

EUROPEAN COMMISSION

ENTERPRISE AND INDUSTRY DIRECTORATE-GENERAL

Brussels,

SANCO/C8/AM/sl/ares(2010)1064599

EudraLex

The Rules Governing Medicinal Products in the European Union

Volume 4

Good Manufacturing Practice Medicinal Products for Human and Veterinary Use

Annex 11: Computerised Systems

Legal basis for publishing the detailed guidelines: Article 47 of Directive 2001/83/EC on the Community code relating to medicinal products for human use and Article 51 of Directive 2001/82/EC on the Community code relating to veterinary medicinal products. This document provides guidance for the interpretation of the principles and guidelines of good manufacturing practice (GMP) for medicinal products as laid down in Directive 2003/94/EC for medicinal products for human use and Directive 91/412/EEC for veterinary use.

세부 가이드라인 발행의 법적 근거: 사람 의약품 관련 EC 법률에 관한 디렉티브 2001/83/EC의 제47조와 동물 의약품 관련 EC 법률에 관한 디렉티브 2001/82/EC의 제51조. 이 문서는 사람 의약품에 대한 디렉티브 2003/94/EC와 동물 의약품에 대한 디렉티브 91/412/EEC에 제시된 의약품 GMP 원칙과 가이드라인의 해석과 지침을 제공한다.

Status of the document: revision 1

문서 상태: 1개정

Reasons for changes: the Annex has been revised in response to the increased use of computerised systems and the increased complexity of these systems. Consequential amendments are also proposed for Chapter 4 of the GMP Guide.

변경 이유: 컴퓨터화 시스템의 사용 증가 및 컴퓨터화 시스템의 복잡성 증가에 따라 이 부록을 개정한다. 이에 따라 GMP 가이드 4장의 개정도 추진한다.

Deadline for coming into operation: 30 June 2011

시행일자: 2011년 6월 30일

gmpeye

원칙(Principle)

This annex applies to all forms of computerised systems used as part of a GMP regulated activities. A computerised system is a set of software and hardware components which together fulfill certain functionalities.

이 부록은 GMP 규제 대상 활동에 사용되는 모든 종류의 컴퓨터화 시스템에 적용된다. 컴퓨터화 시스템은 소프트웨어와 하드웨어 컴포넌트로 구성되어 특정 기능을 수행하는 것이다.

The application should be validated; IT infrastructure should be qualified.

애플리케이션을 밸리데이션한다. IT 인프라스트럭처의 적격성평가를 실시한다.

Where a computerised system replaces a manual operation, there should be no resultant decrease in product quality, process control or quality assurance. There should be no increase in the overall risk of the process.

컴퓨터화 시스템이 수동 작업을 대체하는 경우, 제품 품질, 공정 관리 또는 품질 보증의 저하가 발생해서는 안 된다. 공정의 전반적인 리스크가 증가하지 않아야 한다.

공통(General)

1. 리스크 관리(Risk Management)

Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system.

환자 안전, 데이터 완전성, 제품 품질을 고려하여, 컴퓨터화 시스템의 라이프사이클 전체에 걸쳐 리스크 관리를 적용한다. 리스크 관리 시스템에 따라, 컴퓨터화 시스템의 리스크 평가를 타당하게 실시하고 문서화하며, 평가 결과에 근거하여 밸리데이션과 데이터 완전성 관리 수준을 결정한다.

2. 작업자(Personnel)

There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT. All personnel should have appropriate

qualifications, level of access and defined responsibilities to carry out their assigned duties.

공정 책임자, 시스템 책임자, QP, IT 등 모든 관련자가 긴밀하게 협력해야 한다. 모든 작업자가 지정 업무를 수행하는데 적절한 자격을 갖추어야 하며, 작업자 접근 수준과 책임을 규정한다.

3. 공급업체와 서비스 제공업체(Suppliers and Service Providers)

3.1 When third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerised system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT-departments should be considered analogous.

