

# 데이터 완전성 가이드라인(안) 개발

## 1) 가이드라인의 적용 범위

- 데이터 완전성은 모든 데이터에 요구되는 요소이나, 모든 데이터에 동일한 수준의 관리 절차를 적용해야 하는 것은 아니다. 연관되는 절차와 허가사항에 미치는 영향 등 각 데이터의 중요도를 평가하는 과정을 통해 효과적인 관리 체계를 수립해야 한다.
- 데이터 중요도와 관련하여 고려해야 할 사항은 다음과 같다.
  - 데이터가 어떤 결정에 영향을 미치는가?
  - 데이터가 제품 품질이나 소비자의 안전에 미치는 영향은 무엇인가?
- 데이터의 중요도 또는 (실패 시) 위험평가 요소는 다음을 포함한다.
  - 우발적인 변경, 삭제, 손실, 재생성 또는 고의적 위조에 대한 취약성
  - 위변조 행위의 탐지 가능성
  - 재해 발생 시 완전한 복구 가능성
- 관리 대상 데이터는 다음의 형태를 포괄하며, 데이터를 다루는 주체의 전자, 수기 또는 하이브리드 (종이와 전자 데이터 결합) 시스템 특성에 따라 결정될 수 있다.
  - 종이에 기록, 수동 관찰이나 활동에 따른 종이 기반 출력물
  - 전자적인, 즉 간단한 기계에서부터 고도로 복잡하게 설정 가능한 컴퓨터화 시스템에 이르는 장비 내부 원시 데이터
- 연구 및 개발을 전담하는 조직에서 데이터의 중요도 판단의 기준이란 때로 제품화의 가능성, 제제 및 공정 개발의 진척도에 따라 좌우될 수 있다. 이러한 기준을 적용한 결과의 구체적인 예시로 다음의 범위를 들 수 있다.
  - 제품 및 공정 개발의 주요 파라미터를 설정하는 데 사용되는 근거자료 또는 그 자료를 준비하기 위한 반복시험 결과와 해당 원 데이터 (Raw Data) 그리고 해당 원본을 보증하기 위한 모든 보충 데이터 (Supporting Data)
  - 신약개발 또는 기존 제제의 개량을 위한 초기 단계 연구의 경우, 데이터의 중요도 판단 기준이 해당 프로젝트의 매니지먼트 도구와 직간접적인 연관성을 가질 수 있다. 후보물질이나 제형을 특정할 수 있을 만큼 연구개발의 범위가 축소되고 상용화가 확실시되는 비즈니스 결정이 위험 평가 기준에 포함될 수 있으며, 이 평가 결과를 통해 데이터 관리 범위를 구체적으로 설명할 수 있어야 한다.

- 구체적인 관리 대상의 범위는 조직의 규모와 개발 파트너십 그리고 프로젝트 매니지먼트 규모 및 방식에 차이에 따라 일률적으로 설정하기 어려울 수 있다. 규제, 시장, 분사 및 인수합병과 같은 다양한 요인에 의해 예정에 없이 신설, 폐기되는 연구 개발 프로젝트의 가변성을 고려하여 데이터 완전성을 기하는데 일관적인 원칙을 가지고 임해야 한다. 연구개발 단계에서부터 QbD (Quality by Design, 설계기반 품질고도화) 접근법을 고려하여 상용화 단계의 품질에 유의미한 데이터를 보증하도록 관리의 범위를 신중히 검토하고 적용해야 한다.
- 참고: PIC/S 5.3.4, 5.4.1, 5.5.1 MHRA 4.3

## 2) 데이터 완전성 관련 용어의 정의

### 가) 용어 및 정의

데이터의 신뢰성이라는 매우 한정적이고 특수한 주제에 대한 가이드라인이 영미권에서 시작된 이래로 “Integrity”란 우리말로 완전성, 무결성, 완결성 등 중론 없이 사용되고 있다. 이 외에도 기존에 일반적으로 쓰이지 않았던 어휘의 조합이 점차 구체적인 개념으로 자리잡고 있으며, 아직 이에 대한 국내 규제당국의 공식적인 지침이 발표되지 않았다.

이에 아래 <표 24>와 같이 영어 원문과 동치할 수 있는 국문 단어를 정립함으로써 중요 용어의 오용을 막고 업계 내 일관성 있는 의사소통에 뒷받침 할 수 있도록 한다. 단, GMP, GxP, Validation, CAPA, Deviation, QRM, QS, LIMS 등 기존 제약업계에서 자주 사용되는 용어는 제외하였다. 용어는 식약처 의약품 제조 및 품질관리 가이드라인(2018)<sup>1</sup>에 나온 용어를 우선순위로 두었으나, 여기에 포함되지 않은 용어의 경우에는 외국의 가이드라인(MHRA, WHO, PIC/S )에 나온 용어를 종합적으로 고려하여 정하였다.

---

<sup>1</sup> 식품의약품안전처. (2018) 완제의약품 제조 및 품질관리기준 가이드스(민원인 안내서) 제 2 개정판 및 후보 2018.5. 의약품안전국 의약품품질과

<표 1> 데이터 완전성 관련 용어 및 정의

구분	영문	국문	정의	출처
ALCOA	Attributable	귀속성	기록된 작업을 수행한 개인 또는 컴퓨터 시스템을 식별할 수 있어야 한다. 작업/기능을 수행한 사람에 대해 문서화해야 할 필요성은 숙련되고 자격을 갖춘 직원이 기능을 수행했음을 어느 정도 입증하기 위함이다. 이는 수정, 삭제, 변경 등 기록의 변경 사항에도 적용된다	PICS
	Legible	가독성	모든 기록은 읽을 수 있어야 한다. 정보를 어떤 식으로 사용하려면 읽을 수 있어야 한다. 이는 모든 원본 기록 또는 항목을 포함하여 완전한 것으로 간주되도록 요구되는 모든 정보에 적용된다. 전자 데이터의 '동적' 특성(검색, 문의, 경향 등)이 기록의 내용과 의미에 중요한 경우, 적합한 응용 프로그램을 사용하여 데이터와 상호 작용하는 능력은 기록의 '가용성'에서 중요하다.	PICS
	Contemporaneous	동시성	행동, 사건 또는 결정의 증거는 발생 시에 기록되어야 한다. 이 문서는 수행된 사항, 결정된 사항 및 이유, 즉 당시 결정에 영향을 준 이유를 정확하게 입증하는 역할을 한다.	PICS
	Original	원본성	원본 기록은 (정적인) 종이 또는 (일반적으로 시스템의 복잡성에 따라 동적인) 전자에 기록되는 정보의 첫 번째 캡처로 설명할 수 있다. 원래 동적인	PICS

구분	영문	국문	정의	출처
			상태에서 캡처된 정보는 그 상태로 사용 가능하도록 유지되어야 한다.	
	Accurate	정확성	결과 및 기록의 정확성을 보장하는 것은 강력한 PQS 의 여러 요소를 통해 가능하다. 이것은 다음으로 구성될 수 있다.	PICS
ALCOA +	Complete	완전성	한 이벤트를 이해하려고 할 때 그 이벤트를 재구성하는 데 핵심적인 모든 정보가 중요하다. 일련의 정보가 완전한 것으로 간주되는 데 필요한 세부 수준은 정보의 중요도에 따라 다르다	PICS
	Consistent	일관성	GDP 는 프로세스 중에 발생할 수 있는 일탈을 포함하여 예외 없이 모든 프로세스에서 적용해야 한다. 여기에는 데이터에 대한 모든 변경 사항을 캡처하는 것이 포함된다.	PICS
	Enduring	영구성	기록은 필요한 전체 기간 동안 존재하도록 유지되어야 한다. 즉, 기록 보존 기간 내내 지울 수 없고/지속 가능한 기록으로 온전히 유지되고 액세스할 수 있어야 한다.	PICS
	Available	가용성	기록은 필요한 보존 기간 동안 언제든지 검토할 수 있어야 한다. 정기적인 출하 결정, 조사, 경향, 연례 보고서, 감사 또는 검사 여부를 검토할 책임이 있는 모든 해당 직원이 읽을 수 있는 형식으로 된 기록에 액세스할 수 있어야 한다.	PICS

