РУКОВОДСТВО

Целостность данных и валидация компьютеризированных систем.

Настоящее Руководство разработано Федеральным бюджетным учреждением «Государственным институтом лекарственных средств и надлежащих практик» при поддержке компании «PQE групп».

Благодарности

Настоящее Руководство было разработано авторским коллективом Федерального бюджетного учреждения «Государственного института лекарственных средств и надлежащих практик» в составе: В.Н. Шестаков, Н.Н. Чадова, Т.В. Николко, И.В. Фальковский, В.А. Орлов, Н.В. Архипова, М.М. Соттаева, В.В. Горячкин и компании «PQE групп» в составе: Джильда д'Инчерти и Данило Нери.

I. ОБЩИЕ ПОЛОЖЕНИЯ

1 ВВЕДЕНИЕ.

В целях обеспечения безопасности пациентов и качества продукции Минпромторгом России издан приказ от 14 июня 2013 года № 916 "Об утверждении Правил надлежащей производственной практики" (зарегистрирован в Министерстве юстиции Российской Федерации 10 сентября 2013 года № 29938). Правила надлежащей производственной практики устанавливают требования к организации производства и контроля качества лекарственных средств для медицинского применения и ветеринарного применения с тем, чтобы производители могли гарантировать высокое качество продукции от серии к серии. Принятие решений должно основываться на регулируемых данных, создаваемых и поддерживаемых как единое целое в течение всего жизненного цикла продукта, так чтобы существовала возможность восстановить все предпринятые действия в отношении продукта.

Управление регулируемыми данными развивалось в последнее десятилетие в соответствии с продолжающимся развитием вспомогательных технологий (таких, как увеличивающееся использование электронного сбора данных, автоматизация систем и использование дистанционных технологий) и возросшей сложностью цепи поставок и способов работы (например, через поставщиков услуг). Системы, поддерживающие эти методы работы, могут использовать как ручные процессы с бумажными записями, так и полностью компьютеризированные системы.

В приложении 11 к Правилам надлежащей производственной практики определяются нормативные требования к критическим записям GMP, управляемым с помощью компьютеризированных систем: эти требования в конечном счете направлены на обеспечение целостности этих данных, управляемых с помощью автоматизированных систем.

Принципы целостности данных в равной степени применимы как к не компьютеризированным, так и компьютеризированным системам и не должны ограничивать разработку или внедрение новых концепций или технологий.

Целостность данных определяется как «степень полноты, последовательности и точности данных на протяжении всего жизненного цикла данных», и имеет основополагающее значение в фармацевтической системе качества, которая обеспечивает необходимое качество лекарственных средств. Ненадлежащие методы обеспечения целостности данных и их уязвимость подрывают качество записей и в конечном счете могут подрывать качество лекарственных средств.

Целостность данных применима ко всем элементам системы управления качеством, и изложенные в настоящем документе принципы в равной степени применимы к данным, получаемым с помощью электронных и бумажных систем; эти данные должны оцениваться на предмет выявления потенциальной уязвимости и принятия мер по разработке и внедрению надлежащей практики управления данными в целях обеспечения целостности данных.

Меры, рассматриваемые в настоящем руководстве, ориентированы на то, чтобы обеспечить эффективность инспекционных процессов в отношении фармацевтических производителей, основанную на достоверности предоставляемых документов, и в конечном счете, на целостности исходных данных. Для инспекционного процесса крайне важно, чтобы инспекторы могли определять и в полной мере полагаться на точность и полноту представляемых им доказательств и документации.

Это руководство направлено на использование риск-ориентированного подхода к управлению данными, который включает риск, критичность и жизненный цикл данных. Пользователям данного руководство необходимо понимать управление данными (как жизненный цикл), чтобы идентифицировать данные, оказывающие наибольшее влияние на GMP процессы. Исходя из этого, можно определить и внедрить наиболее эффективный и действенный контроль, основанный на оценке рисков, и обзор данных.

Требования и методы, рассматриваемые в данном руководстве, приведены в соответствие с ожиданиями, определенными в соответствующих руководствах, выпущенных компетентными ассоциациями (например, ВОЗ, PIC/s, ICH, ISPE)

Данное руководство следует рассматривать как средство для понимания позиции Департамента развития фармацевтической и медицинской промышленности Минпромторга России и ФБУ «ГИЛС и НП» в отношении целостности данных и минимальных ожиданий достижения соответствия. Руководство не описывает каждый сценарий, поэтому взаимодействие с регуляторными органами рекомендуется в тех случаях, когда ваш подход отличается от описанного в данном руководстве.

II. ОБЛАСТЬ ПРИМЕНЕНИЯ

2 НАЗНАЧЕНИЕ.

Это руководство ориентировано на создание процесса, объединяющего рациональную организационную практику, эффективные процессы, основанные на оценке рисков, и соблюдение нормативных требований для обеспечения целостности тех записей, которые могут оказать потенциальное влияние на безопасность пациентов и качество продукции.

Поскольку целостность данных применима ко всем элементам системы управления качеством, руководство ориентировано на определение ожиданий в отношении важнейших записей, управляемых с помощью бумажных документов и компьютеризированных систем,

и сфокусировано на требованиях к валидации компьютеризированных систем, что является ключевым требованием для обеспечения целостности записей.

Цели настоящего руководства:

- Поддержка при проверке обеспечения целостности данных на соответствие требованиям GMP.
- Предоставление консолидированных, наглядных рекомендаций регулируемым компаниям по риск-ориентированным стратегиям контроля, которые позволяют реализовать существующие требования к целостности и надежности данных в контексте современных отраслевых практик и глобализованных цепей поставок.
- Способствовать эффективному внедрению элементов целостности данных в планирование и проведение процесса квалификации GMP поставщиков
- Определить процедурную базу, соответствующую нормативным требованиям к управлению компьютеризированными системами, изложенным в приложении 11 к приказу Минпромторга № 916 от 14 июня 2013 года (в редакции приказа от 18.12.2015 № 4148)

3 ОБЛАСТЬ ПРИМЕНЕНИЯ

Этот документ применяется к записям, генерируемым, поддерживаемым в рабочем состоянии и/или хранимым вручную или электронным способом, от создания до архивирования, для поддержания GMP процессов, используемых фармацевтическими компаниями, для гарантирования ими высокого качества производимой продукции, от серии к серии

Требования к целостности данных, изложенные в настоящем руководстве, применимы в равной степени к «бумажным» и электронным данным, генерируемым или используемым в рамках любого процесса, способного оказать потенциальное воздействие на безопасность пациентов и качество продукции на различных этапах производства и дистрибуции фармацевтического продукта.

В случае передачи одного из критических процессов на аутсорсинг, организация, передающая работу, несет ответственность за целостность всех сообщаемых результатов, включая результаты, представленные любой аутсорсинговой организацией или поставщиком услуг (см. раздел 11).

В случае, если регламентирующие данные создаются, управляются и ведутся с помощью электронных записей, связанная с этим целостность обеспечивается соответствующей компьютеризированной системой. Как следствие, это руководство применяется ко всем компьютеризированным системам, способным оказать влияние на GMP, т. е. которые потенциально могут повлиять на безопасность пациента и качество продукции.

III. БАЗОВАЯ КОНЦЕПЦИЯ

4 ПРИНЦИПЫ ЦЕЛОСТНОСТИ ДАННЫХ

Регуляторные органы во всем мире используют знания организаций, которые разрабатывают, производят и упаковывают, тестируют, распространяют и контролируют фармацевтическую продукцию. В процессе оценки и анализа подразумевается взаимодоверие между регуляторным органом и регулируемой компанией (т. е. фармацевтической компанией) в том, что информация, представляемая в досье и

используемая в процессе принятия повседневных решений, является всесторонней, полной и надежной. Данные, на которых основаны эти решения, должны быть прослеживаемыми (**A**ttributable), читаемыми (**L**egible), своевременными (**C**ontemporaneous), подлинными (**O**riginal) и точными (**A**ccurate), - перечень требований, обычно называемый “ALCOA”.

Меры контроля для обеспечения целостности данных встраиваются в фармацевтическую систему качества, которая гарантирует, что лекарственные средства имеют требуемое качество. Целостность данных применима ко всем элементам фармацевтической системы качества, и принципы, изложенные в настоящем документе, в равной степени применимы к данным, создаваемым и электронными и бумажными системами. Для обеспечения точности, полноты, последовательности и надежности записей и данных на протяжении всего периода их необходимости (т. е. на протяжении всего жизненного цикла данных) организации должны следовать надлежащей практике документирования (GDocP).

Усилия и ресурсы, направляемые на контроль целостности данных, необходимо соизмерять с риском для качества продукции, а также сопоставлять с другими запросами ресурсов обеспечения качества. Фармацевтическим компаниям следует разработать и использовать методическую базу, которая обеспечит приемлемое контролируемое состояние, основанное на оценке рисков целостности данных. Методическую базу следует полностью документировать с соответствующем логическим обоснованием.

Ответственность за надлежащую практику в отношении управления данными и их целостности лежит на производителе, проходящем проверку: эти организации несут полную ответственность и обязаны оценивать свои системы управления данными на предмет потенциальных уязвимостей и принимать меры по разработке и внедрению надлежащей практики управления данными для обеспечения сохранения целостности данных.

Менеджмент несет главную ответственность за распределение ресурсов и осуществление мер контроля, направленных на сведение к минимуму потенциального риска для целостности данных, а также за идентификацию остаточного риска.

Регулируемые компании несут ответственность за используемые ими системы и данные, генерируемые этими системами. В компании должна существовать культура, обеспечивающая полноту, целостность и точность данных во всех формах (т. е. в бумажной и электронной форме): каждый оператор, занятый сбором, представлением или поддержанием данных, должен быть надлежащим образом проинформирован об ожиданиях целостности данных и находиться под постоянным контролем.

Заинтересованные стороны, передавшие на аутсорсинг третьей стороне процессы, которые могут оказать влияние на клинические исследования, производство, контроль качества или дистрибуцию, несут ответственность за соответствие третьей стороны требованиям данного руководству.

4.1 Требования ALCOA+

Для обеспечения качественной информированности процесса принятия решений, и для подтверждения достоверности информации, события или действия, послужившие основанием для принятия этих решений, должны быть качественно задокументированы. Надлежащие практики документирования (GDocPs) являются ключом к обеспечению целостности данных, и важной частью ФСК. Применение GDocPs может варьироваться в

зависимости от носителя, используемого для записи данных (т. е. физические или электронные записи), но принципы применимы к обоим.

Ключевые принципы как бумажного, так и электронного документооборота объединены в акроним ALCOA (Прослеживаемость (**A**ttributable), Читаемость (**L**egible), Своевременность (**C**ontemporaneous), Подлинность (**O**riginal) и Точность (**A**ccurate)), который был расширен, добавлением других атрибутов: (Полнота (Complete), Последовательность (Consistent), Устойчивость (Enduring) и Доступность (Available), которые теперь называются ALCOA+.

Выполнение ожиданий ALCOA+, описание которых приведено ниже, гарантирует, что события должным образом задокументированы и данные могут использоваться для принятия обоснованных решений.

Прослеживаемость. Должна быть обеспечена идентификация лица, выполнившего записанное задание. Необходимо документировать, кто выполнил задачу / функцию, подтвердить, что функция была выполнена обученным и квалифицированным персоналом. Это также касается изменений, внесенных в записи: исправлений, удалений, изменений и т.д.

Читаемость. Все записи должны быть разборчивыми – информация должна быть читаема в течение всего периода хранения. Это относится ко всей информации, которая должна будет считаться полной, включая все исходные записи или заметки. В тех случаях, когда динамический характер электронных данных, (см. определение в разделе 5.2) важен для содержания и смысла записи, возможность работать с данными с помощью подходящего приложения должна быть обеспечена в течение периода хранения (т. е. данные должны быть сохранены в электронном формате, который позволяет к ним обращаться и обрабатывать).

Своевременность. Доказательства действий, событий или решений регистрируются по мере их совершения. Эта документация должна служить точным подтверждением того, что и почему было сделано или решено, т. е. что повлияло на решение в то время.

Подлинность. Подлинная запись может быть определена как первая записанная информация, будь то записанная на бумаге (статическая) или в электронном виде (обычно динамическая, в зависимости от сложности системы). Информация, первоначально захваченная в динамическом состоянии, должна оставаться доступной в этом состоянии.

Точность. Обеспечение точности сведений и записей за счет многих элементов устойчивой ФСК может основываться на:

- факторах, связанных с оборудованием, такие как квалификация, калибровка, техническое обслуживание и валидация компьютеризированных систем.
- политике и процедуры контроля действий и поведения,
- процедурах проверки данных на предмет соблюдения процедурных требований
- управлении отклонениями, включая анализ первопричин, оценку воздействия и CAPA
- обученном и квалифицированном персонале, понимающем важность соблюдения установленных процедур и документирования своих действий и решений.

Полнота. Вся информация, критическая для воссоздания события, является уместной и соответствующей. Уровень детализации, необходимый для того, чтобы набор информации считался полным, будет зависеть от критичности информации. Полная запись данных, полученных в электронном виде, включает соответствующие метаданные.

Последовательность. Надлежащая практика документирования должна применяться на протяжении всего процесса без исключения, включая отклонения и изменения, которые могут произойти в ходе процесса.

Устойчивость. Частью обеспечения уверенности, что данные доступны является обеспечение их существования в течение всего периода, в течение которого они могут потребоваться. Это означает, что они должны оставаться нетронутыми и доступными в неудаляемом/ «прочном» формате.

Доступность. Записи должны быть доступны для рассмотрения в любое время в течение требуемого периода хранения для рутинных решений о выпуске, расследований, трендов, годовых отчетов, аудитов или инспекций. Записи должны быть доступны доступны в формате, удобном для чтения персоналу, ответственному за их рассмотрение.

В совокупности эти элементы направлены на обеспечение точности информации, в том числе научных данных, которые используются для принятия критических решений о качестве продукции.

5 ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ.

