련된 특정 측면을 강조한다. 컴퓨터 시스템에 대한 WHO 가이드 라인, 검증에 대한 WHO 가이드 라인 및 우수 크로마토그래피 기준에 대한 WHO 가이드 라인과 같은 다른 WHO 가이드 라인에 제시된 정보를 반복할 의도는 없다. 참고문헌을 확인할 것)

12.1 선택한 컴퓨터 시스템은 의도된 용도에 적합해야 한다.

12.2 GXP 시스템이 데이터를 수집, 기록, 저장 또는 처리하는 데 사용되는 경우, 경영진은 시스템 및 사용자가 데이터에 미칠 수 있는 위험에 대한 적절한 지식을 가지고 있어야 한다.

12.3 컴퓨터 시스템을 갖춘 기기 및 장비가 사용되는 경우 적절하게 설정되고 검증된 소프트웨어를 사용해야 한다. 데이터 생애주기 동안 데이터 조작 가능성을 제거해야 한다.

12.4 설정 가능한 소프트웨어가 없고 전자 데이터 보존이 없는 전자 시스템(예: pH 측정기, 저울 및 온도계)이 사용되는 경우, 데이터 조작을 방지하고 원하는 결과를 얻기 위해 테스트를 반복하는 제어 방식을 갖추어야 한다.

12.5 데이터 완전성 원칙의 과실에 대한 적절한 탐지 수단이 마련되어야 한다. 푸리에 변환 적외선 분광기 488(FTIR) 및 UV 분광 광도계와 같이 사용자 487 구성이 가능한 출력을 가진 독립형 시스템의 경우, 추가 수단을 실현해야 한다.

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

12. COMPUTERIZED SYSTEMS

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

- 12.1. The computerized system selected should be suitable for its intended use.
- 12.2. Where GXP systems are used to acquire, record, store or process data, management should have appropriate knowledge of the risks that the system and users may have on the data.
- 12.3. Suitably configured and validated software should be used where instruments and equipment with computerised systems are used. The potential for manipulation of data should be eliminated during the data life cycle.
- 12.4. Where electronic systems with no configurable software and no electronic data retention (e.g. pH meters, balances and thermometers) are used, controls should be put in place to prevent manipulation of data and repeat testing to achieve the desired result.
- 12.5. Appropriate means of detection for lapses in DI principles should be in place. Additional means should be implemented where stand-alone systems with a user-configurable output is used, for example, Fourier-transform infrared spectroscopy (FTIR) and UV spectrophotometers.

12.6 데이터 세트로 정의된 모든 기록을 검토하고 유지해야 한다. 검토유지의 노력 및/또는 빈도의 감소를 시도하는 경우 적절함이 설명되어야 한다.

액세스 및 권한

12.7 컴퓨터 시스템 사용자의 액세스 및 권한을 정의하는 문서화된 시스템이 있어야 한다. 종이 및 전자 기록은 사용자의 생성 및 삭제를 포함한 전자 정보와 일치해야 한다.

12.8 액세스 및 권한은 데이터 완전성(예: 응용 프로그램 외부에서 데이터를 수정, 삭제 또는 생성할 수 없음)을 보장하기 위해 적절한 제어 방식을 가진 개인의 책임과 기능에 따라야 한다.

12.9 데이터에 대한 이해 상충이 없는 제한된 직원만 시스템 관리자로 임명되어야 한다. 데이터 삭제, 데이터베이스 수정 또는 시스템 구성 변경과 같은 특정 권한은 정당화 없이 관리자에게 할당해서는 안 되며, 이러한 활동은 다른 책임자에 의해 문서화된 승인 증거로만 수행되어야 한다. 기록은 유지되어야 한다.

12.10 고유한 사용자 이름과 비밀번호가 시스템에서 사용되어야 한다.