구분	영문	국문	정의	출처
해외 가이드라인	Audit Trail	점검기록	점검기록은 GXP 기록의 생성, 수정 또는 삭제와 관련한 작업과 그에 관련된 정보가 포함된 메타데이터의 한 형식이다. 점검기록은 원본 기록을 가리거나 덮어쓰지 않고, 종이 또는 전자 기록으로 기록 내의 정보 생성, 추가, 삭제 또는 변경과 같은 수명주기의 세부 사항을 안전하게 기록한다. 점검기록은 작업의 "누가, 무엇을, 언제, 왜"를 포함하여, 매체와 상관없이 기록과 관련된 이러한 이벤트의 히스토리 재구성을 쉽게 한다.	MHRA
	Data Backup	데이터 백업	재난 복구를 위한 현재 (편집 가능한) 데이터, 메타 데이터 및 시스템 설정 세팅(예: 분석 실행과 관련된 변수 세팅)의 사본	PICS
	Data Governance	데이터 거버넌스	데이터 생애주기 동안 데이터가 생성, 기록, 프로세스되는 형식에 관계없이, 완전하고 일관되며 정확한 기록을 유지하고 사용하도록 보장하기 위한 전체적인 조치의 총합	PICS
	Data Integrity	데이터 완전성	데이터가 완전하고 일관성 있고 정확하며 신뢰할 수 있으며 수명주기 내내 이러한 특성이 유지된다. 데이터는 귀속적이고 읽을 수 있고, 동시에 기록되고 원본(또는 실제 사본)이며 정확하므로, 안전한 방식으로 수집 및 유지되어야 한다. 데이터 무결성을 보장하려면 적절한 품질 및 위험 관리 시스템이 필요하다. 여기에는 건전한	MHRA

구분	영문	국문	정의	출처
			과학적 원리 준수와 우수한 문서화 기준이 포함된다.	
	Data Life Cycle	데이터 생애주기	데이터가 폐기될 때까지 생성, 기록, 처리, 수정, 전송, 검토, 보고, 사용, 승인, 보관 및 복구되는 프로세스의 모든 단계를 말한다.	WHO
	Legible	가독성	모든 기록은 읽을 수 있어야 한다. 정보를 어떤 식으로 사용하려면 읽을 수 있어야 한다. 이는 모든 원본 기록 또는 항목을 포함하여 완전한 것으로 간주되도록 요구되는 모든 정보에 적용된다. 전자 데이터의 '동적' 특성(검색, 문의, 경향 등)이 기록의 내용과 의미에 중요한 경우, 적합한 응용 프로그램을 사용하여 데이터와 상호 작용하는 능력은 기록의 '가용성'에서 중요하다.	PICS
	Meta Data	메타데이터	다른 데이터의 속성을 설명하고 컨텍스트와 의미를 제공하는 데이터를 말한다.	PICS
식약처 가이드	Archiving	아카이빙	특정 프로세스 또는 활동을 복구하기 위한 목적으로 관련한 메타데이터(metadata)를 포함한 데이터를 완전한 형태로 장기간 또는 영구적으로 보관하는 것을 말한다.	식약처
	Original copy	원본 기록	최초 생성된 데이터 파일 또는 포맷으로서 완전성을 보존하고 있는 기록을 말한다. 예를 들어, 원본 수기 기록 또는 컴퓨터화 시스템의 경우 원본 전자 데이터 파일이 해당된다.	식약처

구분	영문	국문	정의	출처
	Raw data	원본데이터	확인 또는 행동한 결과로서 최초로 생성된 기록 또는 문서를 말하며, 종이 또는 전자 형태로 존재할 수 있다. 전자 기기이나 전자기록이 저장되지 않고, 결과값이 종이에 출력되는 형태의 pH meter 나 저울과 같은 경우 원본데이터는 그 출력물이 유효사본(True Copy)으로서 원본데이터를 구성할 수 있다. 다만, 원본데이터는 시스템 절차에 규정되어야 한다.	식약처
	True copy	정본	원본(Original Record)과 정확히 동일함이 검증된 사본을 말한다.	식약처

### 3) 데이터 거버넌스

#### ○ 데이터 완전성을 위한 문화 및 정신

- 데이터를 신뢰할 수 있는 문화를 만든다는 것은 품질을 보증하기 위한 책임 있는 자세와 환경을 조성하는 것이다.
- 이것은 각 직원마다 확립되어야 하고, 일관되게 전달할 수 있어야 한다.
- 데이터 완전성을 위한 정직과 같은 윤리적 행동의 기대를 명확하게 정의해야 하며, 모든 직원에게 전달되고 잘 이해되도록 해야 한다.
- 고의적인 데이터 위조, 무단 변경, 데이터 파기 또는 데이터 완전성을 손상시키는 행위가 일어나지 않도록 조치하고 보증하는 것이 필요하다는 것을 인식해야 한다.
- 참고 PIC/S 6.1.7, 6.2.4, 6.2.5, 6.3.1, MHRA 3.1, 3.2, 3.3

#### ○ 경영 리더쉽

- 경영진은 투명하고 개방적인 작업 환경인 동시에 적절한 품질 문화를 조성해야 한다.

- 경영진은 잠재적인 데이터 신뢰성 문제를 포함하여 오류와 실수를 자유롭게 전달하여 시정 및 예방조치를 취할 수 있도록 해야 한다.
- 경영진은 데이터의 품질을 보증할 수 있고 데이터 완전성을 보장할 수 있는 기대하는 활동을 관리할 수 있어야 한다. (예를 들어, 윤리강령 및 행동강령 같은 활동은 기대에 대한 인식과 이해를 보장하여 데이터 완전성 관련 환경이 조정될 수 있도록 도움을 줄 수 있을 것이다.)
- 참고 PIC/S 5.3.1, 6.1.4, 6.1.6, 6.2.2, 6.3.3, 6.5.2, 6.5.3, 6.6.1, 6.6.2, 6.6.3 WHO 4.2

#### ○ 데이터 완전성 정책 및 절차

- 서면으로 된 데이터 완전성 정책이 있어야 한다.
- 데이터 완전성 정책 및 절차의 준수는 정기적으로 경영진에서 보고되어야 한다.
- 데이터 거버넌스 조치는 수명주기 내내 데이터가 완전하고 일관되며 지속적이며 사용 가능해야 한다.
- 데이터는 정기적으로 관리 검토해야 한다. 데이터 완전성을 위해 중요도, 우선순위를 정하여 관리할 수 있어야 한다.
- 데이터는 귀속 가능해야 하며 따라서 개인별로 추적할 수 있어야 한다. 종이 기록인 경우 이니셜, 완전한 자필 서명 또는 도장을 사용하여 이루어질 수 있다. 전자 기록인 경우 데이터 생성, 수정 또는 삭제 작업에 사용자를 연결하는 고유한 사용자 로그온을 사용하여 수행할 수 있다.
- 모든 데이터는 ALCOA+ 원칙에 의해 관리되어야 한다.
- 데이터 완전성의 3 요소<sup>2,3</sup>인 People, Process, Technical 3 요소를 적절하게 관리할 수 있도록 환경변화에 맞는 적절한 절차를 업데이트 해야 한다.
- 데이터 완전성 정책 및 절차를 관리하기 위한 Checklist 를 ‘마.데이터 완전성 Checklist 의 개발(안)’ 에 수기데이터 관리, 자동화장치 등의 관리, 외주업체 관리로 나누어 확인 할 수 있다.  
특히, 자동화 장치 Checklist 에서는 Technical Check 항목과 Process Check 항목으로 확인하여 데이터 거버넌스를 확립 할 수 있도록 하였다.
- 참고 PIC/S 5.6.2, 5.6.3, 7.3, WHO 4.1, 6.1, 10.7, 12.20, 12.21