5.1 Акронимы

«PQS»	Pharmaceutical Quality System - Фармацевтическая система качества
«CSV»	Computerized Systems Validation - Валидация Компьютеризированных Систем
«ER - ЭЗ»	Electronic Record – Электронная запись
«ERES - ЭЗЭП»	Electronic Record & Electronic Signature - Электронная запись и электронная подпись
«ERP» -	Enterprise Resource Planning - Планирование ресурсов предприятия
«ES» – «ЭП»	Electronic Signature – Электронная подпись
«FAT» -	Factory Acceptance Testing - Приёмо-сдаточные испытания на заводе-изготовителе
«GAMP»	Good Automated Manufacturing Practice (GAMP) Guide for Validation of Automated Systems in Pharmaceutical Manufacture (issued by ISPE) – руководство по Надлежащей Практике Автоматизированного Производства (GAMP) для валидации автоматизированных систем в фармацевтическом производстве (Выпущено ISPE)
«GxP»	Good ‘X’ Practice where ‘X’ is used as a collective term for – Надлежащая практика «х», где «х » это: GCP – Good Clinical practice – Надлежащая Клиническая Практика GLP – Good Laboratory Practice – Надлежащая Лабораторная Практика

	GMP – Good Manufacturing Practice – Надлежащая Производственная Практика
	GPvP – Good Pharmacovigilance Practice – Надлежащая Практика Фармаконадзора
«HW»	Hardware – Аппаратное обеспечение
«IQ - КМ »	Installation Qualification (i.e. Configuration Testing) - Квалификация Монтажа (т. е. тестирование конфигурации)
«ISPE »	International Society for Pharmaceutical Engineering - Международное Общество Фармацевтического Инжиниринга
«LIMS»	Laboratory information management system - Система Управления Лабораторной Информацией
«OQ »	Operational Qualification (i.e. Functional Testing) - Квалификация функционирования
«OS - ОС»	Operating System – Операционная Система
«PC - ПК»	Personal Computer – Персональный компьютер
«P&ID»	Piping and Instrumentation Diagram - Схема Трубопроводов и Контрольно-Измерительных Приборов
«PCS - СКП»	Process Control System - Система контроля процесса
«PIC/S»	Pharmaceutical Inspection Convention-Pharmaceutical Inspection Co-operation Scheme - Схема сотрудничества Конвенции по фармацевтическим Инспекциям в области фармацевтических инспекций
«PLC - ПЛК»	Programmable Logic Control - Программируемый логический контроллер
«PQ»	Performance Qualification (i.e. Requirement Testing) – квалификации эксплуатации (т. е. тестирование требований)
«QC - КК»	Quality Control – Контроль Качества
«R&D - ИИР»	Research & Development - Исследования И Разработки
«RACI »	Responsible, Accountable, Consulted, Informed - Ответственный, Подотчетный, Консультированный, Информированный
«RAI - ИОР»	Risk Assessment Index – Индекс Оценки Риска
«RFI - ЗИ»	Request For Information – Запрос Информации
«RT - ТТ»	Requirements Testing – Тестирование Требований
«SAT»	Site Acceptance Testing - Приёмо-сдаточные испытания на площадке клиента.
«SME - ЭП»	Subject Matter Expert – Эксперт по Предмету
«SOP - СОП»	Standard Operating Procedure - Стандартная операционная Процедура
«SW - ПО»	Software – Программное Обеспечение

5.2 Определения

"**Контрольный след**" - процесс, который фиксирует такие детали, как добавления, удаления или изменения информации в записи, как бумажной, так и электронной, без затенения или переписывания исходной записи. Контрольный след облегчает восстановление истории подобных событий, связанных с записью, независимо от носителя, включая информацию, такую как: “кто, что, когда и почему” каждого действия.

"**Компьютеризированная система**" - компьютеризированная система, коллективно контролирует выполнение одного или нескольких автоматизированных бизнес-процессов. Она включает в себя компьютерное оборудование, программное обеспечение, периферийные устройства, сети, персонал и документацию (например: руководства, стандартные операционные процедуры).

«**Валидация компьютеризированных систем**» - это подтверждение посредством оценки и предоставления объективных доказательств того, что характеристики КС соответствуют потребностям пользователя и своему назначению, а также все требования стабильно выполняются.

"**Данные**" - информация, извлеченная или полученная из исходных данных (например, сообщенный аналитический результат). Данные должны соответствовать следующим требованиям ALCOA+

Прослеживаемость (**A**ttributable) до лица, создавшего запись,

Читаемость (**L**egible),

Своевременность (**C**ontemporaneous),

Подлинность (**O**riginal)

Точность (**A**ccurate)),

«+» означает дополнительные требования, обеспечивающие Полноту (Complete), Последовательность (Consistent), Устойчивость (Enduring) и Доступность (Available) данных.

"**Жизненный цикл данных**" - охватывает все этапы жизненного цикла данных (включая необработанные данные), начиная с их создания и записи, обработки (включая преобразование или миграцию), использование, хранение, архивирование/извлечение и заканчивая уничтожением данных. Процедуры уничтожения данных должны учитывать критичность данных и, при необходимости, требования законодательства в отношении их хранения. Архивационные меры принимаются для долгосрочного хранения соответствующих данных в соответствии с законодательством.

"**Обработка данных**" - последовательность операций, выполняемых с данными с целью извлечения, представления или получения информации в определенном формате. Примеры могут включать: статистический анализ для ежегодного обзора продукции. Должна быть обеспечена прослеживаемость любого наперёд определенного параметра, используемого в деятельности по обработке данных. Контрольный след и сохранность записи должны позволять реконструкцию всех действий по обработке данных независимо от того,

включается ли итог обработки в последующий отчёт или используется иначе. Если обработка данных повторяется с постепенным изменением параметров обработки, то это должно быть зафиксировано для обеспечения отсутствия манипуляций параметрами обработки в целях достижения желательных конечных данных.

"**Обзор данных**" - должна существовать процедура, описывающая процесс обзора и утверждения данных. Обзор данных также включает обзор соответствующих метаданных (т. е. контрольный след). Обзор следует основывать на исходных данных или «точной копии». Анализ данных должен быть задокументирован. Процедура должна описывать действия, которые должны быть предприняты, если анализ данных выявит ошибку или упущение. Данная процедура должна позволять вносить исправления или уточнения в данные в соответствии с GMP, обеспечивая читаемость исходной записи и прослеживаемость исправления с использованием принципов ALCOA+

"**Динамическая запись**" - записи в динамическом формате, такие как электронные записи, которые обеспечивают интерактивную связь между пользователем и содержимым записи. Например, электронные записи в форматах баз данных позволяют проследить, оценить тренды и запросить данные результатов хроматографии, хранящихся в электронном виде, позволяют пользователю выполнить повторную обработку данных, просмотреть скрытые поля при наличии соответствующих прав доступа, а также изменять основную линию хроматограммы для более четкого обзора интегрирования.

"**Метаданные**" – это данные, которые являются результатом переосмысления фактических данных, создавая контекст и смысл. Как правило, эти данные описывают структуру, элементы данных, взаимосвязи и другие характеристики данных. Они также позволяют соотнести данные с отдельным лицом (или, если они генерируются автоматически, конкретному источнику данных). Метаданные являются неотъемлемой частью исходной записи. Без метаданных данные не имеют смысла.

"**Исходная запись**" - данные в виде файла или формата, в котором они были первоначально созданы, с сохранением целостности (точности, полноты, содержания и значения) записи, например, оригинальная бумажная запись ручного наблюдения или электронный файл необработанных данных из компьютеризированной системы. Эти данные должны позволять полностью реконструировать деятельность, приводящую к получению данных.

"**Первичная запись**" - запись, которая имеет преимущественную силу в тех случаях, когда данные, которые собираются и хранятся одновременно более чем одним методом не совпадают.

"**Регулируемые данные**" - данные, используемые для GMP целей, требуемые Правилами GMP, относящиеся к операциям, которые могут повлиять на безопасность пациента и качество продукции.

«**Полное время обработки образцов**» - это временной период между созданием (отбором) образцов до завершения их анализа. Это время, необходимое для завершения всех анализов для серии. Этот фактор должен быть определен надлежащим образом, поскольку, если ожидается, что этот период будет коротким, операторы могут быть склонны нарушать целостность данных, с тем чтобы уложиться в ожидаемый период.

"**Регулируемая компания**" - компания, которая должна соответствовать требованиям GMP в соответствии с нормативными требованиями или в связи с бизнес причинами.

"**Статическая запись**" - статическая запись представляет собой документ с фиксированными данными, например, бумажную запись или электронное изображение. Примеры статической записи включают список обучающих записей или статическое изображение, созданное во время сбора данных

"**Истинная копия**" - копия исходной информации должна быть точной копией, имеющей все те же атрибуты и информацию исходной записи. Истинная копия должна сохранять целостность, точность, полное содержание, форматы дат, электронную подпись, разрешения и полный контрольный след. Процесс создания истинной копии (печатной или электронной) должен быть аттестован, полностью описан, копия должна быть заверена путем нанесения даты и подписи на бумагу или путем использования подтвержденной электронной подписи. Истинная копия может храниться в другом электронном формате по сравнению с первоначальной записью, если это необходимо, но должна сохранять эквивалентный статический/динамический характер исходной записи.

IV. СРЕДСТВА ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ ДАННЫХ

6 СИСТЕМА УПРАВЛЕНИЯ ДАННЫМИ

6.1 Система управления данными

Управление данными - это совокупность организационных мероприятий, обеспечивающих целостность данных. Эти организационные мероприятия обеспечивают полноту, последовательность и точность записи на протяжении всего жизненного цикла данных, независимо от процесса, формата или технологии, в которых они генерируются, регистрируются, обрабатываются, сохраняются, извлекаются и используются.

Управление данными должно касаться владения данными и подотчетности на протяжении всего жизненного цикла, а также проектирования, использования и мониторинга процессов / систем в соответствии с принципами целостности данных, включая контроль за преднамеренными и непреднамеренными изменениями данных.

Системы управления данными должны быть неотъемлемой частью фармацевтической системы качества (PQS) для каждого этапа жизненного цикла продукта: PQS должна владеть данными на протяжении всего жизненного цикла и учитывать проектирование, использование и мониторинг процессов / систем в целях соблюдения принципов целостности данных, включая контроль преднамеренных и непреднамеренных изменений и удаления информации.

Эффективная система управления данными продемонстрирует понимание и приверженность руководства надежным практикам управления данными, включая необходимость сочетания соответствующей организационной культуры и поведения (раздел 7.4) и понимание риска, связанного с данными на протяжении их жизненного цикла. Кроме того, должны иметься подтверждения свидетельства доведения необходимой информации до сведения персонала на всех уровнях организации таким образом, чтобы это обеспечивало расширение прав и возможностей в случае неудач и возможностей для улучшения. Это уменьшает стимул к фальсификации, изменению или удалению данных.

Системы управления данными должны включать подготовку персонала в отношении важности принципов целостности данных и создания рабочей среды, которая обеспечивает видимость и активно поощряет предоставление информации об ошибках, упущениях и нежелательных результатах.

Степень, в которой менеджмент компании знает и понимает целостность данных, может повлиять на успех компании в управлении целостностью данных. Руководство должно располагать достаточными знаниями и обладать достаточными полномочиями для предотвращения нарушений целостности данных и обнаруживать их, если они происходят.

6.2 Риск-ориентированный подход к управлению данными

Управление рисками для качества (Quality risk management - QRM) имеет важное значение для эффективной программы управления данными. Усилия и ресурсы, выделяемые на управление данными и записями, должны быть соизмеримы с риском: подход к управлению записями и данными, основанный на оценке рисков, призван обеспечить уверенность, что для обеспечения целостности GMP данных, выделены достаточные ресурсы и применяются необходимые стратегии контроля.

Поскольку не все этапы обработки данных имеют одинаковое значение для качества продукции и безопасности пациентов, для определения важности каждого этапа обработки данных необходимо использовать управление рисками. Эффективный подход к управлению данными основан на риске для целостности данных, определяемом следующими факторами:

- Критичность данных (влияние на принятие решений и качество продукции)
- Подверженность нарушениям (возможность изменения и удаления данных, а также вероятность обнаружения / видимости изменений в процессе рутинной проверки изготовителем). Воздействие определяется потенциальной возможностью удаления, изменения или исключения не зарегистрированным лицом и возможностью обнаружения таких действий и событий.

Риски для данных могут возрастать в результате сложных, непоследовательных процессов с открытыми и субъективными результатами по сравнению с простыми задачами, которые выполняются последовательно, четко определены и имеют четкую цель.

Сокращение усилий и/или частоты контрольных мер может быть оправдано для данных, которые оказывают меньшее воздействие на продукт, безопасность пациента или рабочую среду; если эти данные получены в процессе, который не дает возможности для внесения изменений без доступа к системе высокого уровня или специализированного программного обеспечения / знаний.

Организации должны разработать, внедрить и эксплуатировать документированную систему, обеспечивающую приемлемое состояние контроля на основе риск-ориентированного подхода к управлению целостностью данных с соответствующим обоснованием. Примером подходящего подхода является оценка риска целостности данных (data integrity risk assessment - DIRA), при которой процессы, производящие данные или в результате которых получены данные, картируются, критические воздействия идентифицируются, а присущие риски документируются.

Оценка рисков должна быть сосредоточена на бизнес-процессе, например: производство, контроль качества. Необходимо оценивать потоки данных и методы получения данных, а не просто учитывать функциональность или сложность компьютеризированной системы. Факторы для рассмотрения включают:

- Сложность процесса

- Методы генерирования, хранения и удаления данных и их способность обеспечивать точность, удобочитаемость, неудаляемость данных
- Последовательность процессов и степень автоматизации / человеческий фактор
- Субъективность результата (т. е. процесс является открытым или четко определенным?)
- Результаты сопоставления данных электронной системы и событий, зарегистрированных вручную, могут быть показательными для выявления нарушений, например: явных расхождений между аналитическими отчетами и временем сбора необработанных данных.

6.3 Жизненный Цикл Данных

Жизненный цикл данных относится к тому, как данные генерируются, обрабатываются, сообщаются, проверяются, используются для принятия решений, хранятся и окончательно удаляются в конце срока хранения. Данные, относящиеся к продукту или процессу, могут пересекать различные границы в течение жизненного цикла. Это может включать передачу данных между ручными и IT-системами или между различными организационными границами; как внутренними (например, между производством, КК и ОК), так и внешними (например, между поставщиками услуг или подрядчиками и заказчиками).

Управление данными, как описано в предыдущем разделе, должно применяться на протяжении всего жизненного цикла данных для обеспечения целостности данных. Данные могут храниться либо в исходной системе при условии соответствующего контроля, либо в организованном архиве.