12.11 프로그램 및 방법(예: 획득 및 프로세싱 방법)은 데이터가 ALCOA 원칙을 충족하는지 확인해야 한다. 결과 또는 데이터를 획득 방법과 다른 방법/파라미터를 사용하여 프로세스하는 경우 기록해야 한다. 점검기록 및 세부 사항은 모든 데이터 프로세싱 활동의 재구성을 허용해야 한다.

12.12 데이터 전송으로 인해 데이터의 내용이나 의미가 변경되어서는 안 된다. 전송은 점검기록에서 추적되어야 한다.

12.13 데이터 전송은 검증되어야 한다.

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

Access and privileges

- 12.7. There should be a documented system in place that defines the access and privileges of users of computerized systems. The paper and electronic records should be in line with the electronic information including the creation and deletion of users.
- 12.8. Access and privileges should be in accordance with the responsibility and functionality of the individual with appropriate controls to ensure DI (e.g. no modification, deletion or creation of data outside the application is possible).
- 12.9. A limited number of personnel, with no conflict of interest in data, should be appointed as system administrators. Certain privileges such as data deletion, database amendment or system configuration changes should not be assigned to administrators without justification - and such activities should only be done with documented evidence of authorization by another responsible person. Records should be maintained.
- 12.10. Unique usernames and passwords should be used for systems as appropriate.
- 12.11. Programmes and methods (such as acquisition and processing methods) should ensure that data meet ALCOA principles. Where results or data are processed using a different method/parameters than the acquisition method should be recorded. Audit trails and details should allow reconstruction of all data processing activities.
- 12.12. Data transfer should not result in any changes to the content or meaning of the data. The transfer should be tracked in the audit trail.
- 12.13. Data transfer should be validated.

점검기록 (AUDIT TRAIL)

12.14 GXP 시스템은 점검기록의 내용을 보존할 수 있어야 한다. 점검기록에는 예를 들어 사용자, 날짜, 시간, 원본 데이터 및 결과, 변경 및 변경 사유가 반영되어야 한다.

12.15 소프트웨어가 설치될 때 점검기록이 사용 가능해야 하며, 항상 사용 가능한 상태여야 한다. 데이터 생애주기 동안 활성화 및 검증 증거를 유지해야 한다.

12.16 애드온(add-on) 소프트웨어 또는 구형 컴퓨터 시스템이 사용되는 경우(점검기록 없음), 한정된 임시 기간 동안 완화 조치를 취할 수 있다. 한정된 타임라인 안에 해결해야 한다.

12.17 일상적 데이터 검토에는 점검기록에 대한 검토가 포함되어야 한다. 증거는 보관유지되어야 한다.

전자 서명

12.18 모든 전자 서명은 적절하게 통제되어야 한다. 전자 서명은 다음과 같아야 한다.

- 검증됨
- 개인에게 귀속됨
- 변경과 조작의 우려가 없음
- 국제 표준의 요구 사항을 준수

12.19 문서에 전자 서명이 되었음을 표시하는 서명 또는 각주의 삽입된 이미지는 적절하지 않다.

Audit Trail

- 12.14. GXP systems should provide for the retention of audit trails. Audit trails should reflect, for example, users, dates, times, original data and results, changes and reasons for changes.
- 12.15. Audit trails should be enabled when software is installed, and remain enabled all times. Proof of enabling and verification during the life cycle of data should be maintained.
- 12.16. Where add-on software or legacy systems are used (with no audit trail), mitigation measures may be taken for defined temporary periods. This should be addressed within defined timelines.
- 12.17. Routine data review should include a review of audit trails. Evidence should be maintained.

Electronic signatures

- 12.18. Each electronic signature should be appropriately controlled. An electronic signature should be:
- validated;
 - attributable to an individual;
 - free from alteration and manipulation; and
 - compliant with the requirements of international standards.
- 12.19. An inserted image of a signature or a footnote indicating that the document has been electronically signed is not adequate.

데이터 검토 및 승인

12.20 데이터 승인 뿐만 아니라 일상적이고 정기적인 검토를 위해 문서화된 절차가 있어야 한다.