예를 들어 컴퓨터화 시스템 또는 관련 서비스의 제공, 설치, 구성, 통합, 밸리데이션, 유지관리(예, 원격 접속 방식), 변경 또는 유지나 데이터 처리에 제3자(예, 공급업체, 서비스 제공업체)를 활용한다면, 제조업체와 제3자 사이에 공식 계약서를 체결하고 제3자의 책임을 계약서에 명확하게 규정한다. IT 부서도 이와 유사한 곳으로 간주한다.

3.2 The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment.

제품 또는 서비스 제공업체 선정 시에 중요하게 고려해야 할 요소가 공급업체의 역량과 신뢰성이다. 리스크 평가 결과를 바탕으로 감사의 필요성을 결정한다.

3.3 Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.

COTS 제품과 함께 제공되는 문서를 규제 대상 사용자가 검토하고 사용자의 요구 기준에 부합하는지 확인한다.

3.4 Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.

소프트웨어와 구축 시스템의 공급업체 또는 개발자와 관련된 품질 시스템 및 감사 정보를 실사자가 요청하는 경우에 제공할 수 있어야 한다.

프로젝트 단계(Project Phase)

4. 밸리데이션(Validation)

- 4.1 The validation documentation and reports should cover the relevant steps of the life cycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment.

관련 라이프사이클 단계에서 밸리데이션 문서와 보고서를 작성한다. 제조업체는 리스크 평가 결과에 근거하여 표준, 프로토콜, 허용 기준, 절차, 기록의 타당성을 입증할 수 있어야 한다.

- 4.2 Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.

변경 관리 기록(해당되는 경우)과 밸리데이션 과정에서 발생한 일탈에 관한 보고 자료를 밸리데이션 문서에 포함시킨다.

- 4.3 An up to date listing of all relevant systems and their GMP functionality (inventory) should be available.

모든 관련 시스템과 GMP 기능을 정리한 최신 리스트(인벤토리)를 구비한다.

For critical systems an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available.

중요한 시스템인 경우에는 물리적/논리적 배치, 데이터 흐름, 다른 시스템이나 프로세스와의 인터페이스, 하드웨어와 소프트웨어 전제 조건, 보안 대책을 자세히 기술한 최신 시스템 기술 문서를 구비한다.

- 4.4 User Requirements Specifications should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the life-cycle.

컴퓨터화 시스템의 필수 기능을 기술한 URS가 있어야 한다. URS는 리스크 평가 결과와 GMP 영향 평가 결과를 바탕으로 작성한다. 사용자 요구 기준을 라이프사이클 전체에 걸쳐 추적 관리한다.

- 4.5 The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately.

규제 대상 사용자는 적절한 품질 경영 시스템에 의거하여 시스템이 개발되도록 합리적인 모든 조치를 취해야 한다. 공급업체를 적절하게 평가한다.

- 4.6 For the validation of bespoke or customised computerised systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the life-cycle stages of the system.

베스포크 또는 맞춤 컴퓨터화 시스템의 밸리데이션인 경우, 시스템의 전체 라이프사이클 단계에 걸쳐 품질/성능 요소의 공식 평가 및 보고 절차를 구비한다.

- 4.7 Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered. Automated testing tools and test environments should have documented assessments for their adequacy.

시험 방법과 시험 시나리오의 적절성에 관한 증거를 구비한다. 특히 시스템(공정) 파라미터 기준, 데이터 기준, 오류 처리 등을 고려한다. 자동화 시험 도구와 시험 환경의 적절성을 평가하고 문서화한다.

- 4.8 If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process.

데이터를 다른 데이터 형식이나 시스템으로 이전하는 경우, 이 마이그레이션 과정에서 데이터의 값 및/또는 의미가 달라지지 않았는지 확인하는 점검을 포함하여 밸리데이션을 실시한다.

운영 단계(Operational Phase)

5. 데이터(Data)

Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks.