Данные по способу их записи могут быть:

- **Бумажными.** Бумажная запись ручного наблюдения или деятельности. Данные, полученные вручную на бумаге, могут потребовать независимой проверки, если это будет сочтено необходимым из оценки риска целостности данных, или по другому требованию. Следует учитывать меры по снижению риска, особенно в отношении данных, связанных с высокой критичностью.
- **Электронными.** Электронные записи получаются при использовании как простого оборудования, так и сложных конфигурируемых компьютеризированных систем. Присущий риск для целостности данных, связанный с оборудованием и компьютеризированными системами, может различаться в зависимости от того, в какой степени система (генерирующая или использующая данные) может быть сконфигурирована, а также от возможности манипулирования данными во время передачи между компьютеризированными системами в течение жизненного цикла данных. Следует поощрять использование имеющихся технологий, надлежащим образом сконфигурированных для снижения риска нарушения целостности данных. Простые электронные системы, не имеющие программной настройки и средств электронного хранения данных (например, pH-метры, весы и термометры) могут потребовать только калибровки и/или поверки. В то же время сложные системы требуют "валидации по назначению" (см. раздел 8.1.1). В любом случае тщательная оценка системы является обязательной, поскольку все системы, упомянутые в качестве примеров, могут иметь очень сложную версию. Важно не упускать из виду системы меньшей сложности, например: отдельно стоящие системы с

пользовательскими настройками (такие как Электрокардиографы, Фурье инфракрасные спектрофотометры и спектрофотометры в УФ диапазоне), поскольку данными этих систем возможно манипулировать или повторять измерение для достижения желаемого результата исхода с лимитированной возможностью для обнаружения.

- **Гибридными**, в которых исходную запись составляют как бумажные, так и электронные записи. При использовании гибридных систем должны быть четко определены первичные записи (в любом случае все доказательства должны быть рассмотрены и сохранены). Гибридные системы должны быть сконструированы таким образом, чтобы они отвечали желаемой цели.
- **Прочими**, такие как фотографии, изображения и хроматографические тарелки. Где получить данные (записанные фотографии или изображения, или другого носителя), условия для хранения такого формата на протяжении всего жизненного цикла данных при этом руководствуются теми же соображениями, как и для других форматов, учитывая любые дополнительные элементы, необходимые для этого формата.

Необработанные данные определяются как исходная запись (данные), которая может быть описана как первая запись информации, записанная на бумаге или в электронном виде. Независимо от формата (бумажный или электронный), необработанные данные должны соответствовать требованиям ALCOA+. Информация, первоначально записанная как динамическая, должна оставаться доступной в этом состоянии. Необработанные данные должны позволять полностью реконструировать деятельность. Если данные были зафиксированы в динамическом состоянии и сгенерированы электронным способом, бумажные копии не могут рассматриваться как "необработанные данные".

В случае, если основное электронное оборудование не имеет возможности хранить электронные данные или обеспечивает только печатный вывод данных (например, весы или pH-метры), распечатка представляет собой необработанные данные. В тех случаях, когда основное электронное оборудование хранит электронные данные на постоянной основе, но способно хранить только определенный ограниченный объем данных до их перезаписи. Эти данные должны периодически просматриваться и, при необходимости, сверяться с бумажными записями, и извлекаться в качестве электронных данных, если такая практика поддерживается самим оборудованием.

Требования ALCOA + применяются также к Метаданным (см. 5.2).

6.4 Организационные Требования

6.4.1 Культура качества

Следует уделять большое внимание культуре качества, показателям эффективности, целями и мотивацией на успех мер по управлению данными, задаваемыми высшим руководством,. Политика управления данными (или ее эквивалент) утверждается на самых высоких уровнях организации.

Руководство должно создать рабочую среду (т. е. культуру качества), прозрачную и открытую, в которой персоналу предлагается свободно сообщать о сбоях и ошибках, включая потенциальные проблемы надежности данных, с тем чтобы можно было проводить корректирующие и предупреждающие мероприятия.

Структура организационной подчиненности должна обеспечивать информационный поток между сотрудниками всех уровней. Эффективному управлению данными в одних случаях может способствовать расширение прав и возможностей сотрудников для выявления и сообщения о проблемах через систему качества. В других случаях для достижения эквивалентного уровня контроля может потребоваться уделять больше внимания надзору и вторичному обзору в связи с социальным барьером на пути передачи нежелательной информации. Возможность прямого анонимного обращения к руководству может также быть важной в этой ситуации.

Менеджмент может стимулировать культуру качества посредством следующего:

- Обеспечения осведомленности и понимания ожиданий (например, Кодекс этики и Кодекс поведения);
- Лидерства посредством примера, руководство должно демонстрировать то поведение, которое оно ожидают увидеть от подчиненных;
- Обеспечения отчетности за действия и решения;
- Постоянного и активного участия;
- Установления реалистичных ожиданий с учётом ограничений, которые оказывают давление на сотрудников;

6.4.2 Кодекс этики и политики

Кодекс Ценностей и Этики должен отражать философию менеджмента в отношении качества, достигаемого посредством Политик (т. е. Кодекса поведения), которые соответствует Культуре Качества и создают атмосферу доверия, в которой все сотрудники несут ответственность за обеспечение безопасности пациентов и качества продукции.

Общие стандарты этики и добросовестности компании должны быть установлены и известны каждому сотруднику, и соответствующие ожидания должны сообщаться часто, своевременно и на постоянной основе .

Политики Кодекса поведения должны четко определять нормы этического поведения, такие как честность. Это должно быть доведено до сведения всего персонала и должно быть надлежащим образом понято. Недостаточно ограничиваться только знанием требований, необходимо понимать также то, почему требования были установлены, и каковы последствия невыполнения требований. Нежелательные действия, такие как преднамеренная фальсификация данных, несанкционированные изменения, уничтожение данных или другие действия, нарушающие целостность данных, должны быть устранены незамедлительно. В случае необходимости принимаются дисциплинарные меры. Поведение, соответствующее требованиям, должно быть признано надлежащим образом.

6.4.3 Программы Обучения

Персонал должен быть обучен политике целостности данных и согласен соблюдать ее. Руководство должно обеспечить, чтобы персонал был обучен понимать и различать надлежащее и ненадлежащее поведение (включая преднамеренную фальсификацию), и должен быть осведомлён о потенциальных последствиях.

Кроме того, ключевые сотрудники, включая менеджеров, руководителей и сотрудников службы качества, должны быть обучены мерам по предотвращению правонарушений и обнаружению подозрительных данных.

Руководство должно также обеспечить, чтобы при наборе персонала и периодически после этого (по мере необходимости) весь персонал проходил обучение по процедурам обеспечения надлежащей практики документирования (GDocP) как для бумажных, так и для электронных записей.

6.4.4 Совершенствование Фармацевтической Системы Качества

Применение современных принципов управления рисками для качества и надлежащей практики управления данными к существующей фармацевтической системе качества служит для модернизации системы качества в целях решения задач, которые возникают в связи с генерацией сложных данных.

Фармацевтическая система качества компании должна быть способна предотвращать, обнаруживать и исправлять слабые места в системе или процессах, которые могут привести к нарушениям целостности данных. Компания должна знать данные своего жизненного цикла продукта и интегрировать соответствующие средства контроля и процедуры, чтобы полученные данные были действительными, полными и надежными. В частности, такой контроль и процедурное обновление могут осуществляться в следующих областях:

- Оценка и управление рисками
- Программы расследований
- Практика обзора данных
- Валидация программного обеспечения
- Управление поставщиками/подрядчиками
- Программа обучения, включающая политику целостности данных и СОП по целостности данных.
- Включение целостности данных в программу самоинспекции.
- Показатели качества и отчетность перед высшим руководством.

Следует критически осмыслять эффективность процедур контроля и обзора в достижении желаемых результатов. Показателем зрелости управления данными является организационное понимание и принятие остаточного риска, который определяет приоритетность действий. Организация, которая считает, что "нет риска" сбоя целостности данных, вряд ли сделала адекватную оценку рисков, присущих жизненному циклу данных. Поэтому необходимо подробно изучить подход к оценке жизненного цикла данных, их критичности и степень риска. Это может указывать на возможные режимы отказа, которые могут быть исследованы в ходе проверки.

6.4.5 Показатели качества для обеспечения целостности данных

Должны проводиться регулярные управленческие обзоры показателей качества, в том числе касающиеся целостности данных, с тем чтобы выявлять, обострять и своевременно решать важные вопросы. Следует проявлять осторожность и выбирать ключевые

показатели эффективности таким образом, чтобы не занизить важность и приоритетность целостности данных.

Показатели качества должны охватывать следующие виды действий:

- **Превентивные**, ориентированные на надзор за правилами для предотвращения сбоев целостности (например, уровень осведомленности операторов/супервайзора о целостности данных, полное время обработки образцов)
- **Корректирующие**, ориентированные на мониторинг завершения и результатов выполнения записей по сравнению с требованиями ALCOA+ (например, Интенсивность оценки электронных записей, Интенсивность корректирующих действий по целостности данных)
- **Мониторинг**, ориентированный на контроль количества фактических сбоев целостности и соответствующих последующих действий (например, интенсивность внутренней проверки целостности данных, частота самопроизвольных сбоев целостности, т. е. сообщается операторами)

Эти показатели, направленны на то, чтобы продемонстрировать приверженность руководства обеспечению целостности управления данными GMP. Необходимо иметь независимого эксперта, периодически проверяющего эффективность своих систем и средств контроля.

7 ТРЕБОВАНИЯ К РЕГУЛИРУЕМЫМ БУМАЖНЫМ ЗАПИСЯМ

7.1 СМК для управления записями

Эффективное управление бумажными документами является ключевым элементом фармацевтической СК на любом этапе жизненного цикла продукции. Соответственно, система документации должна соответствовать требованиям GMP и обеспечивать эффективный контроль за документами и записями для поддержания их целостности.

Во всех случаях, когда бумажные записи создаются и используются для обеспечения безопасности пациентов и качества продукции, эти записи должны контролироваться и оставаться надежными на протяжении всего жизненного цикла данных, т. е. соответствовать требованиям ALCOA+.

Процедуры, описывающие надлежащую практику документирования и механизмы контроля документации, должны быть доступны в рамках СМК. Эти процедуры должны определять:

- Создание, согласование и утверждение базовых документов (master documents) и процедуры для использования в течение их жизненного цикла
- Создание, распространение и контроль шаблонов, используемых для записи данных (образцы, журналы и т. д.)
- Процессы извлечения и аварийного восстановления данных
- Процесс создания рабочих копий документов (например, СОП и бланков) для повседневного использования с особым акцентом на обеспечение контролируемости и прослеживаемости копий

- Руководство по заполнению бумажных документов с указанием способов идентификации отдельных операторов, форматов ввода данных и внесения изменений в документы
- Порядок рутинной проверки заполненных документов на точность, подлинность и полноту
- Процессы регистрации, поиска, хранения, архивирования и удаления записей

7.2 Создание Записи

7.2.1 Создание Записей

Бумажные записи создаются в соответствии со следующими правилами:

- Все документы должны иметь уникальный идентификационный номер (включая номер версии) и должны быть проверены, утверждены, подписаны и датированы.
- Использование неконтролируемых документов должно быть запрещено внутренними процедурами; аналогичным образом, использование временных записей (например, на обрывках бумаги) должно быть запрещено.
- Форма документа должна обеспечивать достаточное пространство для вписывания данных, с тем чтобы обеспечить четкость и разборчивость вписанных данных. Должно быть четко указано, какие данные должны быть вписаны в каждое поле.
- Документы должны храниться таким образом, чтобы обеспечить надлежащий контроль версий.
- Неавторизованные или непреднамеренные изменения в основной копии (в мягкой копии) должны быть предотвращены

Риск ненадлежащего использования и/или фальсификации записи "обычными средствами" (т. е. не требующими использования специальных навыков мошенничества) должен быть снижен до приемлемого уровня.

Для типовых записей, хранящихся в электронном виде, должны быть приняты следующие меры предосторожности:

- Доступ к эталонным шаблонам должен контролироваться
- Управление процессами для создания и обновления версий должно быть четким и практичным / проверенным
- Основные документы должны храниться таким образом, чтобы предотвратить несанкционированные изменения
- Мастер-копии должны содержать отличительную маркировку, позволяющую отличить мастер от копии, например, использование цветных бумаг или чернил для предотвращения случайного использования.

Перечень всех эталонных записей должен управляться службой качества. В этом перечне для каждого типа записи должна содержаться, как минимум, следующая информация: наименование, номер, включая номер версии, местонахождение (например, база данных документации, дата вступления в силу, дата пересмотра и т. д.).

Записи в производственных зонах должны надлежащим образом контролироваться назначенными лицами или определёнными процессами. Эти меры контроля должны осуществляться таким образом, чтобы свести к минимуму риск повреждения или потери записей и обеспечить целостность данных

7.2.2 Распределение Записей

Бумажные записи должны распределяться по следующим правилам:

- Обновленные версии должны распространяться своевременно, при этом только текущая утвержденная версия может быть доступна для использования
- Устаревшие основные документы и файлы должны быть архивированы, а доступ к ним ограничен.
- Все выданные и неиспользованные физические документы должны быть собраны и уничтожены соответствующим образом.
- Выпуск контролируется с помощью защищенного штампа или бумажного цветового кода, отсутствующего в рабочих зонах или другой соответствующей системе.
- Незаполненные («чистые») документы должны быть идентифицированы с помощью уникального идентификатора, создание каждого документа должно быть пронумеровано и записано

7.2.3 Ведение и завершение записи

- Рукописные записи должны быть сделаны лицом, выполнившим задание
- Неиспользованные, пустые поля в документах должны быть зачеркнуты, датированы и подписаны.
- Рукописные записи должны быть сделаны четким и разборчивым почерком
- Заполнение полей дат производится в формате, определенном для производственной площадки (например, ДД / мм / ГГГГ или мм / ДД / ГГГГ)
- Операции по заполнению должны осуществляться своевременно
- Записи должны быть нестираемыми. Использование карандашей не допускается
- Записи должны быть подписаны и датированы с использованием уникального идентификатора, присваиваемого автору.
- Должна быть обеспечена прослеживаемость любых определяемых пользователем параметров в рамках деятельности по обработке данных. Записи должны позволять восстанавливать всю деятельность по обработке данных, независимо от того, сообщается ли о результатах этой обработки впоследствии или используется иным образом. Если обработка данных повторяется с постепенным изменением параметров обработки, то это должно быть видимым для обеспечения того, чтобы параметры обработки не были использованы для достижения более желательной конечной точки.
- Поправки в записях должны быть сделаны таким образом, чтобы обеспечить полную прослеживаемость, в том числе:
    - Зачёркивание того, что должно быть изменено способом, позволяющим прочитать зачёркнутое (например, одной линией).

