Integridade de Dados:

Guia Sindusfarma para a Indústria Farmacêutica

28

Jair Calixto
Marineis Jacob

SINDUSFARMA

Mensagem da Diretoria

Quando se trata da qualidade dos medicamentos, todas as etapas do processo produtivo são importantes. Da pesquisa à fabricação, passando pelo registro, pós-registro etc., cada elo é fundamental. Por essa razão, o conceito de "integridade de dados" ganhou mais relevância nos últimos tempos, notadamente por causa da informatização de sistemas.

O Guia Sindusfarma de Integridade de Dados surgiu da necessidade de reunir num único documento informações, procedimentos e cuidados úteis para evitar falhas e riscos que possam eventualmente provocar transtornos aos laboratórios farmacêuticos e consumidores de seus produtos.

Com esta publicação, o Sindusfarma reafirma seu compromisso de contribuir para o desenvolvimento das empresas associadas e da cadeia farmacêutica. Além disso, provê todos os interessados de uma obra de amplo alcance, cujos exemplos e conceitos podem ser aplicados inclusive por outros segmentos industriais.

Nelson A. Mussolini

Presidente Executivo

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Calixto, Jair

Integridade de dados [livro eletrônico] : Guia Sindusfarma para Indústria Farmacêutica / Jair Calixto. -- 1. ed. -- São Paulo : SINDUSFARMA, 2017.

(Manuais SINDUSFARMA ; 28)

2,5 KB ; PDF.

Bibliografia

1. Banco de dados 2. Indústria farmacêutica

3. Informação - Organização 4. Informação - Sistema de armazenagem e recuperação I. Título II. Série.

17-05242 CDD-005.74

Índices para catálogo sistemático:

1. Integridade de dados : Indústria farmacêutica : Processamento de dados 005.74

Número de ISBN

978-85-60162-58-1

Colaboraram para a elaboração deste guia:

- Ana Paula Perillo
- Anderson Clayton Stevaux
- Bruno Katsuji Kawakami
- Daniel Sales
- Daniela C. Barel
- Dielen Hennig
- Eloisa de A. C. Nascimento
- Erika Maellaro
- Eunice Versolato
- Flavia Miotto Sant Anna
- Henrique Pauli
- Jorge Eduardo Sasaki
- Jozie Souza
- Juliana Mauro Agutoli
- Karina Atoji
- Karina Oliveira
- Leandro Cordeiro Rufino
- Luciane Rojas Aronovici
- Mariana Marcusso Cavalare
- Marina Rezende Rodrigues
- Michele Estricanholi
- Mirelle Zinélli Dias
- Miriam L. Watanabe
- Patricia Candido Carneiro
- Sabrina Soares Lima Guedes
- Silvia Martins
- Tiago Rolim
- Tiago Musselli Ceotto

Coordenação

- Jair Calixto

Sumário

Introdução

1. Introdução

Nos últimos anos tem surgido uma nova discussão entre as empresas, os profissionais farmacêuticos e organismos reguladores: o tema *Integridade de Dados.* O que é integridade de dados?

A definição correta será apresentada nas seções à frente, mas de modo geral, integridade de dados é o registro e gestão acurados, completos e consistentes de um dado ou informação. Esse registro pode ser em papel ou em um sistema informatizado.

A necessidade de estabelecer um guia para esse tema se deve ao fato de que os agentes reguladores normalmente atribuem elevada importância ao assunto em virtude de falhas e problemas encontrados nos processos e procedimentos relacionados com os produtos, durante inspeções de Boas Práticas de Fabricação (BPFs). Uma outra razão está relacionada aos sistemas informatizados, que atualmente introduziram outra modalidade de falha na integridade de dados, a eletrônica, distribuída por diferentes campos e áreas de um sistema informatizado.

Existe uma terceira e principal razão: a integridade de dados é parte fundamental de um Sistema Farmacêutico da Qualidade que garante ao medicamento possuir a qualidade requerida[1].

O papel deste guia será o de esclarecer os conceitos de integridade de dados e apresentar exemplos práticos e discussões sobre as ações adequadas para mitigar as falhas e eliminar os riscos inerentes à ausência de dados íntegros, em processos farmacêuticos que podem afetar a segurança do paciente.

Esse guia não tem a intenção de esgotar o assunto, nem tem o propósito de atuar como elemento para a substituição de eventual legislação emitida pelo competente órgão regulador de medicamentos.

Objetivo

2. Objetivos

O objetivo principal desse guia é prover um documento consolidado e ilustrado sobre estratégias de controle baseadas em riscos, as quais habilitam os atuais requerimentos para integridade de dados e confiabilidade, como descrito nos guias internacionais, bem como nos requisitos locais das Boas Práticas, desde o desenvolvimento do produto até a distribuição, implementadas no contexto das modernas práticas da indústria e da cadeia de distribuição globalizada.

Outros objetivos complementares do guia são:

- Facilitar a efetiva implementação dos elementos da integridade de dados dentro da rotina de planejamento e condução de inspeções de Boas Práticas;
- Prover ferramentas para harmonizar as Boas Práticas e garantir a qualidade de inspeções com respeito às expectativas da integridade de dados;
- Fornecer exemplos reais e casos práticos de falhas de integridade de dados no sistema da qualidade e;
- Fornecer medidas de controle das falhas de integridade de dados.

Nota: Esse Guia aplica-se a produtos objeto de regulação pelos órgãos de regulamentação sanitária, sendo direcionado, principalmente, às indústrias farmacêuticas. Porém, os conceitos aqui estabelecidos podem ser aplicáveis a outras indústrias, como a veterinária, a de cosméticos, de suplementos alimentares, de produtos para saúde, de saneantes e de alimentos, desde que haja exigência sanitária nesse sentido, conforme o risco sanitário envolvido e a abordagem do usuário.

Histórico

3. Histórico

O Guia FDA sobre este tema, chamado *Data Integrity and Compliance With CGMP Guidance for Industry*, de abril de 2016, define assim a integridade de dados:

"Para efeitos da presente orientação, a integridade dos dados refere-se à integralidade, consistência e precisão dos dados. Dados completos, consistentes e precisos devem ser atribuíveis, legíveis, contemporaneamente registrados, originais ou cópias fiéis, e precisos (ALCOA)".

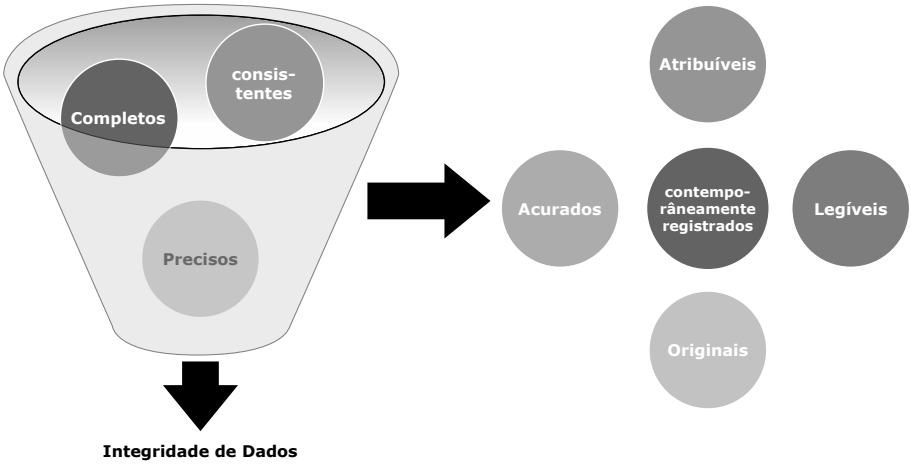


Figura 1 – Elementos que compõem a Integridade de Dados.

Assim, os dados e seus registros, em documentos utilizados na indústria farmacêutica, para serem considerados válidos e verdadeiros, devem ser:

A	• ATRIBUÍVEIS	**Confere a causa, autoria ou posse de algo**
L	• LEGÍVEIS	**Identificação imediata, sem dúvidas**
C	• CONTEMPORÂNEOS	**Registrados no momento da ocorrência**
O	• ORIGINAIS	**Originário, primitivo, autêntico**
A	• ACURADOS	**Precisos, apurados, aprimorados**

Definições e Conceitos

4. Definições e Conceitos

ALCOA: conforme o documento da ”Data Integrity and Compliance With CGMP Guidance for Industry”, da FDA de 2016.

A: atribuíveis. L: legíveis. C: contemporâneos. O: originais. A: acurados.

ALCOA +: a essa lista acima incluir: Complete (Completo), Consistent (Consistente), Enduring (Duradouro) e Available (Disponível).

Assinatura eletrônica: procedimento de autenticação eletrônico, através de ferramentas de identificação (por exemplo a senha pessoal), adotado em substituição a uma assinatura manual para aprovar uma ação ou dados autenticados em um sistema computadorizado.

***Audit log*:** registros de acessos a um sistema computadorizado contendo identificação do usuário, data e hora.

Conferência: ato ou efeito de conferir. Conferir: verificar se está correto; comparar, confrontar, verificar e confirmar se os dados registrados estão de acordo com o dado oficial.

Cópia Verdadeira: Uma cópia exata verificada contra um original.[1]

Por exemplo, cópia em papel de um registro em papel, um scan eletrônico de um registro em papel ou um dado gerado eletronicamente.