#### ○ 교육

<sup>2</sup> ISPE. (2017) GAMP Guide : Records and Data Integritys

<sup>3</sup> ISPE. (2018) GAMP RDI Good Practice Guide: Data Integrity - Key Concepts



- 데이터에 직간접적으로 기여하는 모든 직원은 데이터 관리 정책에 대한 충분하고 정기적인 교육을 받아야 한다.
- 데이터 완전성 교육 내용은 데이터 관리 정책 위반 시 발생할 수 있는 위험성을 포함해야 한다.
- 데이터 완전성을 독립적으로 검토하고 감사하는 직무를 설정하고 자격요건을 부여한다.
- 데이터 완전성에 영향을 미치는 IT 및 공무부서는 특정한 훈련 및 검증이 필요할 수 있다.
- 참고 PIC/S 6.6.4, WHO 8.1, 8.2

#### 4) 데이터 생애주기(Data Life Cycle) 별 필수요건 - 전자데이터

##### 가) 전자데이터의 완전성을 위한 가이드라인(안)

###### ○ 데이터 생성

- 전자 데이터 역시 귀속성, 가독성, 동시성, 고유성, 정확성에 따라 현재 데이터의 관리 지침을 마련해야 한다. – 짧은 기간 데이터를 관리하는 것과 오랜 기간 데이터를 관리해야 할 필요가 있는 경우 그에 따른 프로세스를 마련해야 한다.
- 데이터가 생성될 때 누가 생성했는지를 알 수 있어야 한다. (예, 회사에 같은 사람이 입사할 경우 어떻게 데이터가 저장되는지를 고려할 수 있어야 한다. 퇴사한 ID 를 다시 부여할 수 없어야 한다.)
- 데이터가 시스템에 생성될 때 그 데이터를 읽을 수 있는 값의 범위, 한계를 정확히 표시하고있는지 검토해야 한다. (예, 화면에서 본 데이터와 출력된 데이터가 같아야 한다. 소수점 표기가 있을 경우 자릿수 표기에 유념해야 한다. 올림, 반올림 등의 규칙을 명확히 정하여 적용해야 한다.)
- 데이터가 생성될 때 그 시점에 정확히 생성되는지 확인해야 한다. (예, 실험 시 저장하는 데이터는 그 즉시 저장해야 한다. 만약, 기억력에 의존하여 저장할 경우 오류가 발생할 가능성이 있다. 서버시간, 기기 PC 의 OS 시간이 표준시간인지 확인해야 하며, 그 시간을 데이터가 만들어지는 시점에 동시적으로 기록하는지 확인해야 한다.)
- 데이터는 메타데이터로써 특징을 가지고 있어야 한다. (예, 데이터와 연결된 데이터들이 함께 생성되어야 한다. 데이터 생성 주체, 시간, 저장위치,

연결된 데이터(초기 샘플 No. = 최종 샘플 데이터) 등이 함께 저장되어야 한다.

- 데이터는 시스템 내 자체 검사를 통해 정확성을 확보하거나, 시스템에서 기능을 제공하지 않을 경우 데이터가 정확하다는 것을 보증 할 수 있는 시스템을 갖추고 있어야 한다. 이 시스템은 반드시 전자시스템일 필요는 없으며, 수동 작업과 병행하여 진행할 수 있다. 즉, 2 차 검토가 포함되어 검토되어야 한다.
- 수기작성을 위해 관리하는 전자데이터(양식 등)등 도 관리 범위에 포함해야 한다.
- 데이터를 생성할 수 있는 사람이 정의되어야 한다. 즉, 교육을 받아 시스템을 능숙하게 다룰 수 있다는 것을 문서화할 필요가 있다.
- 생성되는 데이터가 많을 경우 이에 대한 위험평가 후 관리방안을 마련할 수 있어야 한다.
- 참고 PIC/S 9.2, WHO 12.7, 12.8, 12.9, 12.10, MHRA 6.7, 6.9, 6.16

#### ○ 데이터 저장

- 데이터가 저장하는 공간에 대한 접근 관리를 해야 한다.
- 데이터를 저장하는 공간이 공용 공간인지 개인 공간인지에 따라 관리 기준을 정할 수 있어야 한다.
- 임시로 데이터를 저장하고, 그 데이터를 이동하는 행위는 데이터의 고유성을 훼손할 수 있다. (예, 공용으로 사용하는 PC 또는 공통으로 로그인되는 바탕화면 등에서의 데이터 저장은 데이터 무결성을 저해할 수 있으므로 별도의 관리하는 공간에 저장해야 한다.)
- 저장한 데이터는 다시 확인 할 수 있어야 하며, 다시 확인할 때는 원본 그대로의 상태여야 한다.
- 데이터를 별도의 엑셀파일로 옮겨 분석하거나, 저장할 때는 원본데이터와 함께 저장되어 관리되어야 한다.
- 참고 PIC/S 9.5, WHO 12.11, MHRA 6.11, 6.12

#### ○ 데이터 수정 및 삭제

- 데이터를 수정하거나 삭제할 필요가 있는 사항인지 검토되어야 한다.
- 데이터를 수정하거나 삭제하는 것은 가능하면 권장하지 않는다.

- 데이터를 수정하는 사람, 삭제하는 사람이 누구인지 확인할 수 있어야 한다.
- 데이터를 수정하기 전 값과 수정한 후, 삭제하기 전 값을 확인할 수 있어야 한다.
- 데이터를 수정하거나 삭제해야 한다면, 수정이나, 삭제 이유를 반드시 남길 수 있어야 한다.
- 데이터를 수정하거나 삭제한 시간이 현재 시간이어야 한다.
- 데이터를 수정하거나 삭제 할 경우 그와 관계된 값도 수정되어야 한다.
- 참고 PIC/S 9.8, WHO 12.14, MHRA 6.15

#### ○ 데이터 검토<sup>4</sup>

- 데이터를 정기적으로 확인할 필요가 있는지 위험평가 결과에 따라 검토해야 한다.
- 데이터를 저장하고, 수정하고, 삭제하는 행위에 대해 적절히 관리되고 있는지 문서화해야 할 필요가 있다.
- 검토 대상이 되는 데이터는 사용자의 ID 정보를 포함하여 데이터와 연계된 메타데이터 전체를 의미한다. 따라서, 관련된 데이터를 정기적으로 검토할 수 있는 시스템 구축이 필요할 수 있다.
- 전자서명을 적용할 경우 전자서명에 이름, 서명일시, 서명의 의미를 포함하여 관리해야 한다.
- 전자서명을 적용할 경우 복사/위조/변조가 불가능해야 하며, 전자 기록과 연결되어야 한다.
- 참고 PIC/S 9.4, 9.6, WHO 12.12, 12.13, 12.15, 12.16, 12.20, 12.21, 12.22, MHRA 6.19

#### ○ 데이터 아카이빙

- 짧은 기간 저장할 수 밖에 없는 경우 2 차적인 수단을 통해 관리해야 한다. (예, 출력 및 백업 등)
- 데이터를 가공하고, 분석하여 활용한 경우 원본데이터와 함께 보관해야 한다.
- 데이터를 보관하는 기간을 정하여, 그 기간안에 데이터의 훼손 등을 방지할 수 있어야 한다.