- Причина исправления, где возможно, должна быть четко зафиксирована и проверена, если это критично.
- Кто и когда внес изменение (инициалы и дата)

7.3 Проверка Записей

Подход к проверке содержания конкретных записей, таких как критические бумажные записи и соответствующие исправления, должен быть ориентирован на обеспечение проверки требований ALCOA+ и соблюдения всех применимых нормативных требований.

Должна существовать процедура, описывающая процесс проверки и утверждения данных. Проверка данных должна быть задокументирована, и в протоколе должно содержаться положительное заявление о том, были ли обнаружены проблемы, дата проверки и подпись рецензента.

Процедура должна описывать действия, которые должны быть предприняты, если анализ данных выявит ошибку или упущение. Эта процедура должна позволять корректировать или уточнять данные, чтобы обеспечить видимость исходной записи и прослеживаемость коррекции с использованием принципов ALCOA+.

В случае аутсорсинговых процессов фармацевтическая компания должна гарантировать, что критические данные, полученные от Поставщика, будут рассмотрены; ответственность за анализ данных должна быть документирована и согласована обеими сторонами.

7.4 Истинные копии

7.4.1 Истинные копии бумажных документов

Копии оригиналов бумажных документов (например, аналитические протоколы, отчеты, проверки и т. д.), как правило, очень полезны для целей коммуникации, например, между компаниями, работающими в разных местах. Эти записи должны быть под контролем в течение их жизненного цикла, чтобы гарантировать, что данные, полученные с другой площадки (дочерней компании, подрядчика и т. д.) сохраняются как «истинные копии», когда это целесообразно, или используются в качестве «краткого отчета», когда не соблюдаются требования «истинной копии» (например, резюме сложных аналитических данных).

Истинная копия должна обеспечивать сохранение полного смысла данных и возможность восстановления их истории.

Оригинальные записи и истинные копии должны сохранять целостность записи. Истинные копии оригиналов записей могут храниться вместо оригиналов записей (например, при сканировании бумажных записей), если существует документированная система проверки и записи целостности копии. Организации должны учитывать любой риск, связанный с уничтожением оригинальных записей.

7.4.2 Бумажные записи, полученные из компьютерных систем

Бумажные записи, генерируемые простыми электронными системами, такими, например, как весы, pH-метры или простое технологическое оборудование, которые не хранят данные, предоставляют ограниченную возможность влиять на представление данных путем (повторной) обработки, изменения электронных меток даты/времени. В этих обстоятельствах оригинал записи должен быть подписан и датирован лицом, создающим запись, а также приложен к досье на серию.

Такой подход разрешен только для простых систем и для записей, содержимое которых статично.

Статический формат записи, такой как бумажная или электронная запись, является фиксированным и практически не допускает взаимодействия между пользователем и содержимым записи. Например, после печати или преобразования в статический электронный формат записи теряют возможность повторной обработки или более детального просмотра исходных значений.

И наоборот, записи в динамическом формате, такие как электронные записи, допускают интерактивную связь между пользователем и содержимым записи. Например, электронные записи в форматах баз данных позволяют пользователю отслеживать тренды и запрашивать данные; записи хроматограмм, сохраняемые в электронном формате позволяют пользователю или проверяющему (при наличии соответствующих прав доступа) для повторной обработки данных и увеличить масштаб, чтобы просмотреть детали более четко.

Многие электронные записи важно сохранять в их динамическом (электронном) формате, чтобы обеспечить взаимодействие с данными. Данные должны храниться в динамической форме, где это имеет решающее значение для их целостности или более поздней проверки. Это должно быть оправдано с учетом риска. Для такого рода записей запрещается ведение единственных бумажных записей и удаление соответствующих электронных записей.

7.5 Хранение Записей

Срок хранения каждого типа записей должен (как минимум) соответствовать срокам, указанным в соответствующих требованиях GMP. Следует учитывать так же другие существующие нормативные требования, которые могут предусматривать более длительные сроки хранения. Записи могут храниться внутри организации или с помощью внешней службы хранения, при условии подписания соответствующего соглашения о качестве.

Мероприятия по архивации должны быть организованы так, чтобы обеспечивать восстановление и читаемость данных и метаданных на протяжении всего периода хранения.

7.6 Утилизация Записей

Необходимо организовать документированный процесс удаления записей таким образом, чтобы обеспечить удаление данных, подлежащих удалению по истечении установленного срока хранения. Система должна гарантировать, что текущие записи не подвергнутся случайному уничтожению и что исторические записи непреднамеренно не будут возвращены в число текущих записей (например, исторические записи перепутаны/перемешаны с существующими записями).

Должна иметься запись / реестр, свидетельствующая о надлежащем и своевременном уничтожении изъятых из обращения записей.

Должны быть приняты меры для снижения риска удаления неправильных документов. Права доступа, позволяющие удалять записи, ограничиваются несколькими лицами.

В случае распечатки, которая не является постоянной (например, термотрансферная бумага), заверенная ("истинная") копия может быть сохранена, а оригинал, не являющийся постоянным может быть уничтожен. Бумажные документы могут быть заменены Сканами при условии соблюдения принципов "подлинной копии" (см. раздел 8.4).

8 ТРЕБОВАНИЯ К РЕГУЛИРУЕМЫМ ЭЛЕКТРОННЫМ ЗАПИСЯМ

Регулируемые электронные записи (т. е. создаваемые и используемые для обеспечения безопасности пациентов и качества продукции) управляются с помощью большого количества компьютерных систем, используемых компаниями в операционной деятельности. Эти системы варьируются от простых автономных до больших интегрированных и сложных систем, многие из которых влияют на качество продукции. Каждая регулируемая организация несет ответственность за полную оценку и контроль всех компьютеризированных систем и управление ими в соответствии с требованиями GMP.

Организации должны быть в полной мере осведомлены о характере и областях задействования компьютеризированных систем, должны проводить оценки, каждой системы, использования ее по назначению и функционирования, а также любые риски или уязвимости для целостности данных, на которые может быть оказано воздействие. Особое внимание следует уделять определению критичности компьютеризированных систем и любых связанных с ними данных в отношении качества продукции.

Все компьютеризированные системы, потенциально влияющие на качество продукции, должны эффективно управляться в соответствии со зрелой структурой качества, которая призвана обеспечить защиту систем от актов случайного или преднамеренного вмешательства, изменения или любых других действий, которые могут повлиять на целостность данных.

При определении уязвимости и риска данных важно, чтобы компьютеризированная система рассматривалась в контексте ее использования в рамках бизнес-процесса.

Для обеспечения соответствия регулируемых электронных записей требованиям ALCOA+, соответствующие компьютеризированные системы должны обеспечивать Надежность, Безопасность, Прослеживаемость, Проверяемость и Подотчетность.

Эти требования отражены в приложении 11 к Правилам надлежащей производственной практики, утвержденным приказом Минпромторга России от 14 июня 2013 г. №916, в котором определяются нормативные требования к критическим записям GMP, управляемым с помощью компьютеризированных систем, которые ориентированы на обеспечение целостности этих данных, управляемых с помощью автоматизированных систем.

8.1 Валидация компьютеризированных систем

Компьютеризированные системы должны соответствовать нормативным требованиям и соответствующим руководящим указаниям, которые включают требование валидации: системы должны быть валидированы для использования по назначению, что требует понимания функций компьютеризированной системы в рамках конкретного процесса компании.

Валидация компьютеризированной системы (ВКС) - это документированный процесс " достижения и поддержания соответствия применимым правилам GMP и пригодности для целевого использования путем реализации принципов, подходов и мероприятий жизненного цикла в рамках валидационных планов и отчетов, а также путем применения соответствующих оперативных средств контроля на протяжении всего срока службы системы".

Для обеспечения целостности электронных данных компьютеризированные системы должны быть валидированы на уровне, соответствующем их использованию и применению. Валидация должна предусматривать необходимые меры контроля для обеспечения целостности данных, включая оригинальные электронные данные и любые распечатки или отчеты в формате PDF из системы. В частности, этот подход должен обеспечить выполнение требований ALCOA+ и надлежащее управление рисками целостности данных на протяжении всего жизненного цикла данных. Поэтому при проверке компьютеризированных систем и последующем контроле изменений требуется внедрение и подтверждение того, что все необходимые средства контроля для обеспечения целостности данных имеются и что возникновение ошибок в данных сведено к минимуму.

Деятельность по валидации должна гарантировать, что параметры конфигурации и элементы управления для обеспечения целостности данных задействованы и управляются в вычислительной среде (включая программное обеспечение приложений и операционных систем). Мероприятия включают, но не ограничиваются:

- документирование спецификаций конфигурации для коммерческих готовых систем, а также разработанных пользователем систем, где применимо
- ограничение параметров конфигурации безопасности для системных администраторов независимым персоналом, где это технически возможно
- отключение параметров конфигурации, позволяющих перезаписывать и повторно обрабатывать данные без возможности отслеживания
- ограничение доступа и применение штампов времени/даты.

Использование валидационных данных от поставщика системы в отрыве от её конкретных конфигурации и назначения неприемлемо. В данном случае валидационные мероприятия поставщика следует рассматривать как своего рода функциональную верификацию, которая может не соответствовать требованиям к квалификации эксплуатации

Этот документ интегрирует риск-ориентированный подход к валидации КС в бизнес-процессы, определяя документацию, требуемую для каждого из этапов валидации, и ответственности на каждом шаге процесса валидации. В разделе 10 настоящего документа обобщается передовой отраслевой опыт в области валидации компьютеризированных систем, основанных на оценке рисков, включая руководящие указания и методологию из руководящих принципов, выпущенных наиболее авторитетными ассоциациями (например, PIC/S, ISPE).

8.1.1 Сбор/Ввод данных

Системы должны быть разработаны для правильного сбора данных, полученных с помощью ручных или автоматизированных средств.

Для ручного ввода:

- Ввод данных должен осуществляться только авторизованными лицами, система должна регистрировать данные о входе, лице, делающем запись, и времени, когда запись была сделана
- Данные должны быть введены в указанном формате, который контролируется программным обеспечением, деятельность по валидации должна проверить, что недействительные форматы данных не принимаются системой
- Все данные, введённые вручную должны быть проверены, либо вторым оператором, либо валидированными компьютерными средствами.
- Изменения в записях регистрируются в контрольном журнале и проверяются надлежащим образом авторизованным и независимым лицом.

Для автоматизированного сбора данных:

- Интерфейс между исходной системой, системами сбора и регистрации данных должен быть валидирован для обеспечения точности данных
- Данные, полученные системой, должны быть сохранены в памяти в формате, который не подвержен манипуляциям, потерям или изменениям
- Программное обеспечение системы должно включать валидированные проверки для обеспечения полноты полученных данных, а также любых метаданных, связанных с данными
- Все необходимые изменения данных должны быть разрешены и контролироваться в соответствии с утвержденными процедурами. Например, ручная интеграция и повторная обработка результатов лабораторных исследований должны выполняться утвержденным и контролируемым образом. Служба качества компании должна принимать меры, обеспечивающие внесение изменений в данные только в случае необходимости и назначенными лицами.

8.2 Безопасность

8.2.1 Доступ к системе

Средства контроля доступа пользователей, как физические, так и электронные, должны быть сконфигурированы и применены для запрещения несанкционированного доступа, изменения и удаления данных.

Для всех сотрудников, нуждающихся в доступе и использовании конкретной электронной системы, устанавливаются и присваиваются индивидуальные логины и пароли. Общие учетные данные для входа не позволяют проследить за человеком, который выполнял действие; по этой причине общие пароли (даже если они оправданы по причинам финансовой экономии) должны быть запрещены.

В случае, если система не включает в себя функции контроля доступа (например, если для нее не требуется пароль или должна использоваться общая учетная запись пользователя), должна быть реализована одна из следующих эквивалентных мер контроля:

- Бумажный журнал, заполняемый вручную, обеспечивающий прослеживаемость обращений к системе
- Стороннее программное обеспечение, позволяющее обеспечить доступ к системе только предварительно авторизованным операторам

Пригодность этих альтернативных методов должна быть обоснована и задокументирована.

8.2.2 Авторизация Пользователя

Следует в полной мере использовать механизмы контроля доступа для обеспечения того, чтобы люди имели доступ только к функциям, соответствующим их служебной роли, и чтобы действия относились к конкретному лицу. Компании должны быть в состоянии продемонстрировать уровни доступа, предоставленные отдельным сотрудникам, и обеспечить наличие исторической информации об уровне доступа пользователей.

Контроль доступа должен применяться как при входе в операционную систему, так и на уровне приложений. Индивидуальный вход в систему на уровне операционной системы может не потребоваться, если имеются соответствующие средства управления для обеспечения целостности данных (например, невозможно изменить, удалить или создать данные вне приложения).

Доступ администратора к компьютерным системам, используемым для запуска приложений, должен контролироваться. Обычные пользователи не имеют доступа к критически важным аспектам программного обеспечения, например, системные часы, функциями удаления файлов и т. д. Права системного администратора (разрешающие такие действия, как удаление данных, изменение базы данных или изменение конфигурации системы) не должны назначаться лицам, непосредственно заинтересованным в данных (создание данных, просмотр или утверждение данных).

Схема авторизации пользователей должна обеспечивать разделение обязанностей.

8.2.3 Резервное копирование

Процессы резервного копирования и восстановления должны быть документированы с помощью процедуры, определяющей операции резервного копирования и шаги восстановления, которые должны выполняться в случае необходимости. Процессы резервного копирования и восстановления должны быть протестированы для обеспечения возможности полного восстановления данных и метаданных в случае сбоя системы. Должен быть создан механизм (автоматический или ручной) проверки резервного копирования для обеспечения его надлежащего функционирования.

Процессы резервного копирования и восстановления должны быть документированы (например, с помощью процедуры адресации), валидированы и проходить периодическую проверку. Каждая резервная копия должна проверяться для обеспечения ее правильного функционирования.

Обычные резервные копии (например, носители, на которых хранятся копии данных) должны храниться в удаленном месте (физически раздельно) на случай аварии.

8.2.4 Проверка Переноса Данных

Перенос данных - это процесс передачи данных и метаданных между типами носителей или компьютеризированными системами. При необходимости перенос данных может изменить

формат данных, с тем чтобы сделать их пригодными для использования или видимыми в альтернативной компьютерной системе.