다른 시스템과 전자적으로 데이터를 교환하는 컴퓨터화 시스템은, 정확하고 안전한 데이터 입력과 처리를 확인하는 빌트인 점검 기능을 적절하게 구비하여 리스크를 최소화한다.

6. 정확성 점검(Accuracy Checks)

For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management.

중요한 데이터를 수동으로 입력하는 경우, 데이터의 정확성을 추가로 점검한다. 이 점검을 다른 작업자가 하거나 밸리데이션된 전자적 수단으로 할 수 있다. 잘못된 데이터나 정확하지 않은 데이터를 시스템에 입력함으로써 발생하는 결과와 중요성을 고려하여 리스크 관리를 실시한다.

7. 데이터 저장(Data Storage)

7.1 Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period.

물리적 수단과 전자적 수단을 모두 사용하여 데이터가 손상되지 않게 관리한다. 저장된 데이터의 접근성, 가독성, 정확성을 점검한다. 보관 기간 동안 데이터의 접근성을 확보한다.

7.2 Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically.

모든 관련 데이터를 정기적으로 백업한다. 백업 데이터의 완전성과 정확성, 그리고 데이터 복원 능력을 밸리데이션 시에 점검하고 주기적으로 모니터링한다.

8. 인쇄물(Printouts)

8.1 It should be possible to obtain clear printed copies of electronically stored data. 전자적으로 저장된 데이터의 명확한 인쇄 사본을 확보할 수 있어야 한다.

8.2 For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry.

배치 출하 승인을 뒷받침하는 기록인 경우, 최초 입력 이후에 데이터가 변경되었는지 보여 주는 인쇄물을 만들 수 있어야 한다.

9. 감사 추적(Audit Trails)

Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.

리스크 평가 결과에 근거하여, 모든 GMP 관련 변경 및 삭제 기록을 생성하는 기능을 시스템에 통합시키는 것을 고려해야 한다(시스템 생성 "감사 추적"). GMP 관련 데이터를 변경하거나 삭제하는 경우에는 이유를 문서화한다. 감사 추적 데이터를 활용할 수 있고 이 데이터를 일반적으로 이해되는 형식으로 전환하며 정기적으로 검토할 필요가 있다.

10. 변경 관리와 구성 관리(Change and Configuration Management)

Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure.

시스템 구성을 포함하여 컴퓨터화 시스템의 모든 변경을 지정 절차에 따라 관리하며 추진한다.

11. 주기적 평가(Periodic evaluation)

Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.

컴퓨터화 시스템을 주기적으로 평가하여, 유효한 상태로 유지되고 GMP 기준에 부합하는지 확인한다. 적절한 경우에는 현재 기능 범위, 일탈 기록, 인시던트, 문제, 업그레이드 이력, 성능, 신뢰성, 보안, 밸리데이션 상태 보고 등을 평가한다.

12. 보안(Security)

12.1 Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.

허가 받은 사람만 컴퓨터화 시스템에 접근할 수 있도록, 물리적 및/또는 논리적 관리 대책을 구비한다. 시스템의 무허가 접근을 방지하는데 적합한 방법으로는, 키, 패스 카드, 개인 코드와 패스워드, 생체 인증, 컴퓨터 설비와 데이터 저장 지역의 접근 제한 등이 있다.

12.2 The extent of security controls depends on the criticality of the computerised system.
컴퓨터화 시스템의 중요도에 따라 보안 관리 수준을 정한다.

12.3 Creation, change, and cancellation of access authorisations should be recorded.
접근 허가 권한의 생성, 변경, 취소 정보를 기록한다.

12.4 Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.
일자과 시간을 포함하여 데이터를 입력, 변경, 확인, 삭제한 사람의 정보를 기록할 수 있게 데이터와 문서의 관리 시스템을 설계한다.

13. 인시던트 관리(Incident Management)

All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.