12.21 오류, 불일치 또는 누락이 확인된 경우 CAPA 를 기록해야 한다.

12.22 원본 데이터, 메타 데이터 및 점검기록 기록을 검토한 후 결론을 문서화 및 서명하고 날짜를 기입해야 한다.

가. 데이터 백업, 보존 및 복원

12.23 서면 절차에 따라 데이터를 백업하고 보관해야 한다. 검증된 절차와 제어 방식으로 데이터와 기록을 확실히 보호해야 한다.

12.24 데이터와 기록은 적절한 보호를 제공하는 안전한 장소에 보관해야 한다. 액세스는 통제되어야 한다.

12.25 보존 기간은 승인된 절차로 정의해야 한다.

12.26 데이터가 파괴된 이유를 문서화해 반영한 기록을 보관유지해야 한다.

12.27 백업과 복원 프로세스를 검증하고 정기적으로 테스트해야 하며, 이 때 데이터 크기, 완전성과 데이터 및 메타 데이터의 정확성 검증이 포함되어야 한다.

13. 시정 및 예방 조치

13.1 최신 GMP (current GMP)요구 사항을 충족하지 못하는 컴퓨터 시스템(예: GXP 데이터 획득, 처리, 해석, 보고용)을 사용하고 있다면, 해당 시스템을 업그레이드하기 위한 작업 계획을 문서화 및 실현하여 최신 GMP 를 준수해야 한다.

Data review and approval

- 12.20. There should be a documented procedure for the routine and periodic review, as well as approval of data.
- 12.21. CAPAs should be recorded where errors, discrepancies or omissions are identified.
- 12.22. A conclusion following the review of original data, metadata and audit trail records should be documented, signed and dated.

Data backup, retention, and restoration

- 12.23. Data should be backed up and archived according to written procedures. The validated procedures and controls should ensure the protection of data and records.
- 12.24. Data and records should be kept in a secure area which provides appropriate protection. Access should be controlled.
- 12.25. Retention periods should be defined in authorized procedures.
- 12.26. Records reflecting documented reasons for the destruction of data should be maintained.
- 12.27. Backup and restoration processes should be validated and periodically tested, including verification of data size, completeness and accuracy of data and metadata.

13. CORRECTIVE AND PREVENTIVE ACTIONS

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

13.2 데이터 완전성에서 GMP 과실이 확인되면, 근본 원인 분석, 영향 및 위험 평가를 수행해야 한다. 적절한 CAPA 를 구축하고 실현해야 한다. 조사 결과 재료, 제품, 환자, 보고된 정보 또는 응용 서류의 데이터, 임상 시험 보고서 등에 중대한 영향 또는 위험이 있는 것으로 밝혀지면, 보건 당국 및 기타 관련 기관에 통보해야 한다.

참고 문헌 및 추가 자료

(참고: 이 섹션은 업데이트될 예정입니다)

WHO Basic Principles in Good Manufacturing Practices

WHO Guideline on Validation

WHO Guideline on Computerized Systems

WHO Guideline on Good Chromatography Practices

Medicines and Healthcare Products Guideline

U.S. Food and Drug Administration Guideline

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

International Society for Pharmaceutical Engineering (ISPE) Baseline

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

References and further reading

(Note: This section will be updated)

1. WHO Basic Principles in Good Manufacturing Practices
2. WHO Guideline on Validation
3. WHO Guideline on Computerized Systems
4. WHO Guideline on Good Chromatography Practices
5. Medicines and Healthcare Products Guideline
6. U.S. Food and Drug Administration Guideline
7. Pharmaceutical Inspection Convention and Pharmaceutical Inspection Co-operation Scheme (PIC/S) Guideline
8. International Society for Pharmaceutical Engineering (ISPE) Baseline

부록 1

데이터 완전성 관리의 예

이 부록은 데이터 완전성의 본문 내용에 근거한 데이터 완전성(DI) 관리의 몇 가지 예를 반영하였다. 이들은 예시이며 설명의 목적으로만 의도된 것임에 유의해야 한다.