Процедуры переноса данных должны содержать обоснование и быть тщательно разработаны и проверены для обеспечения целостности данных в течение жизненного цикла данных

8.3 Прослеживаемость

8.3.1 Контрольный след

Система должна обеспечивать автоматическую запись аудиторского следа, который представляет собой форму метаданных, содержащих информацию, связанную с действиями, относящимися к созданию, изменению или удалению регулируемых электронных записей. Контрольный след обеспечивает безопасную запись сведений о жизненном цикле, таких как создание, добавление, удаление или изменение информации в записях, без искажения или перезаписи исходной записи. Контрольный след облегчает восстановление истории таких событий, связанных с записью, независимо от ее носителя, включая информацию «кто, что, когда и почему», относящуюся к событию.

Записи аудиторского следа должны быть сделаны в понятной форме и содержать по крайней мере следующую информацию:

- Имя лица, внесшего изменение в данные;
- Описание изменения
- Время и дата изменения
- Причина изменения

Функции аудиторского следа должны быть постоянно включены, а доступ к ним заблокирован. Как и другие функциональные возможности, направленные на обеспечение целостности данных, контрольный след должен верифицироваться в ходе валидации системы.

Система должна базироваться на надлежащим образом контролируемых/синхронизированных часах для регистрации событий во времени с целью обеспечения возможности реконструкции и прослеживаемости, включая информацию о часовом поясе, в котором эти данные используются в случае нескольких удалённых площадок. Операторам не разрешается изменять эталонное время и / или часовой пояс.

В случае отсутствия в системах автоматического аудиторского следа, для фиксации изменений данных в качестве временной меры, могут быть использованы бумажные записи только до тех пор, пока система с работающим аудиторским следом не станет доступной.

8.3.2 Проверка Аудиторского Следа

Данные аудиторского следа, относящиеся к регулируемым электронным записям, подлежат аудиту регулируемым пользователем с целью проверки правильности выполнения операций и внесения каких-либо изменений (модификации, удаления или перезаписи) в исходную информацию в электронных записях. Все изменения должны быть должным образом санкционированы.

Проверка связанных с данными аудиторских следов должна быть частью рутинной проверки данных в процессе утверждения.

Периодичность, функции и обязанности по проверке аудиторских следов должны основываться на оценке риска в соответствии с релевантностью GMP данных, записанных в компьютеризированной системе. Например, в случае изменений в электронных данных, которые могут оказать непосредственное влияние на качество лекарственных средств, ожидается, что контрольный след будет пересматриваться каждый раз, когда данные генерируются, или в момент использования данных (т. е. когда данные используются для принятия критического решения GMP).

Регулируемый пользователь должен создать СОП, которая подробно описывает, как проверять контрольный след. Процедура подробно определяет процесс, которому должно следовать лицо, ответственное за проверку аудиторского следа.

Действия, связанные с аудиторским следом должны быть документированы. Записи должны храниться вместе с другими документами GMP.

8.4 Проверяемость

8.4.1 Электронные Копии

Система должна позволять создавать точные и полные копии записей как в читаемой, так и в электронной форме, пригодные для инспектирования, проверки и копирования инспекторами.

8.4.2 Архивирование

Данные должны периодически архивироваться в соответствии с письменными процедурами. Архивные копии и резервные копии данных должны физически сохраняться в разных местах.

Данные должны быть доступными и читаемыми, а их целостность должна поддерживаться на протяжении всего периода архивирования.

Должна быть предусмотрена процедура восстановления архивных данных в случае необходимости проведения расследования. Процедура восстановления архивных данных должна регулярно проверяться.

8.4.3 Удаление

Должны быть разработаны процедуры, описывающие процесс удаления хранящихся в электронной форме данных. Эти процедуры должны содержать руководство для оценки данных и их распределения в периоды хранения и описывают порядок удаления данных, которые более не требуются.

8.5 Контроль и учёт

8.5.1 Электронная подпись

Электронные подписи, используемые взамен рукописных подписей должны контролироваться для подтверждения прослеживаемости и аутентичности и принадлежности конкретному лицу, подписавшему запись

Использование электронной подписи должно контролироваться с особым вниманием к:

- Тому, как подпись закреплена за владельцем
- Как факт электронной подписи регистрируется в системе, чтобы его нельзя было изменить или манипулировать без признания недействительной подписи или статуса записи.

- Как запись подписи будет связана с сделанной записью и как это можно проверить.
- Безопасность электронной подписи, т. е. чтобы она могла применяться только "владельцем" этой подписи.

Ожидается, что для демонстрации пригодности будет проведена надлежащая валидация процесса подписания, связанного с системой, и что будет сохранен контроль над подписанными записями

В случае подготовки бумажной или pdf-копии документа с электронной подписью метаданные, связанные с электронной подписью, сохраняются вместе с соответствующим документом.

Электронная подпись или системы электронной подписи должны предусматривать “проявления подписи", т. е. отображение в пределах видимой записи, которое определяет, кто подписал ее, их название и дату (и время, если они значительны) и значение подписи (например, проверено или утверждено).

Вставленное изображение подписи или сноска, указывающая на то, что документ был подписан в электронной форме (если он был введен иным способом, чем процесс заверения электронной подписи), являются недостаточными. Если документ подписан в электронной форме, то метаданные, связанные с подписью, сохраняются.

9 ЖИЗНЕННЫЙ ЦИКЛ ВАЛИДАЦИИ НА ОСНОВЕ РИСКА

В соответствии с этим руководством (раздел 9.1.1), процесс компьютерной валидации является ключевым шагом для обеспечения целостности электронных данных, создаваемых и поддерживаемых в регулируемых целях.

Компьютеризированные системы, которые могут влиять на качество продукции или услуг и целостность данных, подпадают под действие правил GMP и нуждаются в валидации. Цель настоящего Раздела заключается в определении процесса валидации компьютеризированной системы на протяжении всего жизненного цикла системы согласно соответствующим наиболее важным руководящим принципам (PIC/S, GAMP) и обеспечении процедурных рамок для выполнения требований надлежащей производственной практики. Этот раздел, посвящённый процессу валидации компьютеризированных систем, определяет действия, которые должны быть выполнены до выпуска системы, во время её использования вплоть до вывода системы из эксплуатации.

Процесс валидации обеспечивает документированное доказательство, позволяющее с высокой степенью уверенности сделать вывод о том, что компьютеризированная система функционирует в соответствии с ее спецификациями, а также требованиями к качеству и нормативным требованиям на постоянной и воспроизводимой основе. Кроме того, процесс валидации должен обеспечить документальное подтверждение того, что система включает в себя автоматизированные функции, ориентированные на обеспечение соответствия GMP критических электронных записей требованиям ALCOA+.

Данное руководство способствует применению риск-ориентированного подхода к спецификации, проектированию и проверке компьютеризированных систем, которые могут повлиять на качество продукции и безопасность пациентов на следующих этапах:

- Требования и планирование: этап планирования ориентирован на решение необходимых задач, обязанностей, процедур и сроков на основе рисков, связанных с

системой. Проект внедрения основан на документе спецификации требований пользователей (URS), ориентированном на детализацию потребностей бизнеса и пользователей (с точки зрения бизнес-процессов, процессов соответствия, а также технических и нефункциональных стандартов), которые будут определены на начальных этапах проекта внедрения.

- Спецификации и сборка: на основе URS поставщик / исполнитель создает набор документов спецификаций для определения конструкции / конфигурации системы. Количество и уровень детализации спецификаций можно варьировать в зависимости от типа системы и ее предполагаемого использования. Матрица прослеживаемости демонстрирует взаимосвязь между спецификациями и соответствующими требованиями.
- Тестирование и приемка: проверка системы направлена на подтверждение того, что спецификации были выполнены: это может включать в себя несколько этапов обзоров и тестирования в зависимости от типа системы, применяемого метода разработки и его использования. Тестирование должно основываться на результатах оценки функциональных рисков.
- Выпуск: система официально принята к использованию и выпуску в операционную/производственную среду в соответствии с контролируемым и документированным процессом, включая утверждение от владельца бизнес-процесса, технического владельца и представителей службы качества.
- Работа через вспомогательные процессы: после выпуска система будет управляться через вспомогательные процессы, ориентированные на поддержание утвержденного статуса
- Завершение использования: когда система выводится из эксплуатации, данные, поддерживаемые системой, должны быть доступны в течение срока хранения

Обычно ожидается, что будет проведена перспективная валидация компьютеризированных систем; однако для уже установленных систем может быть приемлемым проведение ретроспективной валидации на основе оценки всех исторических данных (данные которые уже были произведены системой) для существующей компьютеризированной системы.

9.1 Компьютеризированная система и категории

Компьютеризованная система считается состоящей из всего аппаратного обеспечения, прошивки (микропрограммного обеспечения), установленных устройств и программного обеспечения, контролирующего работу компьютера. Контролируемая функция может состоять из оборудования, подлежащего контролю, и оперативных процедур, определяющих функцию такого оборудования, или же это может быть операция, для которой не требуется оборудование, отличное от оборудования в компьютеризированной системе.

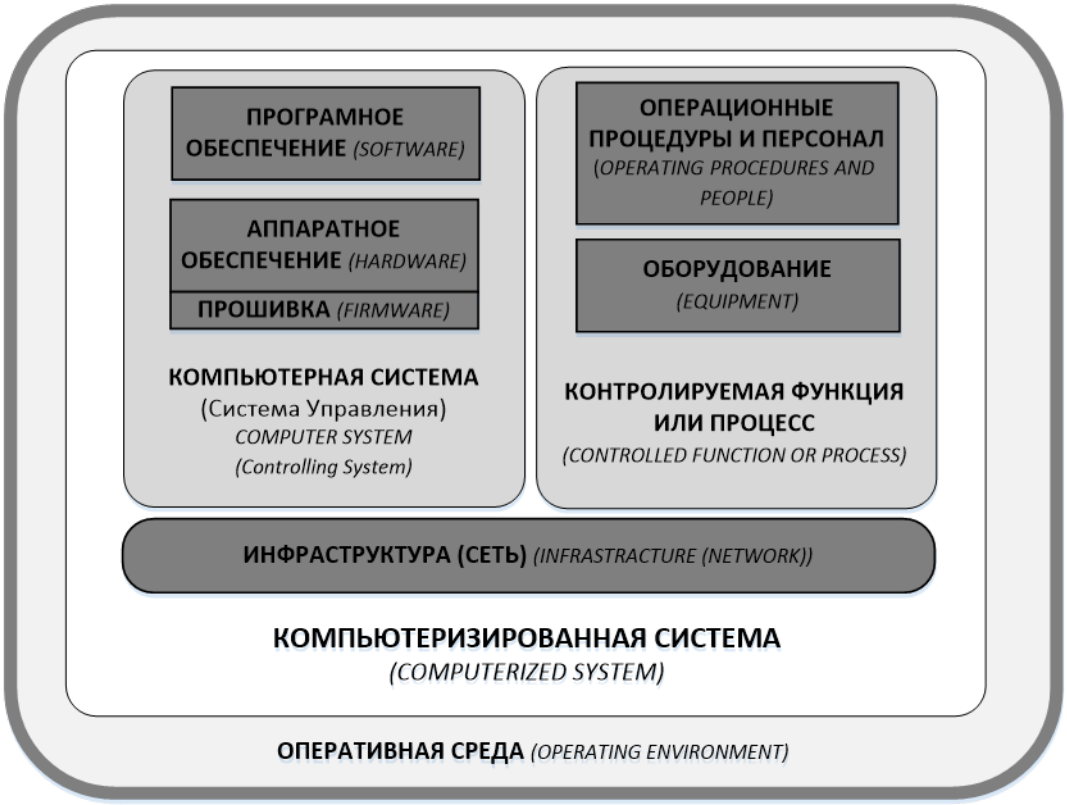

Рис.1 Надлежащая практика для компьютеризированных систем в регулируемом GXP-окружении. PI 011-3 25 сентябрь 2007

В соответствии с этим определением компьютеризированная система должна рассматриваться как включающая не только Приложения ПО, но и все другие субъекты (связанные инструменты, IT-инфраструктуру, персонал), которые могут повлиять на критический процесс(процессы) GMP, выполняемый через систему. Каждый субъект должен быть задокументирован и находиться под контролем для достижения валидированного статуса.

Риск сбоев или дефектов как правило, повышается с отклонением от стандартного программного и аппаратного обеспечения к пользовательскому программному и аппаратному обеспечению. Повышенный риск обусловлен сочетанием большей сложности и меньшего опыта пользователей. В сочетании с оценкой рисков и оценкой поставщиков классификация может быть частью эффективного подхода к управлению рисками качества.

В большинстве систем имеются компоненты различной сложности, такие как операционная система, не сконфигурированные компоненты и настроенные или настраиваемые компоненты. Для облегчения определения соответствующей стратегии проверки и глубины были определены следующие категории.

Категория	Тип	Описание	Примеры
3	Не конфигурированные компоненты	Параметры времени выполнения могут быть введены и сохранены, но программное обеспечение не может быть настроено в соответствии с бизнес-процессом	Прошивки-приложений Программное обеспечение готовое к использованию (COTS - Commercial Off-The-Shelf) Инструментарий
4	Конфигурированные компоненты	Программное обеспечение, часто очень сложное, которое может быть настроено пользователем для удовлетворения конкретных потребностей бизнес-процесса пользователя. Программный код не изменяется.	– LIMS – Data Acquisition Systems – SCADA – ERP – Clinical Trial Monitoring – DCS – ADR Reporting – CDS – EDMS – BMS Systems – CRM – Spreadsheets – Simple Human Machine Interface
5	Пользовательские приложения	Самостоятельно разработанное и закодированное пользователем с учетом бизнес-процессов программное обеспечение	Самостоятельно разработанные или разработанные на заказ Компьютерные приложения Приложения, управляющие процессом Пользовательские схемы логики Электронные таблицы (макросы)

Как правило, уровень детализации и глубина подтверждающей документации должны возрастать с увеличением категории системы.

Сложные компьютеризированные системы могут состоять из нескольких компонентов, которые могут относиться к различным категориям. В этом случае система должна быть классифицирована в соответствии с высшей категорией множественных компонентов

В случае, если один или ограниченное количество компонентов разработаны на заказ, систему можно все еще расклассифицировать как Категория 4, специфицировав список разработанных на заказ компонентов, классифицированных как Категория 5

9.2 Инвентаризация системы и оценка рисков GMP

Регулируемые компании должны иметь перечень всех используемых компьютеризированных систем. Этот перечень должен включать ссылку на следующее:

- Имя, местоположение и основная функция (т. е. предполагаемое использование) каждой компьютеризированной системы;
- Оценка риска, связанного с системой и соответствующей записью(ы) Поддерживаемые системы (например, прямое воздействие на GMP, косвенное воздействие, не влияет)
- Текущий статус валидации каждой системы и ссылки на существующие валидационные документы.