---

<sup>4</sup> verification of record (secondary checks), 출처: PIC/S 8.8

- 데이터를 장기적으로 보관할 때는 우발적, 고의적 훼손이 발생하는 경우에 대한 대응방안이 마련되어야 한다.
- 보관된 데이터를 다시 확인하고, 검토할 때 그 데이터는 완전해야 하고, 데이터에 대한 가용성을 보증할 수 있어야 한다.
- 참고 PIC/S 9.7, WHO 12.23, 12.24, 12.25, 12.26, 12.27, MHRA 6.17

#### ○ 데이터 폐기

- 데이터의 폐기는 적절한 절차가 만들어져 있을 경우 그에 따르며, 절차가 만들어져 있지 않을 경우 폐기하기 전 충분한 검토를 하여 폐기해야 한다.
- 데이터를 폐기해야 할 사유가 있다면, 폐기하는 주체와 폐기하는 사유를 구체적으로 서면으로 남길 수 있어야 한다.
- 데이터 폐기를 하는 행위는 현재 존재하는 데이터에 영향을 주지 않아야 한다.
- 현재 저장되어 폐기되지 않는 데이터에 영향을 주지 않았다는 것을 증명할 수 있어야 한다.
- 시스템의 업그레이드로 현 시스템에서 데이터를 폐기해야 할 때는 데이터의 이동 및 보존을 선행작업 한 후 그 데이터의 이동 및 보존이 완전한 지 증명했을 경우에만 인정할 수 있다.
- 참고 PIC/S 9.7, WHO 12.26, MHRA 6.17

### 나) 컴퓨터화 시스템의 데이터 완전성을 위한 표준운영절차 (SOP) 의

#### 예시

(Standard Operation Procedure for Data Integrity of Computerized Systems)

#### 1. 목적 (Purpose)

본 문서는 000 연구소에서 운영 중인 컴퓨터시스템으로부터 생성되는 전자데이터에 대한 관리방법에 대해 정의함으로써 전자데이터의 완전성을 보증하기 위함에 그 목적이 있다.

#### 2. 적용범위 (Scope)

☞ 000 연구소 컴퓨터시스템에서 생성되는 전자데이터에 대해 적용한다.

### 3. 책임 (Responsibilities)

#### 3.1 프로세스 책임자

3.1.1 전자데이터 검토의 준비 및 실시를 지원한다.

3.1.2 검토 결과를 감안하여 적절하게 대응 조치를 취한다.

#### 3.2 품질보증 책임자

3.2.1 전자데이터의 검토 결과를 승인한다.

#### 3.3 컴퓨터화 시스템의 전자데이터 검토 담당자

3.3.1 전자데이터를 검토하고 검토결과를 종합하여 보고한다.

### 4. 용어의 정의 (Definitions)

약어 (Abbreviation)	해설 및 정의 (Comment and Definition)	출처 (Reference)
GxP	GLP, GCP, GMP 등을 총칭한다.	KFDA 알기 쉬운 GMP 용어집
SOP	Standard Operating Procedure (표준작업방법서) 특정 제품이나 물품에만 반드시 국한될 필요는 없으나 작업 수행에 관한 지시 사항을 제시하는 승인된 절차 문서를 말한다(예, 설비 운전, 유지 관리 및 세척, 밸리데이션, 시설 청소 및 환경 관리, 검체 채취 및 검사).	KFDA 알기 쉬운 GMP 용어집

### 5. 절차 (Procedures)

#### 5.1. 일반 사항

5.1.1. 컴퓨터시스템을 사용하면 데이터가 전자기록의 형태로 생성되어 저장되는데, 그 데이터를 본 문서에서는 전자데이터라 한다.

5.1.2. 전자데이터는 데이터를 생성하는 시스템과 그 데이터를 전송 받아 결과로서 처리하는 시스템의 기록 모두가 해당된다.

5.1.3. 전자적으로 기록/관리되는 데이터는 데이터 완전성의 확보 및 보증을 위해 다음과 같이 ALCOA Plus 항목 기준으로 기록 및 관리되어야 한다.

5.1.4. 위 표의 완전성 보증 방안에서 언급한 모든 항목은 별도의 체크리스트 또는 전자데이터 검토 기록지(XXX-XX-XXX 첨부 1)에서 관리한다.

ALCOA Plus	완전성 확보 방법 (How to Ensure Integrity)	완전성 보증 방안 (Measure for Guaranteeing Integrity)
귀속성 (Attribute)	작업과정 및 그 결과에 대한 데이터 기록 시 작업자 또는 기록자(기계 또는 시스템 포함)가 기록되어야 하고, 본인이 직접 기록해야 함(직접 로그인(또는 전자서명) 해야 하고 로그인 정보가 노출되지 않아야 함) 어느 기계 또는 기기의 작업에 관한 데이터인지, 어느 계측기에서 얻은 데이터인지, 어떤 연구과정, 시험시스템 또는 분석과정을 거쳐 얻은 데이터인지 확인될 수 있어야 함	보안관리(로그인 및 전자서명 정보가 노출되지 않아야 하거나 1 인 1 계정, 권한 있는 자만이 접근 가능 등); SOP에 따라 관리 로그인하는 자가 작업자로 입력, 작업이 실행된 장비번호 입력, 전자서명에 대한 정보 저장 등 확인 로그인 확인을 위해 접근이력 확인
가독성 (Legible)	한번 기록한 데이터는 어떤 경우라도 유실, 은폐되지 않아야 하므로 데이터를 변경하더라도 원본데이터 및 변경과정을 읽을 수 있어야 함 한번 생성된 데이터는 유실, 은폐되어서는 안되고 정당한 사유로 정해진 절차에 따라 폐기하기 전까지는 그 시스템 안에서 읽을 수 있어야 함 시스템이 업그레이드된 경우 이전 버전으로 생성된 데이터를 읽을 수 있어야 함 작업이 이루어진 현장에서 해당 데이터의 원본(또는 진본)기록을 언제든지 열람할 수 있어야 함	변경이력(점검기록) 확인 (Audit trail) 데이터 백업 및 복구방법에 따라 관리 시스템 업그레이드 시 점검해야 함(변경관리에 따라) 작업현장에서의 조회, 출력
동시성 (Contemporaneous)	작업과 동시에(또는 거의 동시에) 기록되고 저장되어야 함 시스템의 시계를 기록자가 임의 조정할 수 없어야 함	작업 또는 데이터 기록 즉시 저장상태 확인 보안 정책의 사용자 계정관리 방법에 따라 관리
원본성 (원본 또는 진본, Original or True Copy)	모든 출력물은 사전에 정의된 양식으로 등록되어야 하고, 그 양식에는 양식에 대한 번호(서식번호)가 표기되어야 함 데이터가 가공된 경우 그 원본데이터를 오류없이 읽을 수 있어야 하며 변경사유를 알아야 함	필요 양식 확인 점검 기록(Audit Trail) 출력 확인
정확성 (Accurate)	각 파라미터의 정확성, 기록장치 및 출력장치의 정확성이 보증되어야 함 데이터 처리방법(계산식 등)은 정확히 등록되어야 하고, 등록된 방법에 따라 결과가 산출되어야 함다른 시스템으로 데이터 전송 시 생성된 데이터와 동일하게 전송되어야 함	파라미터, 기록, 출력장치 확인 계정 및 권한관리 SOP에 따라 관리함(권한 정의서 관리) 기준정보 관리에 따름(각 시스템 SOP) 인터페이스 확인 인터페이스 오류 이력 확인