Dado: Informações derivadas ou obtidas de dados crus (por exemplo, um resultado analítico relatado).[1]

Dados Brutos: Registros originais e documentação, mantido no formato no qual eles foram originalmente gerados (ou seja, em papel ou eletrônicos), ou como uma ‘cópia’. Dados brutos devem ser simultaneamente gravados com precisão por meios permanentes. No caso de equipamentos eletrônicos básicos, que não armazenam dados eletrônicos ou possuem apenas uma saída de dados impressos (por exemplo, medidor de equilíbrio ou pH), a cópia impressa constitui os dados brutos.[1]

Dado oficial: É o dado que reflete a última posição da empresa. É o dado que deve ser apresentado a uma auditoria, conforme definido nos procedimentos vigentes na empresa.

Dado original/primário: arquivo ou o formato em que foi originalmente gerado, preservando a integridade (exatidão, integralidade, conteúdo e significado) do registro, por exemplo, registro original em papel ou observação manual, original ou arquivo de dados brutos eletrônicos de um sistema informatizado.[1]

Governança de Dados: A soma total de medidas para assegurar que os dados, independentemente do formato no qual são gerados, são registrados, processados, mantidos e usados para garantir um registro completo, consistente e preciso em todo o seu ciclo de vida.[1]

Integridade de Dados: A medida em que todos os dados são completos, consistentes e acurados através de todo ciclo de vida dos dados.[1]

Metadados: Dados que provêm informações sobre os dados brutos (como por exemplo data de criação, usuário responsável, audit trail), que permitam entender o contexto no qual o dado a qual se referem foi criado. São informações estruturadas que descrevem, explicam, ou de outra forma tornam mais fáceis para recuperar, usar ou gerenciar dados. Um valor de dados isolado, não tem sentido sem informações adicionais. Frequentemente descritos como dados sobre dados. Por exemplo, o número "23" não tem sentido sem metadados, como uma indicação da unidade de "mg". Entre outras coisas, os metadados para uma determinada fração de dados podem incluir registro de data/hora de quando os dados foram adquiridos, o ID de usuário que realizou o teste ou análise que gerou os dados, o ID do instrumento utilizado para adquirir os dados, trilha de auditoria, etc.[2]

Registro: vide definição de dado.

Registros Eletrônicos: combinação de informações de forma digital mantida por um sistema computadorizado e utilizados como único registro de uma atividade regulamentada pelas práticas BPx.

Trilha de auditoria (*Audit Trail*): Capacidade do sistema em detectar e registrar qualquer alteração em dados ou parâmetros, especificando:

- Dado criado, alterado ou excluído;
- Data e hora da ação;
- Usuário que executou a ação;
- Parâmetro original;
- Parâmetro novo;
- Texto de justificativa (caso haja);
- Identificação do ponto de acesso a partir do qual foi realizada a modificação.

A trilha é uma cronologia do "quem, o que, quando e porque" de um registro.

Glossário

5. Glossário

Termo	Significado
ALCOA	Atribuíveis, Legíveis, Contemporâneos, Originais e Acurados
ANVISA	Agência Nacional de Vigilância Sanitária
BCP	Business Continuity Plan
BPDs	Boas Práticas de Documentação
BPFs	Boas Práticas de Fabricação
BPLs	Boas Práticas de Laboratório
BPx	Sigla de Boas Práticas, onde 'x' entende-se por Fabricação, Laboratório, Distribuição etc.
CAPA	Corrective Action Preventive Action
CDS	Chromatography Data System
CGMP	Current Good Manufacturing Practice (Boas Práticas de Fabricação Atual)
FDA	Food Drug and Administration (Agência Reguladora dos Estados Unidos)
GMP	Good Manufacturing Practice (Boas Práticas de Fabricação)
GxP	Good x Practice, onde 'x' entende-se por Fabricação, Laboratório, Distribuição etc.
HPLC	High Performance Liquid Chromatography (Cromatografia Líquida de Alta Eficiência)
ICH	International Conference on Harmonisation
kg	Kilograma
mg	Miligrama
N/A	Não Aplicável
PLC	Programmable Logic Controller (Controladores Lógicos Programáveis)

Termo	Significado
RDC	Resolução da Diretoria Colegiada
RH	Recursos Humanos
SAC	Serviço de Atendimento ao Consumidor
SLA	Service Level Agreement
SST	System Suitability Test
VISA	Vigilância Sanitária

Requerimentos Gerais

6. Requerimentos Gerais

A integridade dos dados é influenciada por controles organizacionais, controles técnicos e fatores operacionais. Controles adequados devem ser implementados para evitar quebras de integridade dos dados e, portanto, garantir a confiabilidade dos dados.

A integridade dos dados BPx deve ser protegida durante o ciclo de vida dos dados. A robustez do processo utilizado para a eliminação de dado BPx deve ser assegurada de acordo com um procedimento operacional padrão documentado e de acordo com o tempo de retenção dos dados, ressaltando que o armazenamento de dados de sistemas computadorizados segue o mesmo tempo do armazenamento de dados manuais previstos na legislação aplicável.

A violação da integridade dos dados deve ser considerada seriamente, reportada à gerência de forma urgente e escalada como um evento de qualidade.

Os dados científicos, regulamentares e de conformidade para apoiar a segurança do paciente, a qualidade e fornecimento de produto final são gerados pelos processos do ciclo de vida desse. Como tal, as oportunidades para questões de integridade dos dados são mais prováveis durante a implementação desses processos. Portanto, o projeto, a configuração, a documentação e a utilização desses processos devem levar em conta os controles que impedem quebra da integridade dos dados.

Os dados BPx devem ser protegidos, limitando o acesso ao proprietário da atividade BPx e aos usuários autorizados.

Recomenda-se que o processo para autorizar o acesso do usuário aos dados BPx seja documentado em um procedimento operacional padrão e o proprietário ou delegado (*data owner*) da atividade BPx aprove o pedido assinando a documentação relevante que define as responsabilidades por analisar os dados BPx. No caso de sistemas computadorizados, pode ser escopo de procedimentos de operação do sistema e administração dos usuários. Essa aprovação possibilita verificar se o usuário foi treinado de acordo com sua responsabilidade no uso de dados BPx e que o acesso solicitado é relevante para sua função. As pessoas que utilizam os dados BPx (por qualquer meio durante seu ciclo de vida) devem ter formação, treinamento e experiência apropriados para entender a importância da integridade dos dados ao executar as atividades BPx relacionadas, algumas vezes, definida pela legislação aplicável.

6.1. Controles Organizacionais

Todos os funcionários e/ou usuários que apoiam atividades BPx devem ter uma compreensão clara sobre a integridade dos dados e seu impacto na segurança do paciente e na qualidade do produto. Eles devem entender seu papel dentro de um contexto BPx e sentir-se capacitados para garantir a integridade dos dados.

O sistema de qualidade deve incluir disposições adequadas para:

- Gestão de documentos e registos BPx;

- Boas práticas de documentação;
- Garantir que os funcionários que utilizam dados BPx estejam cientes dos requisitos de integridade de dados;
- Assegurar que os sistemas computarizados que tratam dados BPx sejam adequados para o seu uso pretendido.

Os processos de auditoria de qualidade e auditoria interna (autoinspeção) devem incluir tópicos de integridade dos dados como áreas-chave de foco durante as auditorias BPx.

Os envolvidos nas inspeções BPx devem compreender claramente as disposições da empresa para salvaguardar a integridade dos dados e serem capazes de comunicar as não conformidades encontradas. A empresa deve promover mecanismos adequados para a prevenção, detecção e escalonamento de violações da integridade dos dados BPx.

Os acordos de qualidade entre a empresa e terceiros devem prever os requisitos de integridade dos dados.

6.2. Controles Técnicos

Os sistemas computadorizados utilizados para suportar os dados BPx devem ser robustos, submetidos ao processo de validação e possuir procedimentos pertinentes, tais como: operação, backup dos dados, backup da aplicação parametrizada e/ou configurada, administração dos usuários, administração do sistema, recuperação do sistema e dados, plano de continuidade do sistema e plano de contingência. É esperado que, desde a aquisição do sistema e durante processo de validação, controles técnicos ou adequações sejam previstos para mitigar riscos de integridade de dados. Alguns exemplos de controles aplicáveis:

- *Audit trail*;
- Assinatura eletrônica;
- Backup periódico automático em servidor;
- Recuperação dos dados;
- Inviolabilidade de dados;
- Controle de acesso;
- Intertravamento de processo.

A concepção de sistemas computadorizados deve incluir disposições necessárias para salvaguardar a integridade dos dados BPx.

Para prevenir quebras de integridade de dados, intervenções de suporte corretivas ou preventivas, por indivíduos de suporte técnico durante a execução do processo BPx, devem ser claramente definidas em um procedimento operacional padrão aprovado pelo proprietário da atividade BPx.

É importante definir os atributos críticos de qualidade, considerando o *design*

e a configuração da trilha de auditoria, permitindo a captura independente de eventos de processo que são fundamentais para a investigação eficaz de eventos de qualidade (atributos críticos), que podem afetar a integridade dos dados. Para evitar potenciais problemas, o proprietário da atividade BPx ou delegado deve incorporar a revisão dos dados da trilha de auditoria nas atividades BPx relevantes. A revisão deve ser documentada.