Для каждой системы проводится оценка рисков, в частности оценка необходимых мер контроля для обеспечения целостности данных. Уровень и глубина валидации для целостности данных определяются на основе критичности системы и процесса и потенциального риска для качества продукции, например, процессы или системы, которые генерируют или контролируют данные о выпуске партий, как правило, требуют большего контроля, чем те системы, которые управляют менее важными данными или процессами.

Объем валидации должен включать критерии приемлемости GMP, ранжированные по критичности риска для качества продукта/процесса, целостности данных, риска отказа или сбоя системы. Этот процесс представляет собой одно из наиболее важных предварительных условий планирования валидации, поскольку необходимо определить приоритеты и обратить внимание на те системы (и функции в рамках систем), которые представляют наибольший риск сбоя. Результаты анализа рисков и обоснование критических или некритических классификаций должны быть задокументированы. Риски, потенциально влияющие на соответствие GMP, должны быть четко определены.

9.3 Оценка Поставщика и Соглашение о Качестве

Когда третьи лица (например, поставщики, поставщики услуг или собственный IT отдел) используются чтобы обеспечить, установить, настроить, интегрировать, валидировать, провести техническое обслуживание (например, через удаленный доступ), модифицировать или сохранить компьютеризированную систему или предоставление услуг по обработке данных, должно быть подписано официальное соглашение о качестве между регулируемой компанией и любыми третьими лицами, и эти соглашения должны включать четкие определения обязательств каждой из сторон.

Потенциальные и существующие поставщики систем GMP (поставщики компьютеризированных систем и поставщики услуг) оцениваются на основе бизнес-риска и влияния рассматриваемой услуги или компьютеризированной системы.

Оценка Систем Качества третьей стороны (в качестве компонента оценки рисков) проводится в целях определения объёма валидационных мероприятий, а также для оценки возможности использования документации третьей стороны в рамках этого процесса.

Цель оценки третьей стороной заключается в определении того, отвечают ли поставщики компьютеризированных систем и поставщики услуг требованиям:

- Способность обеспечить высокое качество продукции или услуг,
- Соответствие нормативным требованиям,
- Наличие адекватных процессов обеспечения качества.

Анализ поставщика системы необходимо выполнить для проверки возможности создавать продукт, соответствующий стандарту качества и методологии. Выбранный метод оценки основывается на риске, связанном с системой, сложности системы и предыдущем опыте работы с поставщиком в соответствии с процедурой оценки поставщика.

9.4 Требования и Этап Планирования

9.4.1 Спецификация требований пользователя

Для всех компьютеризированных систем должна быть создана **Спецификация требований пользователя** (URS). Целью документа URS является определение назначения и функций системы, включая все основные требования.

Объем и детализация требований должны быть соизмеримы с риском, сложностью и новизной и должны быть достаточными для поддержки последующего анализа риска, спецификации, конфигурации/дизайна и проверки по мере необходимости.

В спецификации требований пользователя указывается, хранятся ли данные, управляемые системой, в электронном формате и используются ли данные для операций, оказывающих влияние на GMP.

Спецификация требований пользователя включает в себя следующее:

- Критически важные для качества функции
- Идентификация регулируемых электронных записей (ЭЗ), поддерживаемых системой, и подписываемых электронной подписью (ЭП), выполняемой в системе
- Применимые нормативные требования к электронным записям и управлению электронными подписями (также называемые правилами ЭЗЭП)
- Список бизнес-процессов и связанных с ними потоков процессов
- Другие Общие требования (например, эксплуатационные требования, требования к данным, технические требования, требования к интерфейсу, требования к среде, требования к производительности, требования к доступности и требования к безопасности) должны включаться по мере необходимости в зависимости от типа/сложности системы

Требования определяются / согласовываются соответствующим владельцем (владельцами) бизнес-процесса и включаются в согласованные соглашения об именах и с уникальными справочными номерами.

Спецификация требований пользователя считается обязательной также в случае ретроспективной валидации для определения назначения системы, которая должна быть верифицирована посредством интеграционного (end-to-end) теста.

9.4.2 Валидационный план

План валидации - это стратегический документ, подтверждающий, что все валидационные мероприятия проводятся должным образом под контролем руководства с использованием риск ориентированного подхода.

Документ должен определять жизненный цикл валидации и объем валидации путем определения границ системы; результаты оценки поставщика должны рассматриваться вместе с условиями использования документации, предоставленной поставщиком.

В валидационном плане должны быть идентифицированы: перечень создаваемой документации, распределение ответственности (например, матрица распределения ответственности RACI для результатов валидации), а также общие критерии приемлемости для валидационного процесса.

План валидации всегда создаётся в случае внедрения новой системы или существенных изменений существующей.

9.5 Спецификации и Этап Сборки

В зависимости от категории и сложности системы документация по спецификации, рассматриваемая в этом разделе, может быть объединена в один документ.

9.5.1 Функциональная Спецификация

Функциональные спецификации должны содержать точное и подробное описание того, каким образом система удовлетворяет основным требованиям, предъявляемым к компьютерной системе и внешним интерфейсам. Это значит описания функций, представлений и где применимо, ограничений и атрибутов. Документ определяет, что должна делать система, и какие функции и средства разрешены системой, включая перечень проектных целей системы.

Документ должен содержать подробные функциональные описания требований Компании к системе, диаграммы использования, технологические схемы, спецификации процессов, спецификации внешних интерфейсов, рабочие спецификации, спецификации безопасности и контроля, Конфигурируемые элементы, детали логической модели данных, спецификации технологической инфраструктуры, спецификации доступности/ремонтопригодности.

Спецификации должны быть подготовлены и организованы таким образом, чтобы можно было отслеживать каждое требование пользовательской спецификации соотнося их с соответствующими функциональными возможностями и соответствующей документацией по испытаниям, что позволяет отслеживать на протяжении всего жизненного цикла от индивидуальных требований пользователя до соответствующих испытаний. Описание высокого уровня должно быть разбито на подуровни, описывающие отдельные функции;

каждая функция должна иметь систему кодирования, с тем чтобы ее можно было идентифицировать и отслеживать.

Функциональные спецификации должны быть проверены на соответствие требованиям пользователя, что позволяет выполнять квалификацию эксплуатации (OQ) (т. е. функциональное тестирование) и выдачу проектных спецификаций системы.

9.5.2 Спецификации конфигурации

Конфигурационная Спецификация создаётся для описания:

- списка компонентов аппаратного и программного обеспечения, включенных в компьютеризированную систему

- параметров системы (например, длины пароля), которые могут повлиять на одну или несколько функций GMP.

Конфигурационная Спецификация определяет базовые показатели конфигурации системы, адресующиеся к компонентам и интерфейсам ПО, а также параметрам системы, преимущественно фокусируясь на элементах конфигурации, которые могут повлиять на GMP функциональные возможности.

Для идентификации профилей пользователей, определенных в системе, и связанных с ними функций создается Матрица безопасности (включенная в Конфигурационную Спецификацию или как отдельный документ). Соотнесение пользователей каждому профилю выполняется в соответствии с процедурами безопасности.

Конфигурационная Спецификация должна также описывать IT-ландшафт, на котором размещено программное обеспечение, и то, как оно должно быть подключено к любой существующей системе или оборудованию. Поэтому этот документ должен включать также (или давать ссылку на другой документ) описание системного ландшафта и спецификации всех элементов, показанных на ландшафте (например, операционной системы, промежуточного программного обеспечения, вспомогательная деятельность в сфере программного обеспечения, например: программы просмотра PDF-файлов, системных сред, интерфейсов, соответствующих компонентов IT-инфраструктуры, например, серверов).

9.5.3 Проектные спецификации

Проектные спецификации необходимы для пользовательских компонентов для того, чтобы обеспечить детальное, техническое описание функциональной спецификации для того, чтобы объяснить, как система делает то, что определено в спецификации высшего уровня.

Программное обеспечение должно быть разработано в соответствии с признанными стандартами проектирования, где это применимо. Проектные спецификации, определяя проект программного обеспечения, необходимы для изготовленных на заказ приложений: этот тип документации как правило, не требуется для конфигурируемых продуктов, для которых проект программного обеспечения как правило рассматривается и оценивается в ходе оценки поставщика.

Проект программного обеспечения выполняется на двух уровнях. На более высоком уровне он определяет программные модули (подсистемы), которые формируют полную программную систему, интерфейсы между этими модулями, а также интерфейсы к другим внешним системам. На нижнем уровне проект описывает работу отдельных программных

модулей. Для кастомизированных компонентов проектная спецификация должна документировать компоненты разработки программного обеспечения, единицы реализации, дизайн пользовательского интерфейса, дизайн интерфейса, процедуры обработки ошибок и модели физических данных.

9.5.4 Детальная Оценка Рисков

Подробная оценка рисков требуется на этапах спецификации и построения системы посредством выполнения процессного и/или функционального анализа рисков с целью идентификации рисков, которые могут повлиять на правильное или надежное функционирование системы на уровне процессов и функций соответственно.

Оценка функциональных рисков определяет соответствие нормативным требованиям и степень серьезности бизнес-рисков в сравнении с существующими функциональными возможностями системы и поддерживаемыми бизнес-процессами.

Валидационные группы вместе с владельцем бизнес-процесса или его представителями и техническими группами готовят оценку риска на основе требований пользователя и/или функциональных/конфигурационных/проектных спецификаций.

Результат оценки риска должен включать результаты процессного и / или функционального анализа риска, выполненного в соответствии с заранее определенной методологией

В отчете об оценке риска должны быть определены действия по снижению риска, включая объем тестирования и ресурс.

9.6 Фаза испытаний и приемка

Тестирование системы выполняется для проверки соответствия компьютеризированной системы требованиям, определенным до её выпуска.

Объем работ по валидации на этапе тестирования и глубина документации по результатам зависит от таких масштабирующих факторов, как системный уровень риска GMP (9.2) и результат детальной оценки риска (9.5.4), которая выявила наиболее рискованные процессы/функции, на которых должно быть сосредоточено тестирование.

Стратегия испытаний определяет соответствующий подход к испытанию конкретной системы, основанный на следующем:

- Понимание компонентов системы (категорий GAMP), общей сложности системы и новизны системы;
- Уровень GMP риска системы;
- Результаты оценки функциональных рисков;
- Результаты оценки поставщиков, если это применимо.

Стратегия испытаний может варьироваться в широком диапазоне, например, от простого ПО с низким уровнем GMP рисков до сложного ПО с высоким уровнем GMP рисков. Она должна определяться на возможно более ранних этапах жизненного цикла проекта, и предпочтительно параллельно с разработкой спецификаций системы.

Тестирование системы должно быть организовано на разных фазах, внедрения системы в непрерывный процесс контроля качества.

Тестирование включает:

- Тестирование поставщика (например, тестирование ввода в эксплуатацию, модульное и интеграционное тестирование), выполняемое поставщиком ПО в соответствии с его системой качества или предопределенным планом качества и проекта,
- Валидационное тестирование, выполняемое в квалификационной и / или производственной среде по заранее определенным протоколам для следующих этапов валидационного тестирования:
    - квалификация монтажа
    - квалификация функционирования
    - квалификация эксплуатации

В случае, если Оценка поставщика определяет, что его методы управления качеством и практики тестирования являются надлежащими, тестирование, проведенное поставщиком в рамках жизненного цикла разработки программного обеспечения, может быть использовано для сокращения усилий регулируемой компании по проверке, (только для квалификации монтажа и функционирования). Документация по испытаниям, предоставляемая поставщиком, должна быть официально оценена, рассмотрена и одобрена регулируемой компанией.

Любой подключенный прибор / оборудование и соответствующие компоненты IT-инфраструктуры, включенные в Компьютеризированную систему, проходят квалификацию до начала этапа IQ для демонстрации надлежащего функционирования и калибровки подключенных приборов.

Тестовая документация (например, протокол квалификации) должна описывать подход к предполагаемому тестированию, тестированию окружения, перечень тестов и соответствующие критерии приемлемости, результаты тестирования вместе с выявленными отклонениями (если таковые имеются) и критерии для различных этапов приемки. Результаты каждого этапа испытаний документируются в специальных отчетах.

9.6.1 Системная среда

Тесты должны выполняться в среде, квалифицированной соответствующим образом, по заранее разработанному плану тестирования с использованием разработанных тестовых спецификаций, включающих заранее определенные ожидаемые результаты.

Среды, используемые для разработки и/или внедрения автоматизированной системы, могут различаться в зависимости от категории и сложности системы.

Создание среды разработки, квалификации (также называемой средой качества или средой валидации) и производственной среды рассматривается и документируется в Конфигурационной Спецификации и верифицируется (по крайней мере, для среды квалификации и производственной среды). Для документального подтверждения того, что среда квалификации эквивалентна и производственной среде, должны быть выполнены соответствующие проверочные мероприятия.

9.6.2 Перенос данных

Перенос данных в значительной степени зависит от конкретной технологии и файловой структуры переносимых электронных записей.

Там, где это возможно, действия по переносу данных должны включать использование программных средств для автоматизации некоторых или всех операций извлечения, преобразования, загрузки и проверки. Инструменты должны быть пригодны для использования по назначению. Строгость спецификации инструмента и действий по верификации должны быть соизмеримы с рисками.

Данные должны быть проверены каждый раз, когда они переносятся (либо внутри платформы системы, либо из одной системы в другую), либо их состояние преобразуется.

Эта проверка дает объективные доказательства того, что программные средства переноса данных подходят для использования по назначению, а также обеспечивает уровень уверенности в общем процессе переноса. Типичным подходом на этом этапе является работа с относительно небольшим объемом данных, который впоследствии может быть полностью проверен, чтобы гарантировать отсутствие ошибок данных

9.6.3 Протокол квалификации монтажа

Квалификация монтажа (IQ) (также называемая конфигурационным тестированием) - это деятельность по проверке установки и конфигурации аппаратных и программных компонентов системы и соответствующей документации.

Квалификация монтажа должна осуществляться после «замораживания» конфигурации, которая подлежит проверке. Любые изменения, внесенные позднее в конфигурацию, должны пройти процедуру управления изменениями.

При Квалификации монтажа надо учитывать условия, в которых будут проводиться испытания. Как правило, настоятельно рекомендуется специальная среда тестирования; во время IQ должны быть выполнены необходимые управляющие действия, чтобы дать документальное подтверждение того, что тестовая и производственная среда эквивалентны.