시스템 이상과 데이터 오류를 포함한 모든 인시던트를 보고하고 평가한다. 중요 인시던트의 근본 원인을 파악하고, 이를 바탕으로 시정/예방 조치를 추진한다.

14. 전자 서명(Electronic Signature)

Electronic records may be signed electronically. Electronic signatures are expected to: 전자 기록서에 전자적으로 서명할 수 있다. 전자 서명은 다음 기준에 부합해야 한다.

- a. have the same impact as hand-written signatures within the boundaries of the company,
회사 내부에서는 수기 서명과 동일한 의미를 갖는다.
- b. be permanently linked to their respective record,

해당 기록에 영구적으로 연계된다.

- c. include the time and date that they were applied.
서명 일자와 시간을 포함한다.

15. 배치 출하 승인(Batch release)

When a computerised system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches. This should be performed using an electronic signature.

증명 및 배치 출하 승인을 기록하는데 컴퓨터화 시스템을 사용한다면, QP만 배치의 출하 승인을 증명할 수 있는 시스템이어야 하며, 배치의 출하를 승인하거나 증명한 자를 명확하게 파악하고 기록할 수 있어야 한다. 전자 서명으로 실시되어야 한다.

16. 비즈니스 연속성(Business Continuity)

For the availability of computerised systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system). The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.

중요 공정을 지원하는 컴퓨터화 시스템의 가용성 유지를 위해, 시스템 고장에 대비하여 중요 공정의 계속적 지원을 보증하는 대책(예, 수동 시스템 또는 대체 시스템)을 구비한다. 대체 방안을 적용하는데 걸리는 시간은 리스크를 바탕으로 정하며, 해당 시스템과 그 시스템이 지원하는 비즈니스 절차에 적절해야 한다. 이러한 대응 방안을 적절하게 문서화하고 시험한다.

17. 아카이브(Archiving)

Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested.

데이터를 아카이브할 수 있다. 이 데이터의 접근성, 가독성, 완전성을 점검한다. 시스템을

변경한다면(예, 컴퓨터 설비나 프로그램), 데이터 검색 능력이 확보되어야 하며 이 능력을 시험한다.

용어 정의(Glossary)

애플리케이션(Application): Software installed on a defined platform/hardware providing specific functionality

지정 플랫폼/하드웨어에 설치되어 특정 기능을 제공하는 소프트웨어.

베스포크/맞춤 컴퓨터화 시스템(Bespoke/Customized computerised system): A computerised system individually designed to suit a specific business process
특정 비즈니스 절차에 맞춰 설계된 컴퓨터화 시스템

COTS 소프트웨어(Commercial of the shelf software): Software commercially available, whose fitness for use is demonstrated by a broad spectrum of users.
상업적으로 구입 가능하며 다양한 사용자를 통해 용도 적합성이 증명된 소프트웨어.

IT 인프라스트럭처(IT Infrastructure): The hardware and software such as networking software and operation systems, which makes it possible for the application to function.
애플리케이션의 기능을 가능하게 하는, 네트워킹 소프트웨어나 운영 체제 같은 소프트웨어와 하드웨어.

라이프사이클(Life cycle): All phases in the life of the system from initial requirements until retirement including design, specification, programming, testing, installation, operation, and maintenance.

디자인, 규격 설정, 프로그래밍, 시험, 설치, 운영, 유지관리를 포함하여, 초기 기준 설정부터 폐기까지 시스템의 일생을 구성하는 모든 단계.

공정 책임자(Process owner): The person responsible for the business process.
비즈니스 절차를 책임지는 자.

시스템 책임자(System owner): The person responsible for the availability, and maintenance of a computerised system and for the security of the data residing on that system.
컴퓨터화 시스템의 가용성 및 유지 관리, 그리고 그 시스템에 있는 데이터의 보안을 책임지는 자.

제3자(Third Party): Parties not directly managed by the holder of the manufacturing and/or import authorisation.

제조 및/또는 수입 허가 보유자가 직접적으로 관리하지 않는 자.

gmpeye