예 1: 품질 위험 관리 및 데이터 완전성 위험 평가

위험 관리는 GMP(Good Manufacturing Practice)의 중요한 부분이다. 데이터 완전성 과실 가능성을 방지할 수 있도록 제조업체를 지원하기 위해 위험을 식별 및 평가하고, 제어를 확인 및 실행해야 한다.

예를 들어, 고장모드 및 영향분석(FMEA - Failure Mode and Effects Analysis) 모델(또는 기타 도구)을 사용하여 데이터가 획득, 처리, 기록, 저장 및 보관되는 시스템과 관련된 위험을 식별하고 평가할 수 있다. 심각도, 발생과 탐지 분류와 전반적인 위험 우선 순위 번호 또는 위험 요소를 기반으로, 수정 및 예방 조치(CAPA)를 확인, 실현 및 평가해야 한다.

	심각도			
O C C U R R E N C E		낮음	중간	높음
	낮음			
	중간			
	높음			
		높음	중간	낮음
	탐지			

예를 들어, 샘플의 무게 측정 중 날짜 입력이 워크 시트상에 동시에 기록되지 않았지만 샘플의 무게를 측정한 활동이 발생한 날의 저울 사용기록에서 출력을 할 수 있는 경우, 여전히 데이터 완전성으로 간주된다.

ANNEX 1

EXAMPLES IN DATA INTEGRITY MANAGEMENT

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

Example 1: Quality risk management and data integrity risk assessment

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

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

O C C U R R E N C E	Severity			
		LOW	MEDIUM	HIGH
	LOW			
	MEDIUM			
	HIGH			
		HIGH	MEDIUM	LOW
Detection				

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

그러나 활동에 대한 다른 추적 수단이 없는 경우의 위험도는 매우 다르다. 본 건의 데이터 완전성의 과실과 관련된 위험을 평가할 때, 심각도는 "낮음"으로 분류될 수 있다(데이터는 출력물에 나와 있음). 정기적으로 발생하지 않으며(발생이 "낮음") 검토자가 이를 쉽게 탐지할 수 있다(탐지가 "높음"). 따라서 전체 위험 요소는 낮은 것으로 간주될 수 있다. 계량식 분석 보고서에 기록이 작성되지 않은 근본 원인은 여전히 확인되어야 하며, 이를 방지하기 위해 적절한 조치를 취해야 한다.

예 2: 데이터 완전성의 GDP (Good Documentation Practice)

문서는 주의하여 관리해야 한다. 이들은 잘못된 입력, 조작 및 인적 오류를 제거할 수 있도록 적절히 설계되어야 한다.

종이 시스템

형식

직원이 정확한 정보를 적시에 기록할 수 있도록 형식을 설계하고 준비해야 한다. 날짜, 시간(시작, 완료), 서명, 이니셜, 결과, 배치 넘버, 장비 식별 번호 등과 같은 항목을 제공해야 한다. 시스템은 담당자에게 적절한 단계에서 항목을 작성할 것을 지시해야 한다.

빈 양식 (blank form)

빈 양식을 사용하지 않는 것이 좋다. 빈 양식이 사용되는 경우(예: 워크 시트, 실험실 노트북과 마스터 생산과 관리 기록 보충) 적절한 제어 방식이 준비되어야 하며, 예를 들어 완료시 조정될 목적으로 여러 개의 번호가 표식된 빈 양식이 사용에 포함될 수 있다. 마찬가지로 문서 제어 그룹에서 스탬프 처리하거나 공식적으로 발행한 바인딩된 페이지 매김 노트북을 사용하면, 비공식 노트북과 노트북 페이지의 공백을 탐지할 수 있다. 승인에는 날짜가 포함된 두 세 개의 서명이 포함될 수 있다(예: "준비한 사람" 또는 "입력한 사람", "검토한 사람" 및 "승인한 사람").