Квалификация всех подключенных приборов / оборудования и соответствующей IT-инфраструктуры рассматривается в качестве предварительных условий для этапа квалификации IQ.

Протокол квалификации монтажа (IQ) определяет испытания, которые должны проводиться на компьютеризированной системе; он должен содержать по крайней мере следующие проверки:

- правильность установки аппаратного и программного обеспечения в соответствии с техническими характеристиками и базовыми показателями конфигурации системы
- соответствие настройки конфигурации тому, что указано в спецификациях конфигурации (если применимо)
- наличие документации по системе

Для стандартного программного обеспечения документация поставщика (например, руководства, инструкции) могут использоваться для разработки протокола квалификации монтажа.

9.6.4 Протокол квалификации эксплуатации

Цель Квалификации эксплуатации (OQ) состоит в том, чтобы продемонстрировать, что система и каждый из ее определенных критических функций/процессов работает, как определено в соответствующей спецификации(ах).

Тестирование должно основываться на утвержденных спецификаций (функциональные спецификации, спецификации требований пользователя и т. д.), а также результатах детальной оценки рисков для определения типологий тестов. Испытания по наихудшему сценарию проводятся для критических функций, и в них должны быть включены доказательства проведения испытаний, в частности, предельных значений параметров системы, предельных значений данных и обработки ошибок

Если система управляет регулируемыми электронными записями и подписями, протокол квалификации эксплуатации содержит также тесты, направленные на обеспечение мер контроля для обеспечения целостности данных (см. раздел 9.1.1). Кроме того, если тестирование общих нормативных требований включено в документированный контроль, выполняемый поставщиком, фаза OQ включает проверку надежности тех функциональных возможностей, которые позволяют выполнять нормативные требования (например, Контрольный след, безопасность), применимые к конкретной среде и предполагаемому использованию каждой регулируемой компании.

Каждый тест проводится с использованием заранее определенных данных и сценариев. Полученные результаты сопоставляются с ожидаемыми, выводимыми из функциональных спецификаций.

В случае использования для целей валидации автоматизированных средств тестирования, они должны быть оценены на предмет их адекватности.

9.6.5 Протокол квалификации эксплуатации

Этап квалификации эксплуатации (PQ) (также называемый проверкой требований или приемочными испытаниями пользователей) ориентирован на демонстрацию того, что система работает эффективно и воспроизводимо, пригодна для использования по назначению и что как система, так и ее операционная среда (включая пользователей) готовы к запуску в производство.

Квалификация эксплуатации PQ должна выполняться в основном назначенными представителями пользователей и должна быть ориентирована на подтверждение:

- Этапы IQ/OQ завершены и соответствующие отчеты утверждены (любое отклонение проанализировано и закрыто)
- Все связанные с системой СОП, установка/администрирование и руководства пользователя утверждены и доступны
- Все пользователи, которые могут получить доступ к системе, обучены и записи подтверждающие обучение доступны
- Доступ для каждого пользователя был создан в соответствии с его навыками и обязанностями
- Проверка бизнес-процессов, поддерживаемых системой (сквозные тесты), основана на результатах детальной оценки рисков (раздел 10.5.4)
- Восстановление системы и данных в рабочей среде (резервное копирование и восстановление данных)

Тесты PQ осуществляется в квалификационной среде. В случае, если такой подход невозможен по техническим причинам, PQ может быть выполнен непосредственно в производственной среде после повторения IQ в производственной среде.

9.6.6 Матрица Прослеживаемости

Матрица Прослеживаемости должна быть создана для демонстрации того, что:

- Бизнес-процессы были правильно переведены на системные функционалы,
- Системные функционалы и бизнес-процессы были должным образом испытаны в квалификационных тестах в соответствии с результатом детальной оценки риска

9.7 Фаза Выпуска

Решение о выпуске компьютеризированной системы в производство должно быть одобрено, по крайней мере, владельцем бизнес-процесса и службой качества. Эти роли определяют валидационный статус системы перед авторизацией развертывания в рабочей среде. Это решение должно быть официально задокументировано в разделе валидационного отчёта или в специальном документе.

9.7.1 Валидационный отчет

В валидационном отчете обобщаются действия и соответствующая документация, выпущенная для демонстрации правильного и полного выполнения процесса валидации в соответствии с планом. Валидационный отчет обеспечивает анализ данных, собранных в ходе процесса проверки, и документирует результаты деятельности по проверке, включая любое несоответствие или последующие меры.

Валидационный отчет (или Краткий Валидационный отчет) должен включать:

- Четкое заявление о том, что система проверена и выпущена для рабочего использования,
- Идентификация возможных ограничений,
- Подтверждение того, что все испытания были выполнены в соответствии с планом или утвержденным отклонением от плана,
- Измеримая оценка результатов испытаний и подтверждение соответствия критериям приемлемости системы,
- План действий (если применимо),
- Обновленный список документации / Основной список, включающий процедуры операционной среды, инструкции и элементы управления, которые регулируют использование и управление системой после её выпуска.

После утверждения валидационного отчёта реестр компьютеризированных систем должен быть обновлен, чтобы отразить подтвержденный статус системы и включить ссылку на валидационный отчет.

9.8 Вспомогательные Процессы

9.8.1 Управление Безопасностью

Процедуры безопасности должны быть определены и внедрены для обеспечения высокого уровня защиты данных от потери конфиденциальности, целостности и доступности с учётом системной среды, сетей и программам.

Следующие процессы должны выполняться на протяжении всего жизненного цикла валидации:

- Физическая безопасность, которая включает в себя все соответствующие меры предосторожности для контроля доступа и среды для защиты объектов компьютеризированных систем от кражи, разрушения, неконтролируемого изменения или нарушения.
- Логическая Безопасность:
  - Логическая безопасность включает все меры предосторожности для защиты программ и данных от несанкционированного доступа, неправильного использования или манипулирования, например, защита от вирусов, защита от внешних угроз, процедуры идентификации пользователей, контрольный журнал для созданных, измененных или удаленных данных,
  - Ролевая безопасность должна быть внедрена для обеспечения доступа к GMP данным только предварительно авторизованным операторам в соответствии с соответствующей ролью в организации, сохраняя разделение обязанностей. Процедуры управления безопасностью применяются ко всем пользователям, включая администраторов, супер-пользователей, конечных пользователей и сотрудников службы поддержки (включая сотрудников службы поддержки поставщиков),
  - Должны существовать контрольные процедуры для обеспечения:
    - Установления и поддержки ролей и обязанностей в области безопасности, политик, стандартов и процедур,
    - Выполнения мониторинга безопасности и периодического тестирования, например, ручную проверку журнала доступа к системе, автоматическое уведомление о блокировках, тестирование токенов (если таковые имеются),
    - Создания и ведения списка лиц, имеющих право доступа к системе.

Конфигурация безопасности задокументирована в спецификациях конфигурации системы или в специальном документе (например, матрице безопасности). Доступ к системе ограничен операторами с задокументированным обучением.

Меры контроля для критически важных компонентов системы (например, серверов) включаются и проверяются в процессе квалификации инфраструктуры.

9.8.2 Управление Инцидентами

Инцидент-это любое незапланированное событие, которое не позволяет (или может не позволить) или задерживает выполнение задачи, запланированной к выполнению пользователями, системой, операцией или службой. Инциденты собираются и управляются для совершения связанных действий, которые могут привести к немедленному локальному разрешению, запросу на изменение или CAPA.

Инциденты и их разрешения должны отслеживаться в ходе мониторинга эффективности как процесса, так и автоматизированной системы, в рамках которой произошел инцидент. Это прослеживание обычно выполняется с помощью журнала инцидентов.

Процесс предназначен для обеспечения структуры высокого уровня, поддерживаемой подробными СОП, которые дают рекомендации по сценариям действий (эскалации и оценки) и связанными с ними инструментами. Этот процесс может поддерживаться программными средствами.

9.8.3 Управление Изменениями

Управление изменениями применяется к компьютеризированным системам, подлежащим проверке на протяжении всего жизненного цикла системы от этапа квалификации монтажа до выхода системы «в отставку».

Управление изменениями требует процедур, которые контролируют и сообщают о реализации изменений, которые могут повлиять на элементы конфигурации (документация. аппаратное и программное обеспечение) и/или статус проверки системы. Это включает отслеживание изменений (вызванных инцидентами или запросами на изменение) от их открытия до их разрешения.

Процесс реализации изменений инициирует Управление конфигурацией, которое охватывает идентификацию, запись и отчетность об IT-компонентах, включая их версии, составляющие компоненты и отношения.

Изменения осуществляются в соответствии с заранее установленной процедурой управления изменениями.

9.8.4 Резервное Копирование и Восстановление

В соответствии с пунктом 8.2.3, резервное копирование - это процесс копирования записей, данных и программного обеспечения для защиты от потери целостности или доступности оригинала. Восстановление-это последующее восстановление записей, данных или программного обеспечения при необходимости.

Эти процедуры необходимы для обеспечения восстановления основных систем в случае сбоев системы и последующей потери данных.

Надежность процесса восстановления задокументирована в процессе проверки.

9.8.5 Соглашение об Уровне Сервиса

Для большинства GMP систем среднего или высокого уровня с поставщиком системы и / или интегратором должно быть подписано Соглашение об уровне обслуживания (СУО) для обеспечения адекватного и своевременного обслуживания при инцидентах, а также для надлежащего безопасного хранения, документация системы, созданной во время разработки и сохраняемой на сайте поставщика

Соглашение об уровне обслуживания определяет взаимную ответственность между регулируемой компанией и поставщиком вместе с соответствующими сроками.

9.8.6 Непрерывность Деятельности

Процесс обеспечения непрерывности деятельности включает меры контроля, направленные на обеспечение непрерывности поддержки важнейших процессов в случае сбоя системы (например, ручная или альтернативная система).

Для каждой системы план обеспечения непрерывности деятельности содержит следующую информацию:

- Альтернативные процедуры на случай непредвиденных обстоятельств, используемые вместо этапов процесса, которые включают доступ к компьютеризированным системам,
- Планы управления и методы принятия решений, которые будут использоваться во время аварии компьютеризированных систем,
- Идентификация с точки зрения непрерывности деятельности важных документов, которые необходимо временно хранить до восстановления работы компьютеризированных систем,
- Испытания процедур на случай непредвиденных обстоятельств.

Требование непрерывности бизнеса считается строго применимым только для тех систем, которые поддерживают критически важные по времени процессы, т. е. те системы, которые выполняют процессы, которые не могут быть прерваны без потенциального влияния на безопасность пациента, качество продукции и целостность данных. Необходимость плана обеспечения непрерывности деятельности определяется в валидационном плане.

В качестве подмножества планов обеспечения непрерывности деятельности, планы восстановления конкретных систем в случае аварии должны быть разработаны, утверждены и отработаны. В этих планах должны быть подробно изложены меры предосторожности, принимаемые для сведения к минимуму последствий бедствия, что позволит организации либо сохранить, либо быстро возобновить выполнение важнейших функций. Особое внимание предупреждению бедствий (например, обеспечение избыточности для важнейших систем) уделяется в плане аварийного восстановления.

9.8.7 Архивирование

В случае, если данные архивируются в автономном режиме (т. е. не сразу доступны пользователям), процедура архивирования определяет временные периоды и условия для архивирования данных. Процесс архивирования и извлечения должен быть задокументирован и проходить тестирование в течение жизненного цикла.

9.8.8 Периодический Обзор

Валидационный статус каждой GMP системы периодически пересматривается для того чтобы обеспечить поддержание валидированного состояния. Периодичность и глубина процесса периодического обзора определяются на основе анализа рисков, связанного с системой. Планирование валидаций включается в валидационный мастер план. Процесс периодического обзора осуществляется в соответствии с заранее установленной процедурой.

9.8.9 Процедуры обучения и использования системы

Для каждой GMP системы должны быть разработаны обязательные для выполнения СОП, определяющие использование системы и поэтапное выполнение операций. Кроме того, такие процедуры должны содержать раздел, посвященный специальным, а не рутинным действиям, соответствующим каждой системе, таким как:

- Добавление, изменение и удаление записей.

- Выполнение рутинных периодических задач (например, перестроение индекса базы данных),
- Подготовка (выбор и сортировка, определение последовательностей и т.д.) экранные запросы и печатные отчеты о системных данных,
- Триггерные управляемые пользователем интерфейсы передачи данных в / из других систем,
- Выгрузка или загрузка данных с / на рабочую станцию или устройства удаленного сбора данных из / в систему,
- Обзор Аудиторского Следа.

Учебные планы и учебные записи должны поддерживаться, чтобы продемонстрировать аудиторам, что системы используются квалифицированным и обученным персоналом

9.9 Особые требования к валидации

9.9.1 Валидация Глобальных Систем

Глобальные системы - это такие IT - системы, которые централизованно управляются и используются на нескольких площадках регулируемой компании; эти системы могут быть централизованно внедрены и выпущены или распределены для использования на каждой площадке. Для этих систем жизненный цикл валидации, рассматриваемый в рамках этой процедуры, может быть скорректирован таким образом, чтобы обеспечить максимальное централизованное создание согласованной документации и свести к минимуму усилия по валидации на уровне площадки.

Для каждой глобальной системы подход к валидации определяется в едином глобальном плане валидации, который определяет глобальные и локальные результаты. Локальная реализация может быть детализирована в плане проверки конкретного сайта, созданном в соответствии с вышеупомянутым глобальным валидационным планом.

Процесс валидации для этих систем может включать глобальный пакет валидации, ориентированный в первую очередь на обеспечение функциональной надежности системы. Каждый сайт может официально принять результат глобальной проверки и создает локальную спецификацию / документацию по тестированию, связанную с функциональными возможностями конкретного сайта, если таковые имеются. Процесс валидации должен включать в себя проверку процессов, выполняемых через систему на каждой отдельной площадке.

Глобальная документация должна быть доступна для площадки в случае инспекции. Локальный подход площадки к валидации должен утверждаться глобальной группой для обеспечения гармонизированного и согласованного подхода.

Местная команда должна быть обучена, чтобы быть в курсе стратегии, используемой для проверки на глобальном и местном уровнях.

9.9.2 Валидация «облачных» систем

При использовании «облачных» или "виртуальных" сервисов необходимо уделять внимание пониманию предоставляемых услуг, владению, извлечению, хранению и безопасности данных.