As instalações e os sistemas devem ser configurados de forma a incentivar o cumprimento dos princípios de integridade dos dados manuais ou eletrônicos. Exemplos incluem:

- Não permitir acesso para alterar data e hora do sistema;
- Acesso a relógios para registro de eventos com tempos definidos;
- Acessibilidade dos registros BPx nos locais onde as atividades ocorrem, de modo que não ocorra registro provisório de dados e posterior transcrição para registros oficiais;
- Acesso a dados brutos para indivíduos que realizam atividades de verificação de dados;
- Controle de impressão de formulários em branco para registro de dados;
- Captura de dados automatizada ou impressoras conectadas a equipamentos como balanças;
- Proximidade das impressoras às atividades relevantes;
- Acesso a pontos de amostragem (por exemplo, para sistemas de água);
- Dupla conferência (*doble check)*.

6.3. Fatores Operacionais

Fatores operacionais são potenciais erros de execução do processo (erros humanos) ou não conformidade que resultam em desvios de documentos de qualidade oficiais, o que poderia afetar a integridade dos dados. Quando a integridade dos dados é impactada, os fatores operacionais devem ser gerenciados através dos procedimentos de não conformidades e desvios aplicáveis.

A utilização de dados BPx deve ser projetada de forma a minimizar intervenções manuais desnecessárias. O sistema deverá ser desenhado para operar de forma mais automática possível. Exemplos incluem provisão de funcionalidade para verificação de dados independente (verificação sistematizada), trilha de auditoria independente, listas suspensas padronizadas (catálogo), verificações de edição para entrada de dados etc.

Devem ser evitadas distrações e interrupções visuais e auditivas que possam afetar negativamente as atividades de registro e/ou conferência de dados BPx.

Deve ser disponibilizado tempo suficiente para completar as atividades BPx complexas para dados manuais.

Devem ser fornecidos controles adequados, supervisões ou suporte à decisão para atividades de utilização de dados BPx propensas a erros, tais como:

- Implementação de avisos e alarmes que detectam erros durante o processamento de dados para atividades BPx;
- Estabelecimento de treinamento sobre técnicas de tomada de decisão sólidas para evitar erros de decisão ao executar atividades de uso de dados BPx;
- Realização de exercícios regulares para atividades de uso de dados BPx suscetíveis a incidentes e cenários de emergência;
- Fornecimento de ferramentas de diagnóstico e auxílios à tomada de decisões, tais como fluxogramas, esquemas, calculadoras, folhas de registros oficiais, de forma que auxilie os funcionários a executar atividades complexas de registro de dados BPx;
- Garantia de que os sistemas computadorizados que envolvam as atividades de registro de dados BPx contenham exibições nítidas e tenham mecanismos efetivos de feedback para evitar erros operacionais;
- Garantia de que a transcrição de dados seja realizada de forma automática. Quando a interface entre sistemas não for possível, a transcrição do papel para o sistema eletrônico deve seguir o procedimento operacional padrão aplicável, incluindo práticas de dupla verificação.

Nota: Registros manuais originais não devem ser eliminados após serem transcritos**.**

Controles adequados devem ser implementados para evitar o descumprimento relacionado às atividades de manipulação de dados BPx, tais como:

- Treinamento e *coaching* específicos de prevenção de descumprimento de procedimentos;
- Processos e ferramentas para detecção, análise, relatórios e acompanhamento de descumprimento.

Sistema de Governança de Dados *(Data Governance)*

7. Sistema de Governança de Dados *(Data Governance)*

7.1. Definição:

A soma total das disposições destinadas a garantir que os dados, independentemente do formato em que são gerados (papel e/ou eletronicamente), são registrados, tratados, conservados e utilizados para garantir um registro completo, coerente e preciso ao longo do ciclo de vida dos dados.

A governança de dados deverá tratar da propriedade dos dados durante todo o ciclo de vida e considerar o projeto, a operação e o monitoramento de processos/sistemas para cumprimento dos princípios de integridade de dados, incluindo o controle sobre as alterações intencionais e involuntárias nas informações.

Não se espera que as organizações implementem uma abordagem forense para verificação de dados em uma base rotineira, mas, em vez disso, projetar e operar um sistema totalmente documentado que forneça um estado aceitável de controle com base no risco de integridade dos dados com fundamentação de apoio. Além da análise de dados de rotina, o sistema de governança de dados mais amplo deve garantir que as auditorias periódicas sejam capazes de detectar oportunidades para falhas de integridade de dados dentro do sistema da empresa.

7.2. Regras e Responsabilidades

O programa de governança de dados deve incluir políticas e procedimentos de governança que abordem os princípios gerais listados abaixo:

Aplicabilidade a dados em papel e eletrônicos: Os requisitos para uma boa gestão de dados e registros que garantem um controle rigoroso da validade dos dados aplicam-se igualmente aos dados em papel e eletrônicos. As organizações sujeitas a BPx devem estar plenamente conscientes de que a substituição de sistemas manuais de papel para sistemas eletrônicos não elimina por si só a necessidade de controles de gerenciamento robustos.

Aplicabilidade aos contratantes e aos contratados: Os princípios dessas diretrizes aplicam-se aos contratantes e aos contratados. Os contratantes são, em última análise, responsáveis pela solidez de todas as decisões tomadas com base nos dados BPx, incluindo os que são feitos com base nos dados fornecidos pelos contratados. Os contratantes devem, portanto, realizar a devida diligência para assegurar-se de que os contratados têm programas adequados para garantir a veracidade, integridade e confiabilidade dos dados fornecidos.

Boas práticas de documentação: Para obter decisões robustas e conjuntos de dados baseados em necessidade de ser confiável e completa, devem ser seguidas boas práticas de documentação, a fim de assegurar que todos os registros, tanto em papel como eletrônicos, permitam a reconstrução completa das atividades relacionadas.

Gestão da Governança: Para estabelecer um sistema de gestão de dados

robusto e sustentável, é importante que a alta administração assegure que os programas adequados de gestão de dados sejam implementados. A alta gestão é responsável pela implementação de sistemas e procedimentos para minimizar o potencial risco para integridade dos dados e para identificar o risco residual, utilizando técnicas de gestão.

7.2.1. Alguns exemplos práticos de políticas e procedimentos

As empresas devem possuir vários procedimentos que de alguma forma impactem integridade de dados, incluindo, mas não limitados a:

- Boas práticas de documentação;
- Abordagem para o ciclo de vida do dado;
- Validação de sistemas computadorizados;
- Gerenciamento de Riscos;
- Gerenciamento da Segurança da Informação;
- Administração do Sistema;
- Controle de mudanças, especialmente definindo tópicos relacionados à intervenção manual de bancos de dados pela Tecnologia da Informação;
- Gerenciamento de desvios;
- Backups e restauração, incluindo monitoramento de erros de backups;
- Recuperação de desastre;
- Plano de Contingência nas áreas (*BPC: Business Continuity Plan*);
- Arquivo e retenção dos dados;
- Recuperação completa dos dados, brutos e metadados, incluindo *audit trail* (trilha de auditoria);
- Revisão do *audit trail* (trilha de auditoria) na área, antes da próxima etapa de produção e principalmente antes da liberação do produto.

7.3. Elementos de governança eficaz devem incluir:

- Aplicação de princípios modernos de gestão de riscos e bons princípios de gestão de dados ao atual sistema de gestão da qualidade para integrar os elementos que asseguram a validade, a integridade e a confiabilidade dos dados. Por exemplo, o monitoramento de riscos e a aplicação de métricas de qualidade adequadas podem ajudar a gerir a conscientização necessária para uma boa tomada de decisão para reduzir os riscos de integridade dos dados;
- A administração deve assegurar que o pessoal não esteja sujeito a pressões ou incentivos comerciais, políticos, financeiros e de outra natureza organizacional que possam afetar adversamente a qualidade e a integridade de seu trabalho;

- A gerência deve alocar recursos humanos e técnicos adequados de forma que a carga de trabalho, as horas de trabalho e as pressões sobre os responsáveis pela geração de dados e manutenção de registros não aumentem os erros;
- A administração deve também sensibilizar o pessoal para a importância do seu papel na garantia da integridade dos dados e a relação destas atividades com a garantia da qualidade dos produtos e a proteção da segurança dos pacientes.

A liderança é essencial para estabelecer e manter um compromisso de toda a empresa com a confiabilidade dos dados como um elemento essencial do sistema de qualidade.

A gerência deve criar um ambiente de trabalho no qual a equipe seja encorajada a comunicar falhas e erros, incluindo questões de confiabilidade de dados, para que ações corretivas e preventivas possam ser tomadas e a qualidade dos produtos e serviços da organização sejam melhoradas. Isso inclui garantir um fluxo de informação adequado entre o pessoal em todos os níveis. A alta administração deve encorajar ativamente práticas de gerenciamento que possam ser esperadas para o relato ativo e completo de tais questões.

Análises de gestão e relatórios regulares de métricas de qualidade facilitam esses objetivos. Isso requer a designação de um gestor de qualidade que tenha acesso direto ao mais alto nível de gestão, a fim de comunicar diretamente os riscos para que a alta administração esteja ciente e possa alocar recursos para resolver quaisquer problemas. Para cumprir esse papel, a unidade de qualidade deve conduzir e reportar à administração relatórios de risco documentados e formais dos principais indicadores de desempenho do sistema de gestão da qualidade. Esses devem incluir métricas relacionadas com a integridade dos dados para ajudar a identificar oportunidades de melhoria. Por exemplo:

- Rastreamento e tendência da ocorrência de dados inválidos e discrepantes pode revelar variabilidade imprevista em processos e procedimentos anteriormente considerados robustos, oportunidades para aprimorar procedimentos analíticos e sua validação, validação de processos, treinamento de pessoal ou fornecimento de matérias-primas e componentes;
- A revisão regular do *audit trail* pode revelar um processamento incorreto dos dados, ajudar a evitar a comunicação de resultados incorretos e identificar a necessidade de formação adicional do pessoal;
- As inspeções de rotina em sistemas de registros manuais podem revelar lacunas nos controles de segurança que inadvertidamente permitem que o pessoal potencialmente altere os registros de data/hora. Essas descobertas ajudam a aumentar a conscientização dos gestores quanto à necessidade de alocar recursos para melhorar os controles;
- Monitoramento dos contratados com rastreabilidade, tendência e métricas de qualidade associadas com o contratante e que ajudam a identificar melhor os riscos que podem indicar a necessidade de um engajamento mais ativo e alocação de recursos adicionais pelo contratante para garantir que os padrões de qualidade sejam atendidos.