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

Example 2: Good documentation practices in data integrity

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

Paper systems

Formats

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

Blank forms

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

데이터 기록 오류

데이터 및 결과 입력(전자 및 종이 기록)에는 실수가 없어야 한다. 주의를 기울여 입력한다. 부정확한 정보가 기록된 경우, 오류 이유가 문서화되고 원래 항목을 읽을 수 있게 유지하고 수정 사항에 서명 및 날짜가 기입된 경우, 이를 정정할 수 있다.

예 3: 데이터 입력

데이터 입력에는 샘플 수신 등록, 샘플 분석 결과 기록, 로그 북 항목, 레지스터, 배치 제조 기록 항목 및 사례 보고 양식의 정보와 같은 예가 포함된다. 종이 기록상의 소스 데이터 기록은 지울 수 없는 잉크여야 하며 오류가 없어야 한다. 책임 있고 적절하게 훈련된 개인이 전자 기록에 직접 입력해야 한다. 입력은 개인(전자 기록에서 고유의 사용자 이름과 비밀번호를 보유함)으로 추적 가능하고 날짜(가능한 경우 시간)까지 추적 가능해야 한다. 적절한 경우, 두 번째 사람이 입력을 확인해야 한다. 또는 가능하다면 이러한 데이터를 사용하기 위해 바코드와 같은 기술적 수단을 통해 입력해야 한다. 추가 제어 방식에는 데이터가 검증된 후 중요한 데이터 항목을 잠그고 그 데이터가 변경되었는지 탐지하기 위해 점검기록을 검토하는 것이 포함될 수 있다.

예 4: 데이터 세트

만일 어떤 결과나 데이터를 배제하기 위해 문서화되고 정당한, 과학적 설명과 절차가 없다면, 모든 데이터는 데이터 세트에 포함되어야 한다. 추세에서 벗어나거나 비정상적인 결과를 얻을 때마다, 서면 절차에 따라 조사해야 한다. 여기에는 잘못된 기준, 실패, 반복 및 기타 비정상적 데이터에 대한 CAPA 조사 및 결정이 포함된다. 원본 전자 데이터의 검토에는 무효, 삭제, 잘못되거나 거부된 데이터가 저장된 위치를 포함하여, 데이터가 저장된 모든 위치에 대한 점검이 포함되어야 한다. 다른 전자 폴더나 다른 운영 체제 로그에는 데이터와 메타 데이터가 없어야 한다. 전자 데이터는 표준 운영 절차에 따라 보관해야 한다. 관련 메타 데이터가 관련 데이터 세트와 함께 보관되거나 관련 문서를 통해 데이터 세트로 안전하게 추적 가능한지 확인하는 것이 중요하다. 아카이빙(기록 저장소)에서 데이터 및 데이터 세트를 성공적으로 회수할 수 있어야

Error in recording data

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

Example 3: Data entry

Data entry includes examples such as sample receiving registration, sample analysis result recording, logbook entries, registers, batch manufacturing record entries, and information in case report forms. The recording of source data on paper records should be in indelible ink and free from errors. Direct entry into electronic records should be done by responsible, appropriately trained individuals. Entries should be traceable to an individual (in electronic records thus having a unique username and password) and traceable to the date (and time, where possible). Where appropriate, the entry should be verified by a second person or entered through technical means such as bar-coding, where possible, for the intended use of these data. Additional controls may include locking critical data entries after the data are verified and review of audit trails for critical data to detect if they have been altered.

Example 4: Dataset

All data should be included in the dataset unless there is a documented, justifiable, scientific explanation and procedure for the exclusion of any result or data. Whenever out of trend or atypical results are obtained, they should be investigated in accordance with written procedures. This includes investigating and determining CAPA for invalid runs, failures, repeats and other atypical data. The review of original electronic data should include checks of all locations where data may have been stored, including locations where voided, deleted, invalid or rejected data may have been stored. Data and metadata should not be found in other electronic folders or in other operating system logs. Electronic data should be archived in accordance with a standard operating procedure. It is important to ensure that associated metadata are archived with the relevant data set or securely traceable to the data set through

한다. 여기에는 메타 데이터가 포함된다. 이는 절차에 따라 수행해야 하며 규정된 시간 간격으로 확인해야 한다.