Обязанности заказчика системы (т. е. регулируемой компании) и исполнителя (поставщика IT-услуг) определяются техническим соглашением или договором. Это обеспечивает своевременный доступ к данным (включая метаданные и контрольные журналы) владельцу данных и национальным компетентным органам по запросу. Контракты с поставщиками определяют ответственность за архивирование и непрерывную читаемость данных в течение всего периода хранения (см. архивирование).

В настоящее время регулируемым компаниям предоставляются следующие виды услуг:

- Программное обеспечение как услуга (Software as a Service, SaaS) –регулируемые компании используют приложения, работающие на инфраструктуре, принадлежащей поставщику IT-услуг. Регулируемые компании не управляют и не контролируют базовую инфраструктуру или даже отдельные возможности приложений, за исключением ограниченных пользовательских параметров конфигурации приложений
- Платформа как услуга (Platform as a Service, PaaS) – регулируемые компании используют IT-инфраструктуру, размещенную поставщиком IT - услуг, для запуска приложений, созданных с использованием операционных систем, языков программирования и инструментов, поддерживаемых поставщиком IT-услуг. Регулируемые компании не управляют и не контролируют базовую облачную инфраструктуру, включая сеть, серверы, операционные системы или хранилище, но по-прежнему контролируют развернутые приложения и, возможно, конфигурации среды размещения приложений
- Инфраструктура как услуга (Infrastructure as a Service, IaaS) – владелец использует основные вычислительные ресурсы, такие как обработка, хранение, сети, где клиент может развертывать и запускать произвольное программное обеспечение, которое может включать операционные системы и приложения. Клиент не управляет базовой облачной инфраструктурой, но имеет контроль над операционными системами, хранилищем, развернутыми приложениями и, возможно, ограниченный контроль над выбранными сетевыми компонентами (например, брандмауэрами хоста).

Надежность компьютеризированной системы, используемой регулируемой компанией, всегда находится в зоне ответственности регулируемой компании, которая должна документировать соответствующий процесс валидации, используя документацию, предоставленную поставщиком системы.

Жизненный цикл валидации осуществляется в соответствии с изложенным в предыдущих разделах гарантируя, что следующие конкретные меры должным образом проверены / подтверждены:

- Оценка поставщика выполнена на месте и до определения стратегии валидации в плане валидации
- План валидации учитывает результаты этапа оценки поставщика
- Документация по валидации может использовать спецификации, документацию по квалификации монтажа (IQ) и функционирования (OQ), предоставленную поставщиком, если эти документы будут признаны адекватными при оценке поставщика

- Эффективный статус соглашения об уровне обслуживания проверен на этапе тестирования IQ
- Квалификация эксплуатации (PQ) / Приемочный тест пользователя (User Acceptance Test UAT) выполняется конечным пользователем регулируемой компании, проверяющим, что система работает по назначению пользователя (на основе URS) во всех предполагаемых рабочих диапазонах.

Выбор систем должен осуществляться на основе надежной оценки поставщиков по всем аспектам предоставляемых услуг. Допускается привлекать консультантов, обладающих знаниями в области IT, для эффективного тестирования «облачного» программного обеспечения, платформы и инфраструктуры, а также для проверки соответствия и управляемости «облачного» приложения. Аудит IT-безопасности должен быть ориентирован как минимум на следующие аспекты:

- Как поставщик уведомляет регулируемую компанию о проблемах, которые влияют на целостность данных, включая, но не ограничиваясь следующими: технические ошибки и ошибки хостинга, ошибки, связанные с нарушениями безопасности, ошибки в программном обеспечении, проблемы резервного копирования и восстановления и / или выполнения плана аварийного восстановления;
- Безопасность авторизации и требования по разделению обязанностей;
- Процесс управления изменениями для улучшений, исправлений, обновлений
- Требования к хранению данных;
- Мониторинг аудиторского следа и журнала событий (Event Log);
- Механизм управления доступом;
- Механизм идентификации и аутентификации;
- Механизм шифрования;
- Квалификация инфраструктуры (даже если инфраструктура управляется третьей стороной)
- Пакет валидации (спецификация и протоколы тестирования). Любые обнаруженные пробелы / несоответствия должны быть устранены посредством корректирующих действий, согласованных Поставщиком, и дополнительных мероприятий по валидации в рамках проекта внедрения (например, дополнительных испытаний), выполняемых регулируемой компанией.

«Облачные» приложения рассматриваются только как соответствующие категориям 4 или 5 по классификации GAMP. С точки зрения регулируемой организации конфигурация облачных приложений, должна рассматриваться как категория 4, в то же время любая пользовательская разработка интерфейсов или передачи данных, влияющих на GMP, связанная облачным приложением, должна рассматриваться как соответствующая категория 5 и должна быть испытана соответствующим образом.

Если «облачная» инфраструктура (IaaS и PaaS) была выбрана для реализации, убедитесь, что она соответствующим образом квалифицирована в соответствии с разделом 9.10, либо поставщиком и/или регулируемой компанией.

9.9.3 Валидация электронных таблиц

Каждая электронная Таблица рассматривается в качестве одиночной Компьютеризированной системы, и поэтому критические электронные таблицы подлежат инвентаризации, оценке риска и валидации соответственно.

Электронные таблицы обычно применяются для повторения алгоритма расчета; использование Excel в качестве базы данных (т. е. электронная таблица, используемая для хранения и архивирования данных GMP) запрещается, если контрольный след не отслеживается с помощью дополнительных мер.

Категория таблицы Excel по классификации GAMP зависит от типа операций, которые выполняются с GMP данными в этой таблице в соответствии со следующим:

- Категория 3 (не конфигурирована) электронная таблица просто использует собственные функции без конфигурации (например, данные валидации, условное форматирование)
- Категория 4 (конфигурирована): электронная Таблица выполняет вычисления с помощью настроенных формул (также формулы, использующие основные функции excel, например, сложение, вычитание, деление)
- Категория 5 (пользовательская): электронная Таблица использует пользовательские макросы, сложные или вложенные логические, или и схожие функции

Каждая система электронных таблиц должна использоваться с учетом следующих факторов:

- Обеспечение безопасности электронной таблицы, гарантируя, что могут быть заполнены только входные ячейки (например, формулы не могут быть намеренно или случайно перезаписаны, параметры разработки отключены).
- Настройка безопасности доступа и проверки авторизации, например, создание электронной таблицу Excel в выделенной папке, с правами доступа, определенными для всех пользователей электронной таблицы.
- Выполнение любых вычислений, связанных с точностью, отображаемой на экране и в отчетах.
- Использование переменных электронной таблицы, (в Microsoft Excel названные имена), дающих возможность создания формулы. (например, вместо включения в формулу ссылки на ячейку A4, определить A4 именем «количество» и включить строку «Количество» в формулу)
- Обеспечение правильности выполнения, резервного копированя выполняется правильно (для электронных таблиц, хранящихся в локальных каталогах).
- Защищённость ссылки на время, включая часовой пояс.
- Проверка того, что заполненная Таблица сохраняется в не редактируемом файле (например, в формате PDF)
- При использовании таблицы как шаблона, настройка должна обеспечивать её сохранение только в защищенной папке.

Результаты жизненного цикла валидации, требуемые в разделах 9.4-9.5-9.6-9.7 должны быть созданы для каждой таблицы, хотя некоторые документы могут быть объединены вместе (например, одно функциональное требование URS/FS документ).

9.10 Квалификация IT-инфраструктуры

IT-инфраструктура поддерживает сетевые системы, участвующие в производственной и управленческой деятельности предприятий компании. На квалифицированной инфраструктуре должны запускаться квалифицированные приложения.

Квалификация инфраструктуры обеспечивает документированную верификацию правильности работы и контролируемого статуса IT-инфраструктуры.

IT-инфраструктура существует для поддержки основного бизнеса, предоставляя: платформу для запуска бизнес-приложений, процессы IT-инфраструктуры, которые облегчают способную и контролируемую IT-среду, общие IT-услуги (например, офисные инструменты, средства интрасети, хранилище файлов)

Следующие этапы связаны с процессом квалификации компонентов IT-инфраструктуры:

- **Планирование**: для выполнения требуемых действий, обязанностей, процедур и сроков, гарантируя, что квалификационные мероприятия выполняются систематическим и контролируемым образом, на основе предопределенной стратегии
- **Спецификация и дизайн**: подробно описывает аппаратную и программную структуру компонентов IT-инфраструктуры, подлежащих квалификации, гарантируя, что документация, связанная с IT-инфраструктурой, организована и интегрирована, чтобы быть легко управляемой и контролируемой
- **Тестирование**: чтобы убедиться, что IT-инфраструктура обеспечивает надежную и точную работу
- **Отчетность**: для подведения итогов проведенной квалификационной деятельности
- **Функционирование**: чтобы гарантировать статус «квалифицировано»

Следующие виды деятельности жизненного цикла должны рассматриваться как обязательные для каждого компонента IT-инфраструктуры, относящегося к GMP:

- Оценка влияния на GMP
- Квалификационный План и Отчетность
- Проектная спецификация
- Испытания при квалификации монтажа (IQ) и функционирования (OQ)
- Вспомогательные процессы:
- Управление изменениями
- Управление конфигурацией
- Резервное копирование и восстановление
- Безопасность инфраструктуры
- Управление инцидентами

Решение вышеперечисленных задач для GMP компонентов позволяют обеспечить документально подтверждённое состояние контроля, необходимого для GMP IT-инфраструктуры. Документация, созданная в течение жизненного цикла, будет представлять собой квалификационную документацию по IT-инфраструктуре, которая содержит документальные доказательства надлежащей работы IT-инфраструктуры, документально подтверждая, что она управляется, как указано в применимых руководящих принципах.

Процесс квалификации IT-инфраструктуры, требуемый Правилами надлежащей производственной практики, должен осуществляться в соответствии со специальным планом.

Квалификация IT-инфраструктуры является необходимым предварительным условием валидации программного обеспечения, которая выполняется в IT-инфраструктуре.

10 ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ ДАННЫХ ДЛЯ АУТСОРСИНГОВОЙ ДЕЯТЕЛЬНОСТИ

Целостность данных играет ключевую роль в обеспечении безопасности и целостности предоставляемых извне продуктов и услуг. Меры по управлению данными подрядчика могут быть значительно ослаблены ненадежными или фальсифицированными данными, предоставленными другими партнерами по цепочке поставок. Это относится ко всем видам деятельности, переданным на аутсорсинг, включая поставщиков сырья, контрактное производство или аналитические услуги.

Первоначальная и периодическая реквалификация поставщиков и аутсорсинговой деятельности должны включать учет рисков целостности данных и соответствующие меры контроля.

Важно, чтобы организация понимала ограничения целостности данных, полученных от поставщика (например, краткие отчеты и копии / распечатки), а также проблемы дистанционного надзора. Дистанционный анализ данных в сводных отчетах является общей необходимостью; однако ограничения дистанционного анализа данных должны быть полностью поняты, чтобы обеспечить надлежащий контроль целостности данных. Важно, чтобы краткие отчеты рассматривались как передача данных, и чтобы заинтересованные стороны не полагались исключительно на данные кратких отчетов. До принятия сводных данных, оценка системы качества поставщика и соблюдение принципов целостности данных должны быть установлены путем аудита на площадке поставщика. Аудит должен дать уверенность в достоверности данных, генерируемых компанией, и включать обзор механизмов, используемых для формирования и передачи сводных данных и отчетов.

Компании должны проводить регулярные проверки рисков, связанных с поставщиками и аутсорсинговой деятельностью, периодически оценивая степень требуемых мер контроля целостности данных.

Между регулируемыми компаниями и поставщиками/подрядными организациями (например, контрактными производителями) должны быть заключены соглашения о качестве, содержащие конкретные положения по обеспечению целостности данных в рамках поддерживаемого процесса (процессов). Это может быть достигнуто путем

формирования ожиданий в области управления данными, а также установки прозрачности отчётов Исполнителя Заказчику об ошибках/отклонениях. Также должно быть установлено требование о немедленном информировании Заказчика о каких-либо сбоях целостности данных, произошедших на стороне Исполнителя. Аудиты поставщиков и, в том числе, поставщиков услуг, проводимые производителем (или третьей стороной от имени производителя), должны включать проверку мер по обеспечению целостности данных в контрактной организации.

11 РЕГУЛЯТОРНЫЕ МЕРЫ В ОТВЕТ НА НЕСООТВЕТСТВИЯ, ВЫЯВЛЕННЫЕ В ОБЛАСТИ ЦЕЛОСТНОСТИ ДАННЫХ

Недостатки, обусловленные нарушением целостности данных, могут по-разному влиять на качество продукции. Распространенность сбоя также может варьировать от действий одного сотрудника до сбоя в рамках всей проверяемой организации.

В случае обнаружения нарушения целостности данных, в первую очередь, следует рассмотреть возможность разрешения выявленных проблем и оценки рисков, связанных с проблемами целостности данных, а также рассмотрения исторических данных. В ответе компании должны быть изложены принятые меры.

Регулируемая компания должна провести детальное расследование, включая обзор всех задействованных лабораторий, производственных операций и систем, а также обоснование любой части операции, которую регулируемый пользователь предлагает исключить. В ходе расследования могут проводиться собеседования с нынешними и бывшими сотрудниками для выявления характера, масштабов и коренных причин неточностей в данных. Эти собеседования могут проводиться квалифицированной третьей стороной.

Расследование должно включать оценку, ориентированную на:

- Масштаб нарушения целостности данных на объекте, не ограничиваясь одним наблюдаемым случаем, но проверяя все другие случаи, когда нарушение могло произойти.
- Влияние нарушения целостности на безопасность пациента и качество продукции определяется с учетом рисков, связанных с текущими операциями, и любого влияния на достоверность данных, представленных в контролирующие органы, включая данные, связанные с регистрационными досье на продукцию
- Выявление корневых причин нарушения целостности данных

Корректирующие и предупреждающие действия, предпринятые для устранения уязвимостей целостности данных, и сроки реализации должны, по крайней мере, включать:

- Временные меры, описывающие действия по защите пациентов и обеспечению качества лекарственных средств, такие как уведомление клиентов, отзыв продукта, проведение дополнительного тестирования, добавление серий продукции в программу последующего изучения стабильности, пострегистрационные изменения и усиленный мониторинг претензий
- Долгосрочные меры, включающие меры по восстановлению и усовершенствованию процедур, процессов, методов, средств контроля, систем, управленческого надзора и

человеческих ресурсов (например, обучение, кадровые усовершенствования), предназначенные для обеспечения целостности данных.

12 ИСТОРИЯ ИЗМЕНЕНИЙ

Дата введения	Номер редакции	Содержание изменения
	01	Введение нового документа