PHARMA SOLUTIONS

Валидация компьютеризированных систем

Филенко Т.Н.

План

- Нормативная база

Обзор действующих нормативных документов

- Термины и определения

Обзор применяемой профильной терминологии и определний.

- Приложении 11 GMP EU (обзор)

Общие указания, управление рисками, персонал, поставщики и провайдеры услуг, валидация, данные, проверка правильности, хранение данных, распечатки, аудит, изменение и управление конфигурацией, периодическая оценка, безопасность, управление инцидентами, электронная подпись, выпуск серии, непрерывность бизнеса, архивирование

- IT-инфраструктура.

Интерпретация понятия и краткий обзор

PHARMA SOLUTIONS

Валидация компьютеризированных систем

- Катерогии компьютеризированных систем.

Обзор категорий

- Необходимая документация.

User Requirements Specification (URS) – спецификация требований пользователя, проект, Functional Specification (FS) – функциональная спецификация, Technical Specification (TS) – техническая спецификация, Configuration Specification (CS) – конфигурационная спецификация.

- Этапы квалификации.

Рассмотрение необходимых этапов квалификации

- Валидационная документация (валидационный мастеплан (ВМП), валидационные протоколы и валидационные отчеты IQ/OQ/PQ).
- Базовый перечень испытаний.
- Заключение.

Нормативная база

- The Rules Governing Medicinal Products in the European Union. Volume 4. EU Guidelines to Good Manufacturing Practice Medicinal Products for Human and Veterinary Use. Annex 11. Computerised Systems. Rev. January 2011.

https://ec.europa.eu/health/sites/health/files/files/eudralex/vol-4/annex11_01-2011_en.pdf

- Guidance For Industry. 21 CFR Part 11. Electronic Records; Electronic Signatures. Validation.

https://www.fda.gov/ohrms/dockets/ac/02/briefing/3901B1_07_GFI-21CFRPart%2011-Validation.pdf

- General Principles of Software Validation; Final Guidance for Industry and FDA Staff

https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm085371.pdf

Нормативная база

- PIC/S Good Practices for Computerised Systems in Regulated "GXP" Environments (PI 011-3) Sept 2007

http://academy.gmp-compliance.org/guidemgr/files/PICS/PI%20011-3%20RECOMMENDATION%20ON%20COMPUTERISED%20SYSTEMS.PDF

- ISPE GAMP 5: A RISK-BASED APPROACH TO COMPLIANT GXP COMPUTERIZED SYSTEMS
- European Commission - The Rules Governing Medicinal Products in the European Union - Volume 4 - Annex 20: Quality Risk Management - March 2008 (Adoption as ICH Q9 guideline Step 4)

http://www.translation-centre.am/pdf/Translat/EU_Other/GMP_Rules/GMP_Rules_Annex_20_en.pdf

Нормативная база

- GAMP Forum – GAMP Good Practice Guide: The Validation of Legacy Systems, November/December 2003

http://www.sublimationscience.com/Validation/Regulatory%20Documents/LegacySystems.pdf

- GAMP Forum – GAMP Good Practice Guide, Testing of GxP Systems, July 2005
- GAMP Forum – GAMP Good Practice Guide, A Risk-Based Approach to Compliant Electronic Records and Signatures, April 2005
- GAMP Forum – GAMP Good Practice Guide, A Risk-Based Approach to Operation of GxP Computerized Systems, 2010

Нормативная база

- IEC 60601-1-4 Medical electrical equipment. Part 1-1. General requirements for safety. Safety requirements for medical electrical systems. April 1, 2000.
- IEC 61506:1997. Industrial-process measurement and control - Documentation of application software.
- IEC 61508. Functional safety of electrical/electronic/ programmable electronic safety-related systems. 1998.
- IEEE Std 1012. Standard for Software Verification and Validation.
- ISO/IEC 12119. Information technology -- Software packages -- Quality requirements and testing.
- ISO 14971. Medical devices -- Application of risk management to medical devices. Part 1: Application of Risk Analysis.

Нормативная база

- GUIDE TO INSPECTION OF COMPUTERIZED SYSTEMS IN DRUG PROCESSING. FEBRUARY, 1983. National Center for Drugs and Biologics and Executive Director of Regional Operations.

Термины и определения

Application: Software installed on a defined platform/hardware providing specific functionality (**Приложение**: Программное обеспечение, установленное на определенной платформе/компьютерном оборудовании и предоставляющее специальные функциональные возможности).

