Приложение № 11
к Правилам
надлежащей производственной практики
Евразийского экономического союза

ТРЕБОВАНИЯ К КОМПЬЮТЕРИЗИРОВАННЫМ СИСТЕМАМ

Принцип

Настоящее Приложение применяется ко всем типам компьютеризированных систем, используемых в рамках деятельности, регулируемой требованиями Правил надлежащей производственной практики Евразийского экономического союза (далее - Правила). Компьютеризированная система представляет собой набор программных и аппаратных компонентов, которые совместно выполняют определенные функции.

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.

Общие требования

1. Управление рисками

Управление рисками должно применяться в течение жизненного цикла компьютеризированной системы и учитывать 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.

2. Персонал

Следует поддерживать тесное сотрудничество между всем значимым персоналом, вовлеченным в данный процесс (например, с владельцем процесса, владельцем системы, Уполномоченными лицами и техническим (IT) персоналом). Весь персонал должен иметь соответствующую квалификацию, уровень доступа и нести определенную ответственность для выполнения возложенных на него обязанностей.

3. Поставщики и провайдеры услуг

3.1. 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, 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 подразделениям информационных технологий производителя.

3.2. Компетентность и надежность поставщиков являются ключевыми условиями выбора провайдеров программного продукта или услуг. Необходимость аудита должна быть основана на оценке

рисков.

3.3. Документация, прилагаемая к коммерчески выпускаемым готовым для использования программным продуктам, должна быть рассмотрена уполномоченными представителями заказчика на предмет соответствия требованиям пользователя.

3.4. Информация о системе качества и аудитах поставщиков или разработчиков программного обеспечения и установленных компьютеризированных систем должна быть доступна для предоставления инспекторам по их требованию.

Стадия проекта

4. Валидация

4.1. Валидационная документация и отчеты должны охватывать соответствующие стадии жизненного цикла компьютеризированной системы. Производители должны быть способны обосновать свои стандарты, протоколы, критерии приемлемости, процедуры и записи на основе оценки рисков.

4.2. Валидационная документация должна включать в себя записи контроля изменений (если применимо) и отчеты о любых отклонениях, выявленных в ходе процесса валидации.

4.3. Должен быть в наличии текущий перечень (реестр) всех используемых компьютеризированных систем с указанием их функциональности, регулируемой требованиями Правил.

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, доступные меры безопасности.

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

4.5. Заказчику следует предпринять все меры, гарантирующие, что компьютеризированная система разработана в соответствии с надлежащей системой управления качеством. Поставщик должен быть оценен соответствующим образом.

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

4.7. Следует представить доказательства соответствия методов и схем тестирования компьютеризированной системы. В частности, должны быть рассмотрены пределы параметров системы (процесса), границы данных и обработка ошибок. Следует документально оформить оценку соответствия применения автоматизированных средств тестирования и режимов их работы.

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

Стадия эксплуатации

5. 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.

6. 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.

7. Хранение данных

7.1. 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.

7.2. 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.

8. Распечатки

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

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

9. Контрольные следы

На основе оценки рисков следует уделить внимание встраиванию в систему возможности создания записей всех существенных изменений и удалений, связанных с областью действия Правил (система, создающая "контрольные следы"). Причины таких связанных с Правилами изменений или удалений данных должны быть оформлены документально. Контрольные следы должны быть доступными, иметь возможность их преобразования в понятную для пользователей форму, регулярно проверяться.

10. Управление изменениями и конфигурацией

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

11. Периодическая оценка

Компьютеризированные системы должны периодически оцениваться для подтверждения того, что они остаются в валидированном состоянии и соответствуют требованиям Правил. Такие оценки должны включать, в случае необходимости, оценку текущего диапазона функциональных возможностей, записей отклонений, сбоев, проблем, истории обновлении (upgrades), отчеты об эксплуатации, надежности, защищенности и о валидационном статусе.

12. Защита

12.1. 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.

12.2. Степень защиты зависит от критичности компьютеризированной системы.

12.3. Создание, изменение и аннулирование прав доступа должно быть зарегистрировано.

12.4. Должна быть разработана система управления данными и документами для идентификации операторов, осуществляющих вход, а также для регистрации изменения, подтверждения или удаления данных, включая дату и время.

13. 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.

14. Электронная подпись

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

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

b) быть неразрывно связанными с соответствующими записями;

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

15. Выпуск серии

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

16. Непрерывность работы

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). 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.

17. Архивирование

Данные могут архивироваться. Эти данные должны проверяться на доступность, удобство чтения и целостность. Если в компьютеризированной системе необходимо провести существенные изменения (например, компьютерного оборудования или программного обеспечения), следует обеспечить и проверить возможность восстановления данных.

Определения

"владелец процесса" (process owner) - лицо, ответственное за рабочий процесс;

"владелец системы" (system owner) - лицо, ответственное за работоспособность и обслуживание компьютеризированной системы, а также за защиту находящихся в ней данных;

"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;

"информационно-технологическая инфраструктура" (IT-infrastructure) - компьютерное оборудование и программное обеспечение, такое как сетевое программное обеспечение и операционные системы, которые делают возможным функционирование приложений;

"компьютеризированная система, изготовленная по индивидуальному заказу" (Bespoke (Customized) computerized system) - индивидуально спроектированная компьютеризированная система для обеспечения конкретного рабочего процесса;

"приложение" (application) - программное обеспечение, установленное на определенной платформе (компьютерном оборудовании) и предоставляющее специальные функциональные возможности;

"серийное программное обеспечение" (commercial of the shelf software) - коммерчески доступное программное обеспечение, пригодность которого для использования продемонстрирована большим количеством пользователей;

"третья сторона" (third party) - стороны, которые не находятся в прямом подчинении держателя лицензии на производство лекарственных средств.