예 5: 지속성

데이터 생애주기 동안 데이터와 메타 데이터를 읽을 수 있어야 한다. 위험 요소에는 마이크로 필름 기록의 희미해짐, 콤팩트 디스크(CD) 및 디지털 다용도/비디오 디스크(DVD)와 같은 광학 미디어 코팅의 가독성 감소, 이러한 미디어가 깨지기 쉽다는 사실이 있다. 마찬가지로, 자성 매체에 저장된 기록 데이터도 성능 저하의 결과로 시간이 지남에 따라 읽을 수 없게 된다. 데이터와 기록은 적절한 조건에서 적절한 방식으로 저장해야 한다.

예 6: 귀속성

데이터는 귀속 가능해야 하며 따라서 개인별로 추적할 수 있어야 한다. 종이 기록인 경우 이니셜, 완전한 자필 서명 또는 인감을 사용하여 이루어질 수 있다. 전자 기록인 경우 데이터 생성, 수정 또는 삭제 작업에 사용자를 연결하는 고유한 사용자 로그인을 사용하여 수행할 수 있다. 또는 생체 인식이거나 비생체 인식될 수 있는 고유한 전자 서명으로 가능하다. 사용자 식별(ID), 날짜 및 타임 스탬프, 전자 서명을 캡처하는 점검기록은 서명된 기록에 안전하고 영구적으로 연결되어야 한다.

예 7: 동시성

직원은 데이터를 생성하고 획득할 때 데이터와 정보를 기록해야 한다. 예를 들어, 샘플의 무게가 측정되거나 준비될 때, 샘플(날짜, 시간, 사람 이름, 저울 식별 번호)의 무게는 그 이전 또는 이후 단계가 아니라 그 시점에 기록되어야 한다. 전자 데이터의 경우 자동으로 날짜와 시간이 찍혀있어야 한다. 하이브리드 시스템은 사용하지 않는 것이 좋지만 구형 컴퓨터 시스템이 교체 대기 중인 경우 문서화된 완화 제어 방식을 구비해야 한다(하이브리드 시스템의 교체는 문서화된 CAPA 계획에서 우선 순위가 되어야 한다). 다른 운영자를 대신하여 활동을 기록하기 위해 필경사를 사용하는 것은 예외적인 사항으로만 고려되어야 한다. 예를 들어, 기록 행위가 제품이나

relevant documentation. It should be possible to successfully retrieve data and datasets from the archives. This includes metadata. This should be done in accordance with a procedure and verified at defined intervals.

Example 5: Enduring

Data and metadata should be readable during the life cycle of the data. Risks include the fading of microfilm records, the decreasing readability of the coatings of optical media such as compact disks (CDs) and digital versatile/video disks (DVDs), and the fact that these media may become brittle. Similarly, historical data stored on magnetic media will also become unreadable over time as a result of deterioration. Data and records should be stored in an appropriate manner, under the appropriate conditions.

Example 6: Attributable

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

Example 7: Contemporaneous

Personnel should record data and information at the time these are generated and acquired. For example, when a sample is weighed or prepared, the weight of the sample (date, time, name of the person, balance identification number) should be recorded at that time and not before or at a later stage. In the case of electronic data, these should be automatically date and time stamped. The use of hybrid systems is discouraged but where legacy systems are awaiting replacement, documented mitigating controls should be in place. (Replacement of hybrid systems should be a priority with a documented CAPA plan). The use of a scribe to record an activity on behalf of another operator should be considered only on an exceptional basis and

활동을 위험에 처하게 하는 경우, 즉 무균 지역 근무자에 의한 문서 라인 개입과 같은 사례에만 발생해야 한다.

예 8: 변경

결과나 데이터가 변경되면 변경한 사람, 날짜, 시간 및 변경 사유를 추적할 수 있어야 한다. 전자 시스템에서 이 추적성은 점검기록을 생성시킨 컴퓨터, 또는 이러한 요구 사항을 충족하는 다른 메타 데이터 필드 또는 시스템 특성을 통해 문서화되어야 한다. 기존의 컴퓨터 시스템에 컴퓨터로 생성된 점검기록이 부족한 경우, 직원은 절차적으로 제어되는 로그 북 사용, 변경 제어, 기록 버전 제어 또는 종이와 전자 기록의 다른 조합과 같은 대체 수단을 사용할 수 있다. 이는 행동의 목적, 대상, 시기, 이유를 문서화하여 추적 가능성에 대한 GXP 규정 기대치를 충족시킬 수 있다.

예 9: 원본성

원본 데이터에는 데이터 또는 정보의 첫 번째 또는 소스 캡처와 GXP 활동 수행을 완전히 재구성하는 데 필요한 모든 후속 데이터가 포함된다(원본데이터의 정의 참조). 어떤 경우에 전자 데이터(고성능 액체 크로마토그래피(HPLC)를 통해 획득한 전자 크로마토그램)가 원본 데이터일 수도 있고, 실험실 안의 로그 시트에 온도를 기록한 것이 원본 데이터로 간주될 수 있다. 원본 데이터를 검토하고 검토 증거를 제시해야 한다(예: 검토자의 서명 및 검토 날짜). 전자 기록의 경우, 검토 및 승인된 전자 데이터 세트에 전자 서명함으로써 일반적으로 의미를 갖게 된다. 데이터 검토의 서면 절차에는 관계 직원이 검토자이자 승인자로서 책임을 이해했다는 점을 보장하는 검토와 승인 서명의 의미를 명확하게 한다. 이는 검토와 승인의 대상인 전자 데이터 및 메타 데이터의 확립된 표준에 대한 완전성, 정확성, 일관성 및 준수를 보장하기 위한 것이다. 데이터 검토의 서면 절차는 빈도, 역할 및 책임, 그리고 점검기록과 같은 의미있는 메타 데이터 검토에 대한 접근 방법을 정의해야 한다. 이 절차는 또한 검토 중에 발견된 이상 데이터를 처리하는 방법을 설명해야 한다. 이러한 검토를 수행하는 직원은 검토 대상 데이터를 포함하는 소프트웨어 시스템뿐만 아니라 검토 프로세스에서도 충분하고 적절한 훈련을 받아야 한다.

should only take place where, for example, the act of recording places the product or activity at risk, such as, documenting line interventions by aseptic area operators.

Example 8: Changes

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

Example 9: Original

Original data include the first or source capture of data or information and all subsequent data required to fully reconstruct the conduct of the GXP activity (*see the definition of raw data*). In some cases, the electronic data (electronic chromatogram acquired through high-performance liquid chromatography (HPLC)) may be the original data, and in other cases, the recording of the temperature on a log sheet in a room - by reading the value on a data logger – may be considered the original data. Original data should be reviewed. Proof of review should be presented (e.g. as a signature (reviewed by:) and date of the review). For electronic records, this is typically signified by electronically signing the electronic data set that has been reviewed and approved. Written procedures for data review should clarify the meaning of the review and approval signatures to ensure that the personnel concerned understand their responsibility as reviewers and approvers to assure the integrity, accuracy, consistency and compliance with established standards of the electronic data and metadata subject to review and approval. Written procedures for data review should define the frequency, roles and responsibilities and approach to review of meaningful metadata, such as audit trails. These procedures should also describe how aberrant data are to be handled if found during the review. Personnel who

예 10: 제어 방식

데이터 완전성 위험 평가(DIRA) (데이터 거버넌스 및 데이터 관리의 모든 영역을 다루어야 하는)의 결과를 기반으로 – 종이 기록이든 전자 기록이든 모든 데이터를 보장하기 위해 적절하고 효과적인 제어 방식을 확인하고 실현해야 한다. 이렇게 하면 ALCOA + 원칙이 충족된다. 제어 방식의 예로 다음이 포함되지만 이에 국한되지는 않는다.

- 출력물을 생성하는 저울 및 pH 측정기와 같은 장비의 자격, 교정 및 유지 관리
- 전자 기록을 획득, 처리, 생성, 유지, 배포 또는 보관하는 컴퓨터 시스템의バリ데이션
- 컴퓨터 시스템 간에 전송되는 동안 데이터의 완전성이 유지되도록 시스템을 검증
- 분석 절차의バリ데이션
- 생산 공정의バリ데이션
- GXP 기록 검토
- 편차, 의심, 추세에서 벗어나고 사양을 벗어난 결과 조사

정확한 GXP 기록을 보장하기 위해 고려할 사항:

- 인증된 사람이 중요한 데이터를 컴퓨터에 입력하는 경우(예: 마스터 프로세싱 공식 입력) 수동으로 입력한 데이터의 정확성을 추가로 확인해야 한다. 이 점검은 제 2의 승인된 사람 또는 검증된 전자적 방법에 의해 독립적인 검증 및 사용 해제함으로써 수행될 수 있다. 예를 들어, 중요한 데이터와 관련된 위험을 탐지하고 관리하려면, 절차에 따라 품질 부서 직원과 같은 제 2자의 확인이 필요하다.
- 스프레드 시트에 입력된 계산 공식

conduct such reviews should have adequate and appropriate training in the review process as well as in the software systems containing the data subject to review.

Example 10: Controls

Based on the outcome of the data integrity risk assessment (DIRA) (which should cover all areas of data governance and data management) – appropriate and effective controls should be identified and implemented to assure that all data, whether in paper records or electronic records, will meet ALCOA+ principles. Examples of controls may include, but are not limited to:

- qualification, calibration and maintenance of equipment, such as balances and pH meters, that generate printouts;
- validation of computerized systems that acquire, process, generate, maintain, distribute or archive electronic records;
- validation of systems to ensure that the integrity of data will remain while transmitting between/among computerized systems;
- validation of analytical procedures;
- validation of production processes;
- review of GXP records; and
- investigation of deviations, doubtful, out of trend and out of specifications results.

Points to consider for assuring accurate GXP records:

- The entry of critical data into a computer by an authorized person (e.g. entry of a master processing formula) requires an additional check on the accuracy of the data entered manually. This check may be done by independent verification and release for use by a second authorized person or by validated electronic means. For example, to detect and manage risks associated with critical data, procedures would require verification by a second person, such as a member of the quality unit staff;
- formulae for calculations entered into spreadsheets;

- 분석 인증서의 사양 값을 과시하는 데 사용되는 사양 범위 필드 등 실험실 정보 관리 시스템(LIMS - Laboratory Information Management System)에 입력된 마스터 데이터
- 적절한 다른 중요한 마스터 데이터. 일단 검증되면, 이러한 중요한 데이터 필드는 통상 추가 수정을 방지하고 공식적인 변경 제어 프로세스를 통해서만 수정되도록 잠겨야 한다.
- 시스템 간의 데이터 전송 프로세스를 검증해야 한다.
- 데이터를 시스템으로 이동하고 시스템에서 내보내려면 계획된 특정 테스트 및 제어가 필요하다.
- 활동이 시간임계적인 경우 인쇄된 기록에는 날짜 및 시간 스탬프가 표시되어야 한다.

- master data entered into the laboratory information management system (LIMS) such as fields for specification ranges used to flag out of specification values on the certificate of analysis;
- other critical master data, as appropriate. Once verified, these critical data fields should normally be locked to prevent further modification and only be modified through a formal change control process;
- the process of data transfer between systems should be validated;
- the migration of data into and exported from systems requires specific planned testing and control; and
- when the activity is time-critical, printed records should display the date and time stamp.