Bespoke/Customized computerised system: A computerised system individually designed to suit a specific business process (**Компьютеризированная система, изготовленная по индивидуальному заказу**: Индивидуально спроектированная компьютеризированная система для обеспечения конкретного рабочего процесса).

Commercial of the shelf software: Software commercially available, whose fitness for use is demonstrated by a broad spectrum of users

Термины и определения

(**Серийное программное обеспечение**: Коммерчески доступное программное обеспечение, пригодность которого для использования продемонстрирована большим количеством пользователей).

IT Infrastructure: The hardware and software such as networking software and operation systems, which makes it possible for the application to function (**Информационно-технологическая инфраструктура** (IT-инфраструктура): Компьютерное оборудование и программное обеспечение, такое как сетевое программное обеспечение и операционные системы, которые делают возможным функционирование приложений).

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

Термины и определения

(Жизненный цикл (lifecycle): Все стадии существования компьютеризированной системы от формирования первоначальных требований до прекращения эксплуатации, включая проектирование, определение технических требований, программирование, тестирование, установку, работу и обслуживание).

Process owner: The person responsible for the business process (**Владелец процесса**: Лицо, ответственное за рабочий процесс).

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 (**Владелец системы**: Лицо, ответственное за работоспособность и обслуживание компьютеризированной системы, а также за защиту находящихся в ней данных).

Термины и определения

Third Party: Parties not directly managed by the holder of the manufacturing and/or import authorisation (**Трети стороны**: Стороны, которые не находятся в прямом подчинении держателя лицензии на производство лекарственных средств).

Qualified Person (QP). The person defined in Article 48 of Directive 2001/83/EC, as amended, and Article 52 of Directive 2001/82/EC (**Уполномоченное лицо.** Лицо, определенное в Статье 48 Директивы 2001/83 / ЕС с внесенными в нее поправками и Статье 52 Директивы 2001/82 / ЕС.

В общем виде, это лицо, назначенное производителем лекарственных средств, которое осуществляет подтверждение соответствия лекарственных средств требованиям, установленным при их государственной регистрации, и гарантирует, что лекарственные средства произведены в соответствии с требованиями GMP)

Приложении 11 GMP EU

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.

Принцип

Данное Приложение применяется ко всем типам компьютеризированных систем, используемых в рамках деятельности, регулируемой требованиями GMP. Компьютеризированная система представляет собой набор программных и аппаратных компонентов, которые совместно выполняют определенные функции.

Приложении 11 GMP EU

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

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.

Применение компьютеризированной системы должно быть валидировано, информационно-технологическая инфраструктура должна пройти квалификацию.

Если компьютеризированная система заменяет ручное управление, это не должно приводить к снижению качества продукции, технологического контроля или обеспечения качества. Общие риски процесса не должны возрастать.

Приложении 11 GMP EU

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.

Управление рисками

Управление рисками должно применяться в течение жизненного цикла компьютеризированной системы и принимать во внимание безопасность пациентов, целостность данных и качество продукции. В рамках системы управления рисками решения по объему валидационных испытаний и проведению контролей целостности данных должны основываться на обоснованной и документально оформленной оценке рисков компьютеризированной системы.

Приложении 11 GMP EU

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.

Персонал

Следует поддерживать тесное сотрудничество между всем значимым персоналом, вовлеченным в данный процесс, таким как владелец процесса, владелец системы, Уполномоченные лица и технический (IT) персонал. Весь персонал должен иметь соответствующую квалификацию, уровень доступа и определенную ответственность для выполнения возложенных на него обязанностей.

Приложении 11 GMP EU

Suppliers and Service Providers

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.

Поставщики и провайдеры услуг

Если задействованы третьи лица (например, поставщики, провайдеры услуг) например, для поставки, установки, настройки, задания конфигурации, интегрирования, валидации, технического обслуживания (например, через удаленный доступ), модификации или поддержания компьютеризированных систем, связанных с ними услуг или обработки данных, то должны иметься надлежаще оформленные договоры между производителем и любыми третьими лицами. В этих договорах должна быть четко установлена ответственность третьих лиц. Аналогичные требования следует предъявлять к IT-подразделениям.

Приложении 11 GMP EU

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.