ALCOA Plus	완전성 확보 방법 (How to Ensure Integrity)	완전성 보증 방안 (Measure for Guaranteeing Integrity)
완전성 (Completeness)	준비사항, 작업에 사용된 물품, 작업내용(파라미터 등), 결과값 등이 자동으로 입력되거나 사용자가 입력하는 내용 모두가 저장되어야 함 메타데이터, 이벤트 재구성이 가능해야 함	입력값, 이벤트 모두 저장 알람 이력 확인
일관성 (Consistent)	저장되거나 처리된 결과물은 자동적으로 또는 임의로 변경되지 않아야 함 데이터가 변경된다는 것은 데이터 자체가 변경되는 것이 아니라 변경이력이 저장되고 변경된 값이 추가적으로 기록되는 것을 의미함	데이터 입력 및 변경 값 변경이력(점검기록) 확인 (Audit trail)
지속성 (Enduring)	데이터는 보관기한 동안 변경이력을 포함하여 훼손, 손상, 변조되지 않아야 함 데이터의 백업 및 아카이빙이 정상적으로 진행되어야 하고 문제 발생 시 복구할 수 있어야 함	데이터 기록, 확인 백업 및 복구 SOP 따라 관리 변경이력(점검기록) 확인 (Audit trail)
유용성 (Available)	데이터는 사용할 수 있도록 조회, 출력되어야 함 데이터는 생성된 데이터, 처리된 결과, 이력(변경이력, 전자서명이력, 접근이력, 권한관리이력 등)이 모두 이용될 수 있도록 출력되어야 함	조회, 출력 확인 점검기록(Audit Trail) 확인 (변경이력, 전자서명이력, 접근이력, 권한관리 이력 등)

## 5.2 전자데이터 검토 주기

연구소에서 발생하는 모든 데이터는 검토주기를 설정하기 위해 검토주기 대상 선정, 검토 주기 대상의 검토 수준 결정, 주기적 검토를 통한 검토 주기 재선정 작업을 진행하는 것을 권장한다.

5.2.1.검토주기 대상 선정: 검토주기 대상을 선정하기 위해 제품 후보 물질 가능성이 있는 실험의 데이터, 제품 개발 시 개발 단계 중 중요한 단계에 있는 데이터를 선정기준에 포함시키는 것이 중요하다.

5.2.2.검토주기 대상의 검토 수준 결정: 검토 대상이 된 데이터 중 중요한 데이터 일 경우 매일 1 회 검토하는 것을 권장한다. 데이터의 완전성을 확보한다는 것은 데이터가 생성되는 가장 가까운 시점에서 검토되는 것이 데이터 완전성을 확보하는데 중요하기 때문이다.

5.2.3.주기적 검토를 통해 검토 주기를 재선정하는 것이 중요하다. 검토 주기는 최초에 설정한 기준에서 데이터 경향에 따라 검토주기를 변경할 수 있다. 데이터 검토주기를 결정할 때는 해당 데이터를 검토할 수 있는 인력, 검토하는 데이터의 사이즈에 따라 고려될 수 있을 것이다. 따라서, 검토주기는 검토인력, 데이터량, 데이터의 신뢰도(경향)에 따라 결정될 것이다.

데이터 중요도 설정 (Data Criticality)	제품 후보 물질 가능성이 있는 데이터 또는 중요한 단계에 있는 데이터 (Critical Data)	관리가 필요하다고 판단되는 데이터 (Non-Critical Data)
검토 시기	1 회/매일*	1 회/N개월*
검토 내용	비인가 사용자의 접근이력 확인 감사추적 검토(결과, 파라미터, 시간, 알람 모두 포함) 시스템 오류 이력 확인	

<Pics PI\_041\_1\_Draft\_3\_Guidance\_on\_Data\_Integrity Section 9.6 Review of data within computerized systems>

### 5.3 전자데이터 검토 실시

5.3.1. 전자데이터의 완전성 보증을 위한 활동 중 SOP 를 통해 관리되는 활동에 대해 검토를 진행한다.

5.3.2. 전자데이터 검토를 실시하고, 전자데이터 검토 기록지(XXX-XX-XXX 첨부 1)에 기록한다.

5.3.3. 전자데이터 검토의 해당 항목의 관련 자료는 첨부한다.

5.3.4. 전자데이터 검토 기록지(XXX-XX-XXX 첨부 1)는 아래와 같이 작성한다.

#### -전자데이터 검토

##### 1) 결과

검토 항목의 내용에 대해 'Yes' 또는 'No'를, 해당사항이 없으면, 'N/A'에 체크한다.

##### 2) 조치 방법

검토 항목에 대한 결과가 적합하지 않으면, 'Investigation'에 체크하고, 해당사항이 없으면, 'N/A'에 체크한다.

##### 3) 비고

결과나 조치 방법을 체크하는데 있어서 특이사항이나 코멘트 내용이 있을 때 기록한다. 또한 해당 항목의 첨부 문서 번호를 기재한다.

#### -전자데이터 검토 결과

##### 1) 항목번호

전자데이터 검토'의 조치 방법에서 'Investigation'에 체크된 항목 번호를 기록한다.

##### 2) 조사 내용

전자데이터 검토'의 조치 방법에서 'Investigation'에 체크된 항목의 조사 내용을 자세히 기록한다.

##### 3) 조치 방법

4) 조사 내용에 대한 결과가 일탈이면, 'Deviation'에 체크하고, 일탈이 아니면, 'N/A'에 체크한다.

#### - 결론

전자데이터 검토 결과'의 조치 방법에서 모든 항목이 'N/A'일 때 'Pass', 항목들 중 하나라도 'Deviation'에 체크 되면 'Fail'에 체크한다.

##### 5.3.5. 전자데이터 검토 완료 후 활동

시정조치가 필요한 항목의 경우 별도의 CAPA 활동을 실시하여 처리한다.

##### 5.3.6. 전자데이터 검토 활동 종료

전자데이터 검토 기록지(XXX-XX-XXX 첨부 1)에 기록된 일탈 발생 항목들이 일탈관리 절차에 따라 조치가 완료되면, 전자데이터 검토 활동이 종료된다.



## 6. 참고 문헌 (References)

[의약품 제조 및 품질관리에 관한 규정 [별표 9] 컴퓨터화 시스템].  
[GAMP 5 : ISPE]

## 7. 양식 (Forms)

첨부 1. 전자데이터 검토 기록지 – 본 보고서 [부록 1] 에 첨부

## 8. 배포부서 (Distribution Departments)

### 다) 자동화장치 등의 관리를 위한 체크리스트<sup>5</sup>

본 체크리스트는 자동화장치를 도입하는 시기부터 체크해야 할 사항이며, 자동화 장치 등의 변경(업데이트, 패치, 고장으로 인한 수리 등)이 발생하는 시점에서 확인해야 할 사항이다.

#### ○ Technical Checklist

- 시스템의 보안 범위를 규정하고 있고 허가된 인원만 시스템을 사용할 수 있도록 권한이 부여되어 있는가?
- 시스템에 대한 물리적인 보안이 적절한가?
- (특정 컴퓨터장비가 집합된 서버실의 키,패스카드,생체인식을 통한 시건장치)
- 시스템 데이터의 원본기록과 실제 사본은 동일 한가?
- 중요한 전자기록의 정확하고 완전한 사본을 생성할 수 있는가?
- 시스템 접근 권한 (ID, 암호)을 설정하였는가?
- 시스템 관련 기록을 포함하여 정확한 기록을 보관했는가?
- 기록의 보존기간 동안 의도적이거나 우발적인 손실, 손상(and/or 변경)으로부터 보호되고 있는가?
- 저장된 데이터는 보존기간 내 복원성, 정확성이 보존기간 동안 검증되었는가?
- 시스템에 수동으로 입력 한 데이터 값이 정확 한가?

---

<sup>5</sup> ISPE. (2018) GAMP RDI Good Practice Guide: Data Integrity - Key Concepts

- 시스템 점검기록(Audit Trail)이 잘 기록 되고 있는가? (전자 기록을 작성, 수정, 삭제 항목에 날짜 및 시간이 기록이 작성되고 수정 사항 변경 사유가 함께 기록되어 있는지 확인한다.)
- 전자서명이 적용될 경우 전자서명에 이름, 서명일시, 서명의 의미가 포함되어 있는가?
- 전자서명은 복사/위조/변조가 불가능하며 전자기록과 연결되어 있는가?
- 시스템의 전자 서명은 실제 소유자만 사용할 수 있도록 식별 코드 및 암호와 같은 고유한 형식으로 구성되었는가?

○ Process Checklist

- 업무를 수행하기 위한 적절한 자격, 접근 수준 및 정의된 책임이 명시되어 있거나 시스템의 교육을 수행하기 위한 절차가 있는가?
- 중요한 전자 기록의 사본을 검토, 복사하는 절차를 마련하였는가?
- 저장된 데이터에 접근성, 내구성, 및 정확성 절차가 수립되었는가?
- 데이터의 Life Cycle 단계별로 관리 절차가 수립되어 있는가?
- 허가된 직원만 입력된 데이터를 수정할 수 있는가?
- Audit Trail 정보는 전자 기록에 필요한 기간만큼 보존되고 Audit Trail 을 검토할 절차가 수립되었는가?
- 시스템 접근 기록은 프로세스의 중요도를 기반으로 주기적으로 검토되고 있는가?
- 시스템 관리자 접근 규제 대상은 최소한의 인원으로 제한되었는가? (시스템 관리자 권한을 가진 작업자는 Audit Trail 의 조치를 할 수 있는가?)
- 시스템 관리자 접근에 수행되는 (시스템 접근 변경, 구성 변경, 데이터 이동, 데이터 삭제 등) 품질 시스템 내에서 승인이 되고 있는가?
- 전자서명이 적용될 경우 서명자는 전자서명에 대한 책임을 인지하고 있는가?
- 전자 서명은 한 개인에게만 주어지는가? (재사용, 재 할당되지 않은가?)
- 두 개인이 식별 코드와 암호의 동일한 조합을 가지고 있지 않은가?
- 전자 서명의 기밀 구성요소는 제대로 작동하고 무단으로 변경되지 않는가?
- 암호 발급을 주기적으로 점검 또는 개정을 하고 있는가?
- 암호 만료 절차를 설정하였는가?
- 분실, 도난, 손상되는 장치를 전자적으로 비활성화 하고 임시 또는 영구 교체를 발행하기 위한 암호정보 관리 절차를 수립하였는가?

## 5) 데이터 생애주기(Data Life Cycle) 별 필수요건 - 수기데이터

### 가) 수기데이터의 완전성을 위한 가이드라인(안)

#### ○ 데이터 생성(작성)

- 기록을 작성하는 사람은 다음의 원칙을 지켜야 한다.
  - 이면지나 접착식 메모지 등에 임시로 기록을 작성했다가 옮겨 적지 않는다.
  - 기존 페이지의 뒷면(원래 사용이 의도되지 않은 면)에 임의로 내용을 추가하지 않는다.
  - 기록하는 내용은 해당되는 작업/ 시험 절차 순서와 동일하게 시간 순으로 작성한다.
  - 기록 시점은 가능한 작업과 동시에, 실시간으로 작성되어야 한다.
  - 기록을 마감할 때 빈 칸이 남아있는지 확인하고 더 이상 작성할 내용이 없는 빈 칸에는 대각선으로 줄을 그어 추가 기입을 방지한다.
  - 모호하거나 알 수 없는 기호나 사전에 협의되지 않은 약어를 사용하지 않는다.
  - 연필이나 수성펜 등 지워지기 쉬운 필기구를 사용하지 않는다.
  - 날짜 기록 방식은 사전에 정해진 방법을 따른다. (년월일 순서 및 자릿수 등)
  - 소수점 기재 방식, 반올림 규칙 등은 사전에 정해진 방법을 따른다.
  - 저울, pH 측정기 등에서 생성되는 원본 데이터를 첨부해야 할 경우 원본 기록에 서명하고 날짜를 기입해야 한다.
  - 작성자가 누구인지 확인할 수 있도록 서명해야 한다.
  - 만일 작업의 특성 때문에 (무균 작업 등) 작업과 동시에 (실시간으로) 작성할 수 없거나, 제 2의 사람이 기록을 담당하게 된다면 기록의 위임이나 시간 차에 대하여 사전에 명문화해야 한다.
  - 사전에 등록된 서명을 사용해야 한다. 필요 시 약식 서명을 추가로 등록할 수 있다.
  - 기록서가 여러 날에 걸쳐 작성되도록 의도된 경우 서명 날짜를 기입한다.
- 기록서 양식은 다음의 사항이 보증되어야 한다.
  - 기록을 위한 충분한 여백이 제공되어야 한다.
  - 기록이 나타내는 작업/ 시험의 순서를 반영한 합리적인 디자인을 갖춰야 한다.
  - 모든 페이지마다 해당 양식의 유효성을 확인할 수 있는 다음의 정보를 갖춰야 한다.

- 전체 페이지 수와 해당 페이지 순서
- 등록된 양식 번호와 버전 정보
- 시행일자
- 페이지가 나중에 추가되는 경우 추가된 페이지 수를 기존 양식에 기재할 수 있다.
- 참조: PIC/S 8.6, 8.9, MHRA 5.2, WHO 11.2

#### ○ 데이터 수정

- 수정할 내용은 한 줄로 그어 원래 내용이 무엇인지 확인할 수 있게 해야 한다.
- 수정 사유와 날짜, 수정한 사람 이름을 함께 기재하여 추적성을 보증할 수 있어야 한다.
- 수정액을 사용하여 완전히 덮어버리거나 잉크로 까맣게 덮어 칠하거나, 찢어내어 원래 내용이 무엇인지 추적할 수 없게 하는 행위는 금지된다.
- 컴퓨터로 생성된 점검기록이 충분하지 않을 경우 수기로 컴퓨터 기록을 보충할 수 있다. 이 경우 해당 양식은 권한이 부여된 사람에 의해 발행된 것을 사용하도록 해야 한다.
- 참조: PIC/S 8.7, WHO 11.2 (예 8)

#### ○ 데이터 배포 및 관리

- 데이터의 중요도에 따라, 특히 컴퓨터 시스템으로 보증할 수 없는 점검기록(Audit Trail)을 보충하는 수기 기록서의 경우 발행 권한이 적절히 통제되어야 한다.
- 발행되었다가 사용하지 않게 된 기록서는 적시에 회수되어 기록의 중복 작성, 오작성을 방지해야 한다.
- 통제된 절차에 의해 발행된 기록서는 유효성을 식별할 수 있도록 서명이나 천공, 스탬핑, 색깔이 다른 용지 등을 사용할 수 있다.
- 데이터의 중요도에 따라 복사한 데이터의 배포 및 회수, 폐기 내역을 기록할 수 있다.
- 외부업체와 복사본을 교신할 경우 사본의 정확성을 검토할 절차를 마련해야 한다.
- 참조: PIC/S 8.4, 8.10

○ 데이터 검토<sup>6</sup>

- 시험실에서 발생한 원본 기록은 시험 후 지정된 담당자가 검증(Verify)해야 한다.
- 검토자는 데이터의 적합성을 이해할 수 있는 적절한 사람이어야 한다.
- 2차 검토의 범위는 생성된 데이터의 중요도를 기준으로 정할 수 있다.
- 2차 검토는 계산법 검증을 포함한다.
- 검토 결과 데이터의 오류를 발견할 경우 조사 방법과 조치할 사항을 정하는 절차가 있어야 한다.
- 참조: PIC/S 8.8, MHRA 6.15