A alta administração é responsável pela implementação de sistemas e procedimentos para minimizar o risco potencial para a integridade dos dados e para identificar o risco residual. Os contratantes devem realizar uma revisão semelhante como parte de seu programa de garantia de fornecedores.

O esforço e os recursos atribuídos à governança de dados devem ser proporcionais ao risco à qualidade do produto e também devem ser equilibrados com outras demandas de recursos de qualidade. Os fabricantes e laboratórios analíticos devem projetar e operar um sistema que forneça um estado de controle aceitável baseado no risco de integridade dos dados e que esteja totalmente documentado com justificativa de suporte.

Sempre que sejam identificadas medidas a longo prazo para alcançar o estado desejado de controle, devem ser aplicadas medidas provisórias para mitigar os riscos e devem ser monitoradas quanto à sua eficácia. Quando são necessárias medidas temporárias ou priorização dos riscos, o risco de integridade dos dados residuais deve ser comunicado à alta administração e mantido sob revisão. Reverter de automatizado/computadorizado para sistemas de papel não irá remover a necessidade de governança de dados. Tais abordagens retrógradas são susceptíveis de aumentar a carga administrativa e o risco dos dados e impedir as iniciativas de melhoria contínua.

Nem todos os dados ou etapas de processamento têm a mesma importância para a qualidade do produto e a segurança do paciente. O gerenciamento de riscos deve ser utilizado para determinar a importância de cada etapa de processamento de dados. Uma abordagem eficaz de gerenciamento de riscos para a governança de dados considerará:

- Dados críticos (impacto na tomada de decisões e na qualidade do produto) e;
- Risco de dados (oportunidade de alteração e deleção e/ou omissão de dados e probabilidade de detecção/visibilidade das alterações pelos processos de revisão de rotina do fabricante). A partir dessa informação, podem ser implementadas medidas de controle proporcional ao risco.

A avaliação dos riscos deve considerar a vulnerabilidade dos dados quanto à alteração, falsificação, supressão, perda ou recriação involuntária ou deliberada, bem como a probabilidade de detecção de tais ações. Também deve ser considerada a garantia de uma recuperação completa dos dados em caso de desastre. As medidas de controle que impedem a atividade não autorizada que aumentam a visibilidade/detectabilidade que podem ser utilizadas como medidas de redução do risco.

As avaliações de riscos devem focar um processo de negócios, por exemplo, Produção e Qualidade, avaliar os fluxos de dados e os métodos de geração de dados e não apenas considerar a funcionalidade ou complexidade do sistema de TI.

7.3.1. Alguns exemplos práticos de Governança

Muitos sistemas de gerenciamento da segurança da informação têm impactos indiretos na integridade de dados e são de responsabilidade da Tecnolo-

gia da Informação. Controles de acesso e segurança devem ser implementados. Aqui listamos alguns exemplos, mas não devem ser limitados a:

- Utilização de sistemas que tenham conformidade com normas vigentes relacionadas a este assunto;
- Usuários personalizados e únicos, com senhas individuais e secretas de forma a assegurar o não repúdio às mudanças e/ou aplicação de assinaturas eletrônicas;
- Limite de tempo para disponibilidade da senha inicial;
- Assegurar concessão de controle de acesso com aprovação prévia;
- Assegurar adequada lista de usuários vigentes;
- Remover acessos e privilégios de acessos não mais necessários, com o máximo de automação possível interligado com sistema no RH (Recursos Humanos);
- Adoção de senhas fortes;
- Modificação de senhas padrão;
- Nova autenticação de usuários no caso de resets e após determinado tempo de inatividade;
- Definição de intervalo máximo para expiração de senhas;
- Assegurar robusto controle de usuários baseados em papéis (*role-based profiles*), por exemplo, o administrador do sistema não deve responder para nenhum gestor da área usuária de forma a evitar conflito de interesses. Se esta situação for inevitável, medidas de controles devem ser implementadas;
- Evitar conflitos de papéis, por exemplo, quem gera o dado, não deve ser o mesmo que revisa e/ou aprova;
- Os acessos devem ser concedidos de acordo com o cargo do profissional e somente deve ter acesso ao sistema após o registro do treinamento no procedimento de operação;
- Limitar o número de administradores do sistema, contudo, não deve haver somente um administrador, para que seja possível sustentação da plataforma em casos de férias, ausências etc.;
- Monitoramento de liga/desliga do *audit trail* (trilha de auditoria);
- Revisão nos logs de acesso.

7.4. Dono *versus* administradores dos dados

Para facilitar o entendimento é apresentada uma tabela de equivalência para as responsabilidades durante e após a validação de um sistema. Durante a fase de operação, estas mesmas responsabilidades são similarmente aplicáveis aos dados.

Basicamente, as responsabilidades da fase de "On Going Operation" – fase de operação do sistema, são majoritariamente relacionadas à análise e manutenção adequada dos dados. Veja a correlação abaixo:

Responsabilidades na Validação	Responsabilidades na Manutenção dos Dados
Dono do Sistema (*System Owner*)	Administrador dos Dados *(Data Stewards)*
Dono do Processo (*Process Owner*)	Dono dos Dados (*Data Owner)*

Ainda é comum encontrarmos situações onde as validações de sistemas são conduzidas sem o estabelecimento claro das responsabilidades dos papéis "dono do sistema" e "dono do processo". Se desde o início da implementação do sistema, estes papéis não estiverem bem definidos, há o risco de a companhia não ter clareza sobre as responsabilidades para a manutenção dos dados, ou seja, administrador dos dados e dono dos dados.

Nem sempre o dono do sistema, durante a implementação, será o administrador dos dados durante a fase de operação do sistema, entretanto, no geral, é comum que o dono do processo seja também o dono dos dados após a implementação do sistema. Não é recomendado que o dono dos dados também seja administrador dos dados, devido a eventual perfil de acesso especial que o administrador do dado possa ter no sistema.

7.5. Dono dos Dados

Definição:

Gestor da área, do negócio, do processo ou processos. Normalmente é o profissional com mais alta escala corporativa que detém o conhecimento do processo.

Responsabilidades do Dono dos Dados:

- Assegurar que os dados gerados pelos sistemas da sua área estejam em conformidade regulatória;
- Assegurar que os dados gerados pelos sistemas da sua área sejam devidamente analisados, incluindo trilha de auditoria (*audit trail*) antes que o produto e/ou análise passe para a próxima etapa de produção e/ou controle;
- Assegurar que os procedimentos relacionados à operação dos sistemas e análise dos dados sejam cumpridos;
- Assegurar que os profissionais da sua área têm adequado perfil de acesso parametrizado no sistema;
- Assegurar que o processo de gerenciamento de desvios relacionados aos dados do sistema da sua área siga o procedimento estabelecido na companhia, que ainda forneça informações corretas para o devido estudo de impacto. Deve ainda garantir que o ciclo se cumpra, incluindo sua finalização. As mesmas responsabilidades são pertinentes também para os processos de CAPA e controle de mudanças;

- Definir procedimento para aplicação em caso de contingência (falta do sistema que geram os dados que suportam a produção e/ou análise), assim como a comunicação corporativa adequada para entrada em contingência;
- Participar da definição da estratégia de backup, por exemplo, definir periodicidade e disponibilidade na recuperação dos dados.

7.6. Administrador dos Dados

Definição:

Gestor da área do suporte e manutenção do sistema. Normalmente é o profissional com mais alta escala corporativa responsável pela disponibilidade, suporte e manutenção dos dados, com conhecimento técnico específico para sustentar a plataforma geradora dos dados e deve fazê-lo com base em procedimentos aplicáveis aprovados, incluindo segurança da informação. No geral, entende-se que não há como assegurar a conformidade com a integridade de dados sem um administrador de dados qualificado para tal responsabilidade.

Responsabilidades do Administrador dos Dados:

- Prover adequados recursos para sustentação do sistema;
- Assegurar devido treinamento ao seu time para tratamento adequado dos dados em conformidade regulatória, enfatizando boas práticas de gerenciamento de dados;
- Assegurar que as mudanças são gerenciadas;
- Assegurar disponibilidade dos dados gerados pelo sistema;
- Assegurar correto gerenciamento de configuração – controle de versão do programa parametrizado, configurado e/ou customizado, incluindo backups das aplicações;
- Assegurar que o procedimento de backup dos dados existe e é seguido, utilizando conceitos de redundância em diferentes locais com comprovações documentais de que a política de backup está sendo cumprida;
- Assegurar que o procedimento de recuperação do sistema existe e é seguido;
- Assegurar adequada administração dos usuários do sistema com corretos perfis de acesso, principalmente quando aplicáveis a usuários de diferentes áreas da empresa;
- Assegurar a execução de testes regulares de backups e recuperação;
- Assegurar que o acordo de nível de serviço (SLA -*Service Level Agreement*) estabelecido seja cumprido, seguido, monitorado e reportado.

7.7. Auditoria do processo de data integrity e sistemas

As habilidades de pensamento crítico devem ser usadas pelos inspetores para determinar se os procedimentos de controle e revisão efetivamente alcançam seus resultados desejados. Um indicador de maturidade de governança de da-

dos é uma compreensão organizacional e aceitação de risco residual, que prioriza ações. Uma organização que acredita não existir risco de falha na integridade dos dados é improvável que tenha feito uma avaliação adequada dos riscos inerentes ao ciclo de vida dos seus dados. A abordagem da avaliação do ciclo de vida dos dados, da criticidade e do risco deve, por conseguinte, ser examinada em pormenor. Isso pode indicar potenciais modos de falha que podem ser investigados durante uma inspeção.

A eficácia das medidas de controle da integridade dos dados deve ser avaliada periodicamente como parte da autoinspeção (auditoria interna) ou de outros processos de revisão periódica. Isso deve garantir que os controles sobre o ciclo de vida dos dados estejam operando conforme o planejado.

Em adição à rotina de verificação de dados, as atividades de autoinspeção devem ser estendidas a uma revisão mais ampla das medidas de controle, incluindo:

- Verificação contínua da compreensão do pessoal sobre a integridade dos dados no contexto da proteção do paciente e garantia da manutenção de um ambiente de trabalho centrado na qualidade e na divulgação aberta das questões, por exemplo, através da revisão da formação contínua em princípios e expectativas de integridade de dados;
- Uma revisão para a consistência dos dados/resultados relatados contra a entrada de dados brutos.

Em situações em que os dados do sistema informatizado de rotina são revistos por um "relatório de exceção" validado, uma amostra baseada em risco de registros/trilhas de auditoria computadorizados deve garantir que as informações relevantes para a atividade GMP sejam relatadas conforme esperado.

7.8. Mudando a cultura da organização e treinamento de data integrity

Pode não ser apropriado ou possível relatar uma citação de inspeção relativa ao comportamento organizacional. Uma compreensão de como o comportamento influencia

(i) o incentivo para alterar, apagar ou falsificar dados e

(ii) a eficácia dos controles processuais, projetados para garantir a integridade dos dados, pode fornecer ao inspetor indicadores úteis de risco, que podem ser investigados mais adiante.

Os inspetores devem ser sensíveis à influência da cultura no comportamento organizacional e aplicar os princípios descritos nesta seção de forma adequada. Uma "cultura de qualidade" eficaz e a governança de dados podem ser diferentes na sua implementação. Dependendo da cultura, as medidas de controle de uma organização podem ser:

- "aberto" (em que a hierarquia pode ser contestada por subordinados, e a comunicação completa de uma falha sistêmica ou individual é uma expectativa de negócios);
- "Fechado" (onde falha de relatórios ou desafiar uma hierarquia é culturalmente mais difícil).

A boa governança de dados em culturas "abertas" pode ser facilitada pela autonomia dos funcionários para identificar e relatar questões através do sistema de qualidade. Em culturas "fechadas", uma maior ênfase na supervisão e revisão secundária pode ser necessária para alcançar um nível equivalente de controle devido à barreira social de comunicar informações indesejáveis. A disponibilidade de escalonamento anônimo para a alta administração também pode ser mais importante nessa situação.

A violação de integridade de dados pode ocorrer a qualquer momento, por qualquer funcionário, de modo que a gerência precisa estar atenta na detecção de problemas e compreender as razões por trás dos lapsos, quando encontrados, para permitir a investigação da quebra da integridade e pôr em prática ações corretivas e preventivas.

Há consequências de lapsos de integridade de dados que afetam os vários stakeholders (pacientes, reguladores, clientes), podendo impactar diretamente na segurança do paciente e minando a confiança na organização e em seus produtos. A conscientização dos funcionários e a compreensão dessas consequências podem ser úteis na promoção de um ambiente em que a qualidade é uma prioridade.

O monitoramento de riscos e a aplicação de métricas de qualidade adequadas podem ajudar a gerir a conscientização necessária para uma boa tomada de decisão para reduzir os riscos de integridade dos dados.

A alocação da gestão de recursos para essas melhorias pode reduzir de forma mais eficiente os riscos de integridade dos dados. Por exemplo:

(i) identificar e resolver as dificuldades técnicas do equipamento utilizado para realizar várias operações BPx pode melhorar a confiabilidade dos dados,

(ii) identificar conflitos de segurança e alocar pessoal independente para executar a administração de sistemas informatizados (incluindo gerenciamento de segurança, backup e arquivamento) reduz possíveis conflitos de interesse.

Influência Organizacional sobre o sucesso do Gerenciamento da Integridade de Dados

8. Influência Organizacional sobre o sucesso do Gerenciamento da Integridade de Dados

A organização do Gerenciamento da Integridade de Dados tem um papel fundamental em determinar a importância desse assunto e qual será a conduta de todos os seus colaboradores e empresas parceiras.

Um programa estruturado de Integridade de Dados fornecerá a todos os envolvidos um entendimento comum sobre o assunto, dando a direção necessária para que ações se desenvolvam até que o conceito faça parte da cultura da empresa.

8.1. Envolvimento do time de Liderança da Empresa

É sabido que todo o movimento que acontece na empresa precisa do apoio incondicional de sua liderança, porém nem sempre isso acontece da forma como o esperado, ou por não entendimento da importância que esse assunto possui para a sobrevivência do negócio ou por não consenso entre os diferentes departamentos envolvidos no processo.

No caso de Integridade de Dados esse assunto não somente engloba conceitos puramente administrativos, como também crenças pessoais e culturais sobre o que é certo ou errado, o que torna essa tarefa ainda mais desafiadora.

E como fazer com que todos na liderança se envolvam conforme a importância desse assunto?

Passo 1 – Base da Pirâmide:

Verifique a Missão e os Valores de sua empresa, eles serão a base para que a unificação dos conceitos de Ética e responsabilidade social seja entendida por todos os líderes.

Saia desse passo sabendo claramente em qual(quais) pilar(es) a Integridade de Dados está vinculada.

Será necessário também definir um responsável por esse assunto e que terá como responsabilidade zelar e organizar as execuções das ações subsequentes.

É importante ressaltar que não importa o nome da função, mas as responsabilidades a serem executadas por este profissional.

Diversos nomes são dados a esta função, entre elas: *Data Integrity Officer*/ Data Integrity Manager ou em português Administrador ou Gerenciador da Integridade de Dados.

Como auxílio na elaboração do que se é esperado para essa função, consulte o anexo I como exemplo.

Passo 2 – Construindo a Cultura:

Não é possível se construir uma cultura sem antes entender como as pessoas que farão parte desse movimento enxergam o tópico.

Coloque os principais líderes em uma única sala e discuta com eles seus conceitos sobre ser Íntegro, ser Ético, discuta a cultura e cheguem a um consenso comum do que realmente consideram importante sobre o tópico, sempre baseado na Missão e nos Valores previamente discutidos, que fará com que o elo da Integridade de Dados comece a se tornar mais forte. Esse é o passo que irá determinar o apoio que estas pessoas darão à implementação.

Como preparação para o próximo passo, discuta o prazo e como será a condução do Passo 3.

Quanto mais alinhada a alta diretoria estiver, melhor serão os resultados com os demais líderes.

Todos em um só discurso.

Entregável deste passo:

> Missão e Valores vinculados com conceito de Ética e Integridade comum à empresa e não somente ao indivíduo. Possíveis ações para o restante da empresa também já podem estar definidas a serem discutidas no Passo 3.

Passo 3 – Alinhando a Cultura:

Os principais líderes (alta direção) que foram envolvidos no passo 2 precisam agora disseminar este conceito para os demais líderes de sua equipe, passando o que já foi discutido e entendendo do seu time se realmente a Missão e os Valores estão representados.

É possível que nesse momento surjam novas ideias e nada impede que o processo retorne ao passo 2 para realinhamento ou que, caso o entendimento seja individual, novos conceitos sejam apresentados para embasar o que foi dito anteriormente.

O que é importante nesse passo é que todos os envolvidos tenham liberdade para colocar seus pontos de vista e que façam também sugestões de ações para que os objetivos comuns sejam alcançados.

Entregáveis deste passo?

- Todos os líderes alinhados;
- Conceitos e tópicos a serem trabalhados claramente definidos;
- Prazos determinados.

Passo 4 - Como está a cultura da empresa com relação à Integridade de Dados?

Seja realista, faça uma análise em conjunto com os líderes de sua empresa, baseado no conceito e tópicos definidos no passo 3. Analise os Comitês internos, os departamentos, passe por cada área. Use os demais tópicos desse guia para orientação.

Esta será a análise principal que permeará todas as demais ações e que fundamentará o envolvimento dos demais times da empresa:

- Time Técnico;
- Time de Comunicação e Recursos Humanos;
- Todos os Funcionários.

As pessoas que precisam ser envolvidas deverão estar definidas nesse passo.

8.2. Envolvimento do time responsável pelo tema

Até esta etapa, é esperado que a alta liderança e os líderes das áreas responsáveis pela comunicação do projeto de Integridade de Dados já estejam envolvidos em toda a preparação do que é esperado pela Empresa no tópico, porém, neste momento, este time propõe ações de como as análises feitas sairão do papel no que tange à mudança ou ajuste da cultura da empresa.

Essas ações definirão o sucesso entre o que foi desenhado e como os demais colaboradores da empresa sentirão e seguirão a Cultura.

Nessas ações de conscientização, os demais colaboradores poderão perceber os seguintes tópicos:

- Realmente este tópico possui importância ou está sendo feito somente porque a Regulamentação exige ou fomos auditados?
- O discurso dos líderes está alinhado com as práticas da empresa?
- Algo que fazia anteriormente e acreditava estar correto precisa agora ser alinhado para este "novo" pensamento?
- Agora realmente posso opinar e falar sobre o que pode ser melhorado com relação à Integridade de Dados?

8.3. Envolvimento do time técnico

Como será descrito em todos os demais tópicos deste guia, a Integridade de Dados passa por ações de Conscientização e também por ações concretas em processos que farão com que a Missão e os Valores da empresa sejam devidamente respeitados e seguidos.

Este um time técnico, que após ter passado pelo processo de conscientização, terá como seu principal papel a análise dos processos da empresa dentro da sua *expertise*.

Esse time complementará as ações previamente definidas pela liderança, detalhando os processos a serem analisados, os riscos envolvidos com relação à Integridade de Dados e as novas ações necessárias para a mitigação desses riscos.

O time técnico é um grupo multidisciplinar responsável por de fato implementar as práticas de análise de gaps, sugestões e implementações de ações mitigatórias.

Todos os técnicos aqui possuem responsabilidades, não se limitando somente a:

- Qualidade – Ciclo de vida do produto, arquivamentos etc.

- Informática/Engenharia – processos informatizados e automatizados.
- Regulatória e Pesquisa Clínica – regulamentações a serem seguidas, dependendo dos produtos fornecidos pela empresa, documentações, processos de pesquisa clínica, relacionamento com entidades etc.
- Atendimento ao Cliente – reclamações, arquivamentos, relacionamentos com clientes etc.
- Compras e Jurídico – Contratos, relacionamento com fornecedores etc.

Desse envolvimento sairão Análises de Riscos por processos, ações a serem realizadas, responsáveis e prazos, lembrando que quanto maior o número de pessoas corretamente envolvidas, maior a chance de sucesso.

8.4. Envolvimento de todos

Este é o momento em que realmente a organização estará envolvida com Integridade de Dados.

Todos, sem exceção, precisam estar alinhados com a cultura da empresa, independentemente de sua crença pessoal sobre o assunto.

Um bom plano desenvolvido e executado nesse momento fará com que todos conheçam o que a empresa considera Íntegro, Ético, certo ou errado e trará a confiança de como a empresa espera que o colaborador aja nas situações em que está exposto.

Quanto mais exemplos relacionados às tarefas do dia a dia melhor.

Todo o processo deverá ocorrer com canais abertos de comunicação para que a real situação da empresa seja verificada e que possíveis pontos de melhoria também sejam colocados pelos demais colaboradores.

8.5. Perpetuação da consciência de Integridade de Dados alcançada e desenvolvimento de novos modelos

A Cultura de Integridade de Dados na empresa já foi iniciada e agora chega o momento esperado, que é realmente viver em seu dia a dia os benefícios alcançados por essa implementação.

Para que exista uma perpetuação desses benefícios, será necessário que o trabalho em cuidar dessa Cultura permaneça e o Gerenciador da Integridade de Dados seja o responsável por organizar as ações necessárias, tais como:

8.5.1. Plano de Comunicação

Existe a necessidade de que seja elaborado um Plano de Comunicação que envolva ações a serem executadas, com periodicidade previamente determinada e com o público-alvo definido para que, continuamente, o assunto Integridade de Dados seja discutido e pensado em todas as tarefas a serem executadas.

Como sugestão, é possível elaborar um plano anual, no qual já se defina o

orçamento e os meses em que tais ações serão executadas. Isso facilitará para que o investimento necessário para as ações e as pessoas envolvidas realmente esteja disponível no momento necessário.

8.5.2. Autoinspeções

As autoinspeções garantirão que, o que foi determinado como mitigação dos riscos encontrados na análise de riscos, realmente está sendo praticado e os riscos estão sendo controlados de forma efetiva.

Como sugestão é possível inserir a autoinspeção do tópico Integridade de Dados às demais rotinas de autoinspeções já existentes na empresa.

A periodicidade dessa autoinspeção deverá fazer parte de procedimento previamente determinado.

8.5.3. Reavaliação periódica dos riscos dos processos

Dentro de uma empresa, as mudanças são constantes e as análises dos riscos relacionados ao tópico de Integridade de Dados deverão também evoluir junto com a organização.

A forma de assegurar que essa integração está acontecendo é através da revisão periódica das Análises de Riscos desenvolvidas.

O período de reavaliação deverá ser definido pela empresa e descrito em procedimento, com treinamento devidamente ministrado, que permita a sua continuidade.

Nessa reavaliação deverá ser levado em consideração:

- Possíveis mudanças de processos/procedimentos;

- Mudanças de legislações e regulamentações.

Treinamentos necessários também deverão ser analisados com relação a sua execução e efetividade.

Cada empresa é única e possui sua forma específica de trabalho e riscos inerentes ao produto entregue.

As sugestões do caminho a se seguir servem como orientação, sendo que o ponto em comum em todas as Organizações é que o apoio ao processo, tanto na implementação quanto em sua continuidade, é fundamental para o sucesso.

Princípios Gerais da Integridade de Dados

9. Princípios Gerais da Integridade de Dados

Nos últimos anos, os órgãos reguladores têm observado, durante inspeções, um aumento nas violações em BPx envolvendo Integridade de Dados. Problemas relacionados à integridade de dados levam riscos à segurança, eficácia e qualidade dos produtos, associado à quebra de confiança das agências reguladoras, dos pacientes e acionistas da empresa.

A manutenção da integridade dos dados gerados envolve um abrangente sistema de governança, o qual deve incluir políticas relevantes e treinamentos dos colaboradores sobre a importância da integridade dos dados, além de controles organizacionais (procedimentos, políticas e programas, por exemplo) e técnicos (acesso a sistemas computadorizados, por exemplo) aplicados às diferentes áreas do sistema de qualidade.

Não é esperado que as organizações implementem uma abordagem forense da verificação de dados em suas rotinas, mas sim que projetem e operem um sistema integralmente documentado, que proporcione um estado aceitável de controle com base em um racional suportado em uma análise de riscos para a integridade de dados.

Os requerimentos de integridade devem ser aplicados igualmente a dados manuais (papéis) e eletrônicos, e os sistemas devem ser projetados para assegurar a qualidade e a integridade dos dados e também encorajar a conformidade com os seus princípios.

Para assegurar que o processo de decisão seja bem informado e para verificar que a informação seja confiável, os eventos ou as ações que levaram a tais decisões devem ser bem documentados. Assim, as Boas Práticas de Documentação são a chave para garantir a integridade dos dados, além de uma parte fundamental de um estruturado Sistema de Gerenciamento da Qualidade.

Os dados que sustentam tais decisões precisam ser completos, bem como precisos, legíveis, contemporâneos, originais e atribuíveis, comumente referidos à sigla "ALCOA", conforme já mencionado acima. Esses princípios básicos e as expectativas de BPx asseguram a confiabilidade dos dados e não são conceitos novos.

O esforço e o recurso atribuídos à governança dos dados devem ser proporcionais ao risco à qualidade do produto e também balanceado com outras demandas de recursos de garantia da qualidade. O risco inerente à integridade do dado pode diferir dependendo do nível em que ele (ou sistema de geração ou uso do dado) pode ser configurado e, consequentemente, manipulado.

O bom gerenciamento de dados e registros é um elemento crítico no Sistema Farmacêutico da Qualidade e uma abordagem sistemática deve estar implementada para garantir um alto nível de segurança que, ao longo do ciclo de vida do produto, todos os registros e dados BPx são precisos, consistentes, fidedignos e confiáveis.

O programa de governança de dados deve incluir políticas e procedimentos que abordem princípios gerais para um bom gerenciamento de dados.

Gerenciamento da governança. Este tópico será tratado com mais detalhes em capítulo próprio.

Cultura de qualidade. A gestão, com suporte da unidade da qualidade, deve estabelecer e manter um ambiente de trabalho que minimize o risco de registros não conformes. Um elemento essencial para cultura da qualidade é o reporte transparente e aberto de desvios, erros, omissões em todo nível da organização, independente da hierarquia. Devem ser tomadas medidas para prevenir, detectar e corrigir deficiências no sistema e nos procedimentos que conduzam a erros, assim como, continuamente, fornecer robustez na tomada de decisão científica dentro da organização. A gestão sênior deve ativamente desencorajar quaisquer práticas esperadas que inibam o reporte transparente de tais questões, como por exemplo, as restrições hierárquicas e uma eventual "cultura interna de culpa".

Gestão do risco de qualidade e princípios científicos sólidos. Tomada de decisão robusta requer um apropriado sistema de gerenciamento da qualidade e dos riscos. Adesão a bases científicas sólidas e princípios estatísticos devem ser baseados em dados confiáveis. Por exemplo, o princípio científico de ser um observador objetivo e imparcial em relação à análise de uma amostra requer que resultados suspeitos sejam investigados e rejeitados do resultado reportado, somente se eles estiverem claramente atribuídos a uma causa identificada. Aderência a bons princípios de registro e manutenção dos dados requerem que qualquer resultado rejeitado seja registrado, junto com uma justificativa documentada para sua rejeição, e que essa documentação esteja sujeita à revisão e retenção.

Ciclo de vida dos dados. A melhoria contínua dos produtos utilizada para garantir sua segurança, eficácia e qualidade requer uma abordagem de governança que assegure o gerenciamento dos riscos e a integridade dos dados, durante todo o seu ciclo de vida.

Concepção de metodologias e sistemas de manutenção de registros. As metodologias e sistemas para manutenção dos registros, sejam eles em papel ou eletrônicos, devem ser concebidos de maneira que incentive a conformidade com os princípios de integridade de dados.

Alguns exemplos incluem, mas não estão restritos a(ao):

- Restrição de acesso à alteração de relógios para registro de eventos cronometrados;
- Acessibilidade de registros de lotes em locais em que as atividades ocorrem, de maneira que o registro de dados *ad hoc* e a transcrição posterior aos registros oficiais não sejam necessários;
- Controle sobre modelos de papel em branco para registro de dados de modo que todos os formulários possam ser reconciliados;
- Direitos de acesso do usuário, o que evita (ou executa uma trilha de auditoria) alterações nos dados;
- Captura automática de dados ou impressoras conectadas a equipamentos, como balanças;

- Proximidade a impressoras para atividades relevantes;
- Assegurar a facilidade de acesso aos locais dos pontos de amostragem (por exemplo, pontos de Sistemas) de modo que a tentação de tomar atalhos ou falsificar amostras seja minimizada;
- Acesso a dados brutos para a realização de atividade de verificação de dados pela equipe.

Manutenção de sistemas de registro. Deve ser levado em conta o progresso técnico e científico para os sistemas implementados e mantidos, tanto para registros em papel quanto para registros eletrônicos. Sistemas, procedimentos e metodologias utilizados para registro e arquivamento de dados devem ser periodicamente revisados e atualizados, caso necessário.

Sistema Farmacêutico da Qualidade. Sistema de gestão para dirigir e controlar uma empresa farmacêutica com relação à qualidade. (ICH Q10 com base na ISO 9000:2005.)

Sistemas Baseados em Papel

10. Sistemas Baseados em Papel

10.1. Considerações Gerais

Dado bruto ou dado primário de registro corresponde ao primeiro registro do dado. A informação deve ser inserida diretamente no documento BPx apropriado. Os dados primários não devem ser documentados em outros lugares, como por exemplo, uso de post-it ou blocos de anotações etc., e, em seguida, transcritas para o documento. No entanto, se os dados primários devem ser registrados em outro lugar que não diretamente no documento BPx, o documento ou registro sobre o qual ele é escrito torna-se o dado bruto original e, por consequência, deve ser retido e anexado ao documento BPx.

Todas as pessoas envolvidas em uma atividade que, ao final, obtenha-se um documento BPx (relatórios, formulários, registros de treinamentos etc.) devem assinar o documento, inclusive os profissionais executando a atividade com observadoras.

Em situações excepcionais (por exemplo, documentar intervenções por operadores da área asséptica), pode ser necessário o uso de um escriba para registrar a atividade em nome da pessoa que realmente executa a atividade ou tarefa. O registro ainda deve ser contemporâneo (no mesmo momento) com a atividade desempenhada e deve identificar a pessoa que executa a atividade observada e a pessoa que completa o registro.

O profissional que executa a atividade observada deve assinar o registro, embora se admita que esse passo homologador seja retrospectivo.

A documentação de BPx é composta de uma série de documentos e registros, garantindo a rastreabilidade e confiabilidade de informações ligadas diretamente ou não ao produto, relatando, por exemplo, a maneira e as condições nas quais cada lote de produto foi fabricado e liberado, ou de como foi conduzido um estudo de validação. Também são registros importantes para o tema, formulários impressos por computador ou gráficas, cujos itens são preenchidos durante a ocorrência de um processo ou estudo/avaliação ou ainda documentos e registros mantidos eletronicamente.

Nos registros em documentos de atividades BPx, os dados deverão estar legíveis, não sendo permitida a utilização lápis e de borrachas, qualquer tipo de corretivo, rabiscos, borrões ou escrever sobre palavras.

Se erros ocorrerem no momento do preenchimento de dados, não é permitido reescrever ou transcrever a documentação. A correção deve seguir um método padronizado para justificar o erro cometido. A correção deve ser feita logo após a complementação de cada etapa individual a ser documentada e antes de se proceder a próxima etapa.

Se um erro for cometido, este não deve ser apagado ou completamente riscado e a correção deve possibilitar a leitura da informação original. No caso de registros mantidos eletronicamente, deve existir total rastreabilidade de alterações, incluindo a identificação dos valores (novo e anterior), quem, quando e se ne-

cessário o porquê da mudança. O sistema deverá armazenar e permitir consultas a esse histórico durante todo o tempo de vigência dos dados.

São considerados críticos os itens cujo erro possa acarretar riscos à qualidade do produto e saúde do paciente. Tais itens críticos podem ser sugeridos, recomendados pelo elaborador, revisor e aprovador dos documentos e definidos através de Análise de Riscos, que deve incluir os cenários de armazenamento de dados críticos, incluindo a definição de quais são os registros críticos da área e/ou do processo.

10.2. Preenchimento dos Documentos

Todo registro realizado em documentos BPx deve ser realizado de forma clara e legível. Dados primários devem ser verdadeiros e registrados por completo, todos os campos previstos para entradas de dados devem ser preenchidos.

Os espaços em branco devem ser anulados com, por exemplo, um traço, assinatura e data. No caso de tabelas ou várias linhas com vários espaços vazios, um único traço é suficiente para inutilizar todos esses espaços, sendo necessário assinar e datar. Se o campo precisar ser deixado em branco por qualquer outro motivo que "Não aplicável" (ou N/A), uma justificativa deve ser escrita sobre o porquê o campo foi deixado em branco. Caixa de seleção indicando "N/A" pode ser usada como alternativa. Procedimentos específicos da empresa devem ser seguidos.

Os dados primários devem ser rastreáveis, por assinatura e data, para a identificação individual da observação e registro dos dados. Todos os colaboradores envolvidos no registro devem ser identificados individualmente.

Todos os registros devem conter a data com dia, mês e ano (definir modelo), visto ou assinatura de quem executou a tarefa, em seu devido campo ou em local visível em documentos onde não consta este espaço.

Na elaboração dos documentos deve haver espaço suficiente para entrada de dados.

Para dados que se repetem, não é permitido sinais de idem, flechas, ou qualquer sinal que indique repetição. O dado deve ser inserido repetidamente quantas vezes se fizerem necessários.

Todos os dados primários originais devem ser mantidos como parte de qualquer documento controlado. Nenhum registro primário deve ser anulado ou eliminado sem documentação ou explicação (por exemplo, evidências de falha do equipamento) que suporte a decisão. Dados anulados devem ser mantidos como parte do documento para fornecer a rastreabilidade completa das mudanças. Páginas anuladas ou danificadas não devem ser eliminadas.

Documentos ou formulários, necessários para capturar ou registrar dados primários devem estar prontamente disponíveis e acessíveis para o responsável pelos registros que devem ser rastreáveis exclusivamente para o número relevante de estudo, projeto, número de lote, número de equipamento etc.

10.3. Conferência de Documentos

Caso o item seja conferido por mais de uma pessoa, um racional deve estar

estabelecido para identificar de maneira individual quem são os conferentes que participaram da conferência.

No caso de cálculos, estes deverão ser realizados, documentados e conferidos tendo a participação de pelo menos duas pessoas. Para cálculos realizados por um sistema eletrônico validado, esses podem ter os resultados conferidos apenas por uma pessoa qualificada.

10.4. Registro de Assinaturas e Rubricas

Observações ou dados devem ser registrados, assinados ou rubricados e datados imediatamente após a conclusão de uma tarefa. Os dados devem ser registrados e assinados pelo indivíduo que executa a tarefa ou imputa o dado, pelo meio gravador.

O objetivo da assinatura ou rubrica é prover responsabilidade para os dados, onde rubricas ou assinaturas são usadas na execução de documentação BPx (por exemplo, registros de produção de lotes), deve haver um registro de assinaturas atualizado e prontamente disponível, que permita que para cada conjunto de rubrica ou assinatura ser associado a um nome completo.

10.5. Práticas Proibidas

As seguintes práticas são proibidas:

- Subscrever ou rasurar dados;
- Uso de "idem" ou de marcas, setas, ou quaisquer outras marcas para denotar informações repetitivas;
- Uso de caneta delével;
- O uso de corretor líquido ou fita de correção;
- Uso de papéis adesivos ("Post-it") em atividades BPx;
- Campos em branco, campos ou seções não usados que não foram invalidados com um traço assinados e datados;
- Datar retroativamente;
- Assinar ou rubricar antes de ter realmente concluído uma etapa ou entrada de dado ou tido feito uma observação;
- Assinar ou rubricar um documento em nome de terceiro, sem efetivamente ter executado a ação.

Os itens abaixo devem ser evitados, a menos que justificados:

- Registros retrospectivos ou tardios, a não ser que apoiados por outros documentos de origem, caso contrário, deve ser relatado como um desvio. Referência ao documento de origem deve acompanhar qualquer registro tardio, e deve ser assinado/rubricado e datado no momento do registro.
- Uso de e-mail como um meio de fornecer documentação de apoio (por exemplo, a uma investigação, desvio, CAPA) geralmente não é permitido,

uma vez que não é considerado um sistema validado. Assim, o uso do e-mail deve ser limitado apenas aos casos especiais em que é a única evidência disponível. Se um e-mail impresso é usado como um anexo, este deve ser assinado e datado pelo receptor do e-mail.