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

Компетентность и надежность поставщиков являются ключевыми условиями выбора провайдеров продукта или услуг (квалификация поставщика услуг). Необходимость аудита должна быть основана на оценке рисков.

Документация, прилагаемая к коммерчески выпускаемым готовым для использования программным продуктам, должна быть рассмотрена уполномоченными (регламентированными) пользователями на предмет соответствия требованиям пользователя (URS).

Приложении 11 GMP EU

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

Информация о системе качества и аудитах поставщиков или разработчиков программного обеспечения и имплементированных (установленных, реализованных, внедренных) компьютеризированных систем должна быть доступна для предоставления инспекторам по их требованию.

Приложении 11 GMP EU

Project Phase

Validation

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.

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

Стадия проекта. Валидация

Валидационная документация и отчеты должны охватывать соответствующие стадии жизненного цикла компьютеризированной системы.

Приложении 11 GMP EU

Производители должны быть способны обосновать свои стандарты, протоколы, критерии приемлемости, процедуры и записи на основе оценки рисков.

Валидационная документация должна включать записи контроля изменений (если применимо) и отчеты о любых отклонениях, выявленных в ходе процесса валидации (*процедура управления отклонениями*).

Приложении 11 GMP EU

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

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.

Должен быть в наличии актуальный перечень (реестр) всех используемых (имеющих отношение к делу) компьютеризированных систем с указанием их функционала в разрезе GMP.

Для критических компьютеризированных систем должны быть в наличии подробное текущее описание физических и логических взаимосвязей, потоков данных и интерфейсов с другими системами или процессами, требуемые ресурсы всего компьютерного оборудования и программного обеспечения, меры безопасности.

Приложении 11 GMP EU

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.

Спецификации требований пользователя должны описывать необходимые функции компьютеризированной системы на основе документально оформленной оценки рисков и влияния с точки зрения соблюдения GMP. Требования пользователя должны прослеживаться на протяжении всего жизненного цикла компьютеризированной системы.

Приложении 11 GMP EU

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.
Регламентированный пользователь должен предпринять все меры, гарантирующие, что компьютеризированная система разработана в соответствии с подходящей *(определенной)* системой управления качеством. Поставщик должен быть оценен соответствующим образом (*квалификация поставщика*).

Приложении 11 GMP EU

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.

С целью валидации компьютеризированных систем, изготовленных по индивидуальному заказу или модифицированных в соответствии с требованиями заказчика, следует разработать документированную процедуру *(процесс)* оценки качества и эксплуатационных характеристик компьютеризированной системы на всех этапах ее жизненного цикла с оформлением соответствующих отчетов.

Приложении 11 GMP EU

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.

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.

Следует представить доказательства соответствия методов и планов тестирования компьютеризированной системы. Особо тщательно должны быть рассмотрены пределы параметров системы (процесса), границы данных и обработка ошибок *(управление ошибками)*. Следует документально оформить оценку соответствия *(адекватности)* применения автоматизированных средств тестирования и режимов их работы.

Приложении 11 GMP EU

Если данные переводятся в другой формат или систему данных, валидация должна включать проверку неизменности количественных значений и/или смысла данных в процессе их миграции.

Operational Phase

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.

Стадия эксплуатации. Данные

Компьютеризированные системы, осуществляющие электронный обмен данных с другими системами, должны включать соответствующие встроенные средства контроля правильного и безопасного ввода и обработки данных с целью минимизации рисков.

Приложении 11 GMP EU

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.

Контроль точности

Для критических данных, вводимых вручную, следует предусмотреть дополнительный контроль точности ввода данных. Этот контроль может осуществляться вторым оператором или с помощью валидированных электронных средств. Критичность и потенциальные последствия ошибочного или неправильного ввода данных в систему должны охватываться системой управления рисками.

Приложении 11 GMP EU

Data Storage

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.

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.

Хранение данных

Данные должны быть защищены от повреждений как физическими, так и электронными мерами. Сохраненные данные должны проверяться на доступность, читаемость и точность. Доступ к данным должен быть обеспечен на протяжении всего периода их хранения.

Приложении 11 GMP EU

Следует выполнять регулярное резервное копирование всех необходимых данных. Сохранность и точность резервных копий, а также возможность восстановления данных должны быть проверены в процессе валидации и периодически контролироваться.

Приложении 11 GMP EU

Printouts

It should be possible to obtain clear printed copies of electronically stored data.

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.

Распечатки

Необходимо иметь возможность получения четких печатных копий данных, хранящихся в электронном виде.

Для записей, сопровождающих разрешение на выпуск серии, следует предусмотреть возможность получения распечаток, указывающих, изменялись ли какие-либо данные с момента их первоначального ввода.

Приложении 11 GMP EU

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.

Прослеживаемость

На основе оценки рисков следует уделить внимание встраиванию в систему возможности создания записей всех существенных изменений и удалений, касающихся GMP (система, создающая «аудиторские следы»). Причины таких изменений или удалений данных должны быть оформлены документально. Аудиторские следы должны быть доступными, иметь возможность их преобразования в понятную для пользователей форму, регулярно проверяться.

Приложении 11 GMP EU

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.

Управление изменениями и конфигурацией

Любые изменения в компьютеризированной системе, включая конфигурацию системы, должны проводиться только контролируемым способом в соответствии с установленной процедурой.

Приложении 11 GMP EU

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.

Периодическая оценка

Компьютеризированные системы должны периодически оцениваться для подтверждения того, что они остаются в валидированном состоянии и соответствуют требованиям GMP. Такие оценки должны включать, в случае необходимости, оценку текущего диапазона функциональных возможностей, записей отклонений, сбоев, проблем, истории обновлении (upgrades), эксплуатационные характеристики, надежность, защищенность, данные о валидационном статусе.

Приложении 11 GMP EU

Security

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.

Защита

Должны иметься в наличии физические и/или логические элементы контроля для обеспечения доступа к компьютеризированной системе только уполномоченным на то лицам. Соответствующие способы предотвращения несанкционированного доступа к системе могут включать в себя использование ключей, карточек доступа, персональных кодов с паролями, биометрических данных, ограничения доступа к компьютерному оборудованию и зонам хранения данных.

Приложении 11 GMP EU

The extent of security controls depends on the criticality of the computerised system.

Creation, change, and cancellation of access authorisations should be recorded.

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.

Степень защиты зависит от критичности компьютеризированной системы.

Создание, изменение и аннулирование прав доступа должно быть протоколировано.

Должны быть разработаны системы управления данными и документами для идентификации операторов, осуществляющих вход, а также для регистрации изменения, подтверждения или удаления данных, включая дату и время.

Приложении 11 GMP EU

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.

Управление инцидентами

Все инциденты (непредвиденные случаи), включая системные сбои и ошибки данных, должны быть записаны и оценены. Следует установить основную причину критических сбоев и использовать эту информацию в качестве основы корректирующих и предупреждающих действий.

Приложении 11 GMP EU

Electronic Signature

Electronic records may be signed electronically. Electronic signatures are expected to:

a. have the same impact as hand-written signatures within the boundaries of the company,

b. be permanently linked to their respective record,

c. include the time and date that they were applied.

Электронная подпись

Электронные записи могут быть подписаны в электронном виде. Электронные подписи должны:

a) в рамках предприятия иметь такое же значение (влияние), как рукописные подписи;

b) быть неразрывно связанными с соответствующими записями;

c) включать время и дату, когда они были поставлены.

Приложении 11 GMP EU

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.

Выпуск серии

Если для протоколирования одобрения и выпуска серии используется компьютеризированная система, она должна предоставлять доступ для выпуска серии только Уполномоченным Лицам, а также должна четко идентифицировать и регистрировать сотрудника, который одобрил и выпустил серию в реализацию. Эти действия должны осуществляться с использованием электронной подписи.

Приложении 11 GMP EU

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.

Непрерывность рабочего процесса

С целью обеспечения работоспособности компьютеризированных систем, сопровождающих критические процессы, следует принять меры предосторожности для гарантии непрерывности поддержки этих процессов в случае выхода системы из строя (например, с использованием ручной или альтернативной системы).

Приложении 11 GMP EU

Время, необходимое для введения в действие альтернативных средств, должно учитывать риски и соответствовать конкретной компьютеризированной системе и сопровождаемому рабочему процессу. Эти меры должны быть надлежащим образом оформлены документально и проверены.

PHARMA SOLUTIONS

Уважаемые коллеги!

Данная презентация представлена в ознакомительном объеме. По всем интересующим вопросам обращайтесь:

Адрес: г. Киев, Проспект победы, 67 корпус В

тел.: +380 73 051 15 68

тел.: +380 95 412 40 50

Сайт: https://pharmsolution.org/