○ 문서 아카이빙

- 보관 기록을 단계별로 설명하는 절차가 있어야 한다. (보관위치 지정, 보관함 식별 방법, 보관 기간 등)
- 보관되는 기록은 접근이 제한되어야 한다.
- 정해진 보관기간 동안 문서의 손상이나 유실을 방지할 수 있어야 한다.
- 참조: PIC/S 8.12, MHRA 6.17, WHO 11.2

○ 데이터 폐기

- 원본 기록을 폐기할 때에는 정해진 절차에 따라 폐기하고 그 내역을 추적할 수 있어야 한다.
- 폐기는 적절한 사람의 승인에 의해 시행되어야 한다.
- 폐기 내역을 작성해야 한다.
- 의도하지 않은 문서를 폐기할 위험을 방지할 절차가 있어야 한다.
- 보존기간은 법적 요구사항보다 짧지 않아야 한다.
- 필요 시 충분한 사본 데이터를 확보하는 것이 권장될 수 있다.
- 참조: PIC/S 8.13, MHRA 6.17

---

<sup>6</sup> 원문 verification of record (secondary checks)

## 나) 연구개발 실험실의 데이터 완전성 및 기록관리를 위한

### 표준운영절차

(Standard Operation Procedure for Data Integrity at Research and Development Laboratory)

#### 1. 목적 (Purpose)

1.1 OOO 연구소에서 생성되는 중요 기록에 대한 관리 절차를 정의함으로써 데이터 완전성을 보장하기 위함

#### 2. 적용범위 (Scope)

2.1 데이터의 중요도 및 위험도 평가 결과에 따라 정한다. 평가 방법은 form-####을 따른다.

2.2 기록의 형태에 따른 적용범위

2.2.1 손으로 작성되거나 출력물로 제공되는 원본 데이터에 적용한다.

2.2.2 컴퓨터 시스템에서 생성되는 전자데이터는 SOP-####을 따른다.

2.3 외부업체나 본사와 주고받는 기록의 경우 수신자가 서명하는 스캔본을 원본으로 할 수 있다.

#### 3. 책임 (Responsibilities)

3.1 데이터 완전성 책임자 (프로세스 책임자/부서)

3.1.1 2.1 항에 따라 선정된 관리 대상 기록의 전 생애주기 동안 데이터 완전성이 보증되는지 본 절차서에 따라 정기적으로 감독할 책임이 있다. 관리 감독의 형태는 자체 감사나 집체식 교육을 포함할 수 있다.

3.1.2 직원의 수기서명을 등록하고 관리한다.

3.1.3 발행 및 회수, 폐기 대상 기록서를 관리한다.

3.1.4 중요한 기록의 보존기간 동안 보관구역의 접근을 제한하고 보관 중인 기록의 현황과 반/출입 내역을 관리한다.

3.1.5 데이터의 중요도 및 위험도 평가를 주도한다.

3.1.6 데이터 완전성 원칙에 위반되는 사항을 발견할 경우 조사를 주도하고 결과에 대해 경영진에게 보고한다.

### 3.2 시험 책임자

#### 3.2.1 적격한 기록 검토자를 지정한다.

### 3.3 경영진

#### 3.3.1 기록 및 데이터의 완전성을 보증할 수 있는 독립적인 직무를 설계하고 지원한다.

#### 3.3.2 데이터 위변조 확인 시 그 위험도에 따라 보건당국 또는 파트너십 업체에 즉시 보고한다.

## 4. 용어의 정의 (Definitions)

상기 용어의 정의 (라. 2))항 참조

## 5. 절차 (Procedures)

### 5.1 직원 교육

#### 5.1.1 데이터에 직간접적으로 기여하는 모든 직원은 데이터 관리 정책에 대한 매년 n 회 교육을 이수해야 한다.

#### 5.1.2 교육 결과는 문서화된 평가 기록을 포함해야 한다. 평가 결과가 미흡할 시 재교육을 진행한다.

### 5.2 기록 작성

#### 5.2.1 기록을 작성하는 사람은 다음의 원칙을 지켜야 한다.

##### 5.2.1.1 이면지나 접착식 메모지 등에 임시로 기록을 작성했다가 옮겨 적지 않는다.

##### 5.2.1.2 기존 페이지의 뒷면(원래 사용이 의도되지 않은 면)에 임의로 내용을 추가하지 않는다.

##### 5.2.1.3 기록하는 내용은 해당되는 작업/ 시험 절차 순서와 동일하게 시간 순으로 작성한다.

##### 5.2.1.4 기록 시점은 가능한 작업과 동시에, 실시간으로 작성되어야 한다.

##### 5.2.1.5 기록을 마감할 때 빈 칸이 남아있는지 확인하고 더 이상 작성할 내용이 없는 빈 칸에는 대각선으로 줄을 그어 추가 기입을 방지한다.

##### 5.2.1.6 모호하거나 알 수 없는 기호나 사전에 협의되지 않은 약어를 사용하지 않는다.

##### 5.2.1.7 연필이나 수성펜 등 지워지기 쉬운 필기구를 사용하지 않는다.

##### 5.2.1.8 날짜 및 시간 기록 방식은 다음과 같다.

##### 5.2.1.8.1 YYYY.MM.DD

5.2.1.8.2 HH.MM (24 시간제 표기를 원칙으로 하되, 출력된 값의 설정이 이와 다를 시 메모를 남겨 혼동을 방지한다.)

5.2.1.9 소수점 기재 방식, 반올림 규칙 등은 SOP-#### 에 따른다.

5.2.1.10 저울, pH 측정기 등에서 생성되는 원본 데이터를 첨부해야 할 경우 원본 기록에 서명하고 날짜를 기입해야 한다.

5.2.1.11 작성자가 누구인지 확인할 수 있도록 서명해야 한다.

5.2.1.12 만일 작업의 특성 때문에 (무균 작업 등) 작업과 동시에 (실시간으로) 작성할 수 없거나, 제 2 의 사람이 기록을 담당하게 된다면 기록의 위임이나 시간 차에 대하여 사전에 정의하는 절차가 있어야 한다.

5.2.1.13 사전에 등록된 서명을 사용해야 한다. 필요 시 약식 서명을 추가로 등록할 수 있다.

5.2.1.14 기록서가 여러 날에 걸쳐 작성되도록 의도된 경우 서명 날짜를 기입한다.

5.2.2 기록서 양식은 다음의 사항이 보증되어야 한다.

5.2.2.1 기록을 위한 충분한 여백이 제공되어야 한다.

5.2.2.2 기록이 나타내는 작업/시험의 순서를 반영한 합리적인 디자인을 갖춰야 한다.

5.2.2.3 모든 페이지마다 해당 양식의 유효성을 확인할 수 있는 다음의 정보를 갖춰야 한다.

5.2.2.3.1 전체 페이지 수와 해당 페이지 순서

5.2.2.3.2 등록된 양식 번호와 버전 정보

5.2.2.3.3 시행일자

5.2.2.3.4 페이지가 나중에 추가되는 경우 추가된 페이지 수를 기존 양식에 기재할 수 있다.

5.2.3 기록 수정 방식

5.2.3.1 수정할 내용은 한 줄로 그어 원래 내용이 무엇인지 확인할 수 있게 해야 한다.

5.2.3.2 수정 사유를 함께 기재해야 한다.

5.2.3.3 수정한 사람을 확인할 수 있어야 한다.

5.2.3.4 수정액을 사용하여 완전히 덮어버리거나 잉크로 까맣게 덮어 칠하거나, 찢어내어 원래 내용이 무엇인지 추적할 수 없게 하는 행위는 금지된다.

5.2.3.5 컴퓨터로 생성된 점검기록이 충분하지 않을 경우 수기로 작성된 기록으로 보충할 수 있다. 이 경우 해당 양식은 권한이 부여된 사람에 의해 발행된 것을 사용하도록 해야 한다.

5.2.4 기록서 발행 (필요 시)

5.2.4.1 기록서 필요 시 사전에 데이터 완전성 책임자에게 발행을 요청한다.



5.2.4.2 데이터 완전성 책임자는 등록된 양식을 출력하고 필요 시 바인딩하여 페이지의 손실과 교체를 방지한다.

5.2.4.3 표지에 고유번호를 기재하고 발행자 서명을 한다.

5.2.4.4 발행되었다가 사용하지 않게 된 기록서는 적시에 회수되어 기록의 중복 작성, 오작성을 방지해야 한다.

5.2.4.5 회수된 데이터 완전성 책임자에 의해 파기되고 그 내역과 사유도 기록해야 한다.

### 5.3 기록 배포

5.3.1 복사한 데이터의 배포 시 사본이 원본과 동일한지 확인한 뒤 배포자 확인 서명을 해야 한다.

5.3.2 데이터의 중요도에 따라 복사한 데이터의 배포 및 회수, 폐기 내역을 기록할 수 있다.

5.3.3 외부업체와 복사본을 교신할 경우 수신인은 데이터의 정확성을 확인하였음을 서명해야 한다.

### 5.4 기록 검토

5.4.1 시험실에서 발생한 원본 기록은 시험 후 지정된 담당자가 검증(Verify)해야 한다.

5.4.2 검토자는 데이터의 적합성을 이해할 수 있는 적격한 사람이어야 한다.

5.4.3 2차 검토의 범위와 주기는 생성된 데이터의 중요도를 기준으로 정할 수 있다.

5.4.4 2차 검토는 계산법 검증을 포함한다.

5.4.5 검토 결과 데이터의 오류를 발견할 경우 조사 방법과 조치할 사항은 SOP-###을 따른다.

### 5.5 기록 보존

5.5.1 당사의 기록 보존기한과 장소는 첨부##을 참조한다.

5.5.2 보관소에 최초 반입 시 다음의 정보를 표지로 만들어 기재해야 한다.

5.5.2.1 기록서의 제목

5.5.2.2 고유번호 (보관구역의 캐비닛 번호나 순번에 따를 수 있다)

5.5.2.3 기록담당 부서

5.5.2.4 기록이 생성된 날짜 또는 연월

5.5.2.5 보존기한

5.5.2.6 기타 기록 식별에 필요한 정보

5.5.3 보관소에 한 번 반입된 기록서는 열람 및 반출에 데이터 완전성 담당자의 승인이 있어야 한다.

5.5.4 기록 보관실은 해충 및 자연부식, 재해(화재 등)을 방지할 수 있는 시스템을 갖춰야 한다.

5.5.5 필요 시 기록 보관실의 온습도를 점검해야 한다.

## 5.6 기록 폐기 (파기)

5.6.1 정기적으로 보존기간을 경과한 원본 기록의 폐기 필요성을 검토한다.

5.6.2 폐기는 데이터 완전성 책임자 및 관련 부서 책임자의 승인 이후에 실시해야 한다.

5.6.3 데이터 완전성 책임자는 정기적으로 폐기 대상 기록서를 수거하여 폐기를 실시하고 해당 내역을 기록해야 한다.

5.6.4 폐기 실시내역은 정기적으로 검토 되어야 한다.

5.6.5 폐기를 시행할 때 의도하지 않은 데이터가 우발적으로 폐기되지 않도록 교차점검을 실시해야 한다.

## 6. 참고문헌

6.1 교육관리 절차

6.2 일탈관리 절차

6.3 문서관리 절차

6.4 시험데이터 관리 절차

6.5 컴퓨터화 시스템의 데이터 완전성 관리 절차

## 7. 첨부

7.1 기록 중요도 및 위험평가서

7.2 직원 서명관리대장

7.3 기록 보관구역 평면도

7.4 기록보관소 반출입대장

7.5 기록보관현황표

7.6 기록 배포관리대장

7.7 기록 폐기대장

7.8 기록서 발행대장

7.9 기록 보존기한 표

7.10 데이터 완전성 점검 기록서

## 다) 수기 작성 기록의 관리를 위한 체크리스트

- GxP 에 영향을 주는 기록을 작성하는 직원의 수기 서명은 모두 등록되어 있는가?
- 모든 중요한 데이터는 등록된 양식에 작성되고 있는가?
- 항상 유효한 양식의 버전을 사용하고 있는가?
- 사용을 완료한 기록서의 공란에 더 이상 사용하지 않음을 나타내는 표기를 하는가?
- 날짜와 시간 표시, 반올림 및 소수점 작성 방법은 통일성 있게 지켜지는가?
- 첨부된 원본 데이터에 확인 서명이 되어 있는가?
- 모든 중요 데이터/ 기록의 작성자가 누구인지 알 수 있는가?
- 수정 시 원래 내용과 사유, 수정자를 알 수 있게 기입하는가?
- 중요 데이터의 이중 점검(2 차 검토)은 적격한 사람에 의해 이루어지고 있는가?
- 발행관리가 필요한 양식의 경우 권한이 있는 사람에 의해 통제되고 있는가?
- 모든 기록서는 각 페이지마다 고유번호와 페이지 번호를 확인할 수 있는가?
- 원본 기록서 보관소의 출입권한을 제한하고 있는가?
- 원본 기록서 보관소의 반출입 및 폐기 내역을 작성하는가?
- 원본 기록서 보관소에 화재방지 시스템 등 물리적 훼손을 방지할 수 있는 시스템이 있는가?

## 6) 외주업체(External Partner)의 관리

### 가) 외주업체(External Partner)의 관리를 위한 가이드라인(안)

- 외주기관 (연구개발과정에서 단위의 시험을 분리된 전문회사에 시행을 의뢰하는 경우, 아웃소싱) 및 협력기관 (연구 개발과정에서 다른 연구기관이나 업체와 협력관계로 일하는 경우)과 연구를 수행하는 경우에는 의뢰하는 연구의 특징이나 중요도에 따라 추후 GLP 나 GMP 의 규제적 관리대상이 되는 지 사전에 검토한다.
- 외주 연구의 중요도에 대한 검토의 결과를 근거로 하여 외주업체와 사전에 연구의 품질(research quality)에 대한 기대치(expectation)에 대해 공식적으로 합의하고, 그 내용을 계약서 (협약서)에 기록한다.
- 연구수행의 품질에 책임을 가진 담당자를 지정한다.
- 연구의 품질에 대한 기대치에는 데이터 완결성, 추적관리와 데이터의 보안에 대한 내용을 포함한다.
- 참고 PIC/S 10.1.1, 10.1.2, 10.1.3, 10.2.1, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6 WHO 2.5, 7.1, 7.2, 7.3, 7.4, 7.5 MHRA 6.15

## 나) 외주업체(External Partner)의 관리를 위한 체크리스트

- 외주업체에서 실험기록서 (전자형태 등)를 쓰고 있는가?
- 외주업체에서 원본데이터의 관리와 저장은 적절하게 되고 있는가? (주기적인 시스템 확인 등 검증 업무)
- 외주업체의 데이터 관리는 FAIR 원칙(findable 확인, accessible 가용, interoperable 상호사용, reusable 재사용)에 맞게 유지되고 있는가?
- 외주업체가 데이터 완전성과 관련한 부서 (담당자)를 지정하고 있는가?
- 외주업체의 데이터의 보안은 적절한가?
- 외주업체와 계약당사자 기관과의 데이터 교환 시 투명하게(숨김없이) 확인할 수 있도록 보장되는가?
- 외주업체의 실험결과보고서에서 서술보고하고 있는 결과와 관련된 연구 및 연계된 연구의 모든 원본데이터의 결과를 보거나 확인할 수 있도록 되어 있는가?