- Se por qualquer razão a transcrição de dados primários ocorrer (por exemplo, uma página de um documento controlado for danificada e deva ser substituída), o documento original deve ser retido e anexado ao documento transcrito juntamente com uma justificativa para a transcrição. No caso em que não pode ser anexo (por exemplo, devido a contaminação), a sua localização deve ser referenciada no documento transcrito.

Falsificação de dados é uma atividade fraudulenta e pode resultar em medidas disciplinares, inclusive demissão. Exemplos de falsificação incluem:

- Criação, alteração, gravação, ou a omissão de dados de tal forma que não representem o que de fato ocorreu;
- O registro de dados que não tenham sido executados ou não refletiram a leitura real ou observação;
- Entrar intencionalmente com uma data diferente da data atual ao registrar a conclusão de uma tarefa;
- Destruir ou anular dados originais sem a documentação e aprovação adequada de apoio;
- Assinar como tendo verificado um passo, uma tarefa, cálculo ou outra entrada sem realmente ter realizado a verificação.

10.6. Fotocópias

Fotocópias de dados brutos, que são assinados e datados e verificados por assinatura ou rubricas, são consideradas cópias "exatas" ou "verdadeiras" desses, podendo ser substituídas pela fonte original. Por exemplo, os dados registrados em papel térmico devem ser fotocopiados e unidos com os dados originais (pois o papel térmico tende a apagar e tornar-se ilegível ao longo do tempo), a menos que outras providências sejam tomadas. Para registros sequenciais ou de várias páginas, essa verificação deve aparecer em cada página.

Fotocópias de dados brutos que são anotadas apenas como "cópia" são consideradas informativas ou apenas para referência e não são consideradas "verdadeiras" ou "exatas" para que possam substituir o documento original.

10.7. Revisão e verificação de Dados Brutos

Uma revisão dos dados pode ser necessária para garantir que as entradas de dados estão completas, legíveis e livres de erros de documentação. A revisão dos dados pode não ocorrer necessariamente no momento da entrada (por exemplo, cadernos de laboratório, folhas de registros utilizadas para monitoramento ambiental, limpeza e calibração); no entanto, os dados devem ser revistos, se necessário, por uma segunda pessoa, em intervalos suficientes para garantir a qualidade e integridade dos dados.

Várias operações de verificação nas BPFs, BPLs e BPDs são realizadas para garantir a precisão das operações e entradas de dados brutos. Entradas de dados brutos manuscritos que não têm o suporte de dados emitido por equipamento (ou seja, as impressões) devem ser verificadas no momento da observação por uma segunda pessoa. Essa pessoa deve documentar a verificação no momento da observação e assinando/rubricando e datando a entrada.

10.8. Algarismos significativos e arredondamentos

Regras adequadas para definir o número correto de algarismos significativos em uma medição e arredondamento de números derivados de um cálculo devem estar descritas em procedimentos internos.

10.9. Treinamento

Os funcionários devem ser treinados nas políticas de integridade de dados, incluindo Boas Práticas de Documentação. Os gestores devem assegurar que os funcionários sejam treinados para compreender e distinguir entre o comportamento adequado e inadequado, incluindo a falsificação e potenciais consequências.

Treinamento de Boas Práticas de Documentação deve ser fornecido e documentado, como parte da integração de funcionários e terceiros, envolvidos em atividades BPx. O treinamento deve ser concluído antes que a pessoa tenha acesso aos dados e atividades.

Sistemas Computadorizados

11. Sistemas Computadorizados

11.1. Introdução

Como já se sabe, é uma tendência que sistemas computadorizados substituam operações manuais, e, por consequência, a geração de registros eletrônicos no lugar de registros em papel.

Portanto, é necessário ter a preocupação em estabelecer políticas e procedimentos de uso dos dados eletrônicos a fim de se manter a sua integridade e garantir a qualidade final do medicamento, assim como é realizado para os registros em papel.

Tratando-se de sistemas computadorizados, pode-se considerar que o ciclo de vida de seus dados eletrônicos será composto por: geração, quando aplicável processamento, uso, retenção, arquivamento/recuperação e destruição.

Pensando nesse ciclo, os próximos tópicos têm como objetivo elucidar os principais pontos que devem ser abordados ao se utilizar dados eletrônicos.

11.1.1. Criação/geração de dados

Ao se utilizar um sistema computadorizado, recomenda-se que sejam levantados que tipos de dados eletrônicos serão gerados e em quais processos estes são utilizados, para que se possa avaliar a sua criticidade e o impacto na qualidade final do produto, segurança do paciente e requerimentos regulatórios.

Como sugestão, é indicado que esteja descrito em procedimento(s) ou política(s) o que é considerado metadado, dado bruto, dado oficial, dado original/primário e cópia verdadeira, conforme já definido anteriormente. Outro ponto que pode ser visto como facilitador é serem exemplificados, de acordo com os dados de sistemas aplicáveis à empresa.

De acordo com o processo ao qual obtemos o dado bruto, este pode necessitar de processamento. Um exemplo deste caso são dados obtidos em equipamentos de laboratório, como HPLC, cujo dado bruto é utilizado como base para outros cálculos e obtenção de novos valores utilizados como resultado final.

Além disso, dados brutos podem passar por processos aos quais necessitem de conversão (por exemplo: equipamento gera valor em "mg" e resultado final deve ser expresso em "kg").

Todo este processo de conversão/processamento dos dados brutos deve ser rastreável, de forma que os dados originais utilizados no processamento não sejam alterados ou perdidos. Deve ser possível obter os resultados finais nas unidades de medida desejada, de forma que os dados originais não sejam alterados e continuem podendo ser consultados em formato do dado bruto.

Outro ponto relevante quando se trata de obtenção de dados é o formato dos arquivos gerados. Esses não devem facilitar sua alteração, recomendando-se que sejam utilizados relatórios em formato não editável e indelével.

11.2. Manutenção dos dados eletrônicos

A manutenção dos dados eletrônicos é de suma importância, pois apenas dessa forma se poderá afirmar que, mesmo com o decorrer do tempo, os dados permanecem íntegros.

Dentro do conceito de manutenção dos dados há diferentes tópicos que devem ser avaliados para que, após esta análise crítica, se possa determinar qual o nível de esforço é necessário para garantir sua manutenção. Alguns desses tópicos a serem considerados estão descritos abaixo.

11.2.1. Registro

Para que o registro de dados ocorra de forma correta e segura, é necessário que a empresa tenha compreensão do processo ao qual deu origem ao dado. Além disso, o conhecimento técnico sobre o sistema facilita que seja determinada a forma mais segura para se realizar o registro dos dados, além de mitigar limitações e vulnerabilidades.

A forma que ocorre o registro dos dados eletrônicos deve garantir que os dados sejam registrados de forma adequada, segura e completa, possibilitando que sejam armazenados e humanamente legíveis (interpretáveis) para análise posterior.

11.2.2. Guarda

Não basta apenas o registro, se não existir a possibilidade de consulta a estes dados. Nesse sentido deve-se pensar de que forma ocorre o armazenamento dos dados registrados, além de situações em que será necessário restaurá-los (*backup e restore*).

Recomenda-se que se faça uma avaliação da criticidade dos dados para definição de como será a política de backup, sendo que quanto maior o risco para a qualidade do produto e segurança do paciente, mais rígidas devem ser as medidas.

É recomendado que o processo de backup esteja oficializado por meio de procedimentos, com alguns pontos definidos de forma detalhada:

- quais os dados devem possuir *backup*: definir quais dados devem ser armazenados em *backup* e descrever onde serão armazenados, como por exemplo o caminho de pastas;
- tipo de gravação: tipo de mídia, como fita, nuvem, servidor externo. Além disso, é importante avaliar o tipo de gravação, se incremental ou diferencial;
- periodicidade que o processo de *backup* ocorre: dados são transferidos para o *backup* diariamente, semanalmente;
- local de armazenamento dos dados: definir o local de armazenamento do *backup* considerando possibilidades de desastres (como desastres naturais ou invasão por hackers);

- período de guarda: definição dos períodos de retenção de dados de acordo com a legislação de boas práticas aplicável.

Além do armazenamento, a restauração deve ter seu processo registrado em procedimento, determinando de que forma deve ocorrer, definindo os responsáveis por realizá-lo e comprovando que os processos sejam robustos.

Um ponto de atenção é a velocidade com que a tecnologia avança, pois o formato de gravação adotado na ocasião por uma empresa, por exemplo, pode tornar-se obsoleto devido essa dinâmica, impossibilitando a restauração de dados antigos.

Portanto, é uma boa prática avaliar a tecnologia utilizada e formatos de armazenamento periodicamente, de forma a se garantir que dados armazenados ainda possam ser restaurados, mesmo que haja necessidade de convertê-los para formatos mais atuais.

Se houver necessidade de alteração no formato de armazenamento, é indicado que essa seja realizada sob controle de mudança e outros documentos de suporte.

Outro ponto de atenção é quando se opta pela guarda dos dados em um terceiro, pois as responsabilidades entre a empresa contratada e a empresa proprietária dos dados devem ser estabelecidas em contrato. A empresa contratada também deverá seguir as legislações e normas adotadas pela empresa contratante em relação à integridade de dados BPx.

11.2.3. Tempo de retenção

Os registros manuais são armazenados como documentos oficiais para consultas e investigações e esses mesmos documentos são arquivados durante o tempo de retenção. Da mesma forma, os registros eletrônicos BPx também precisam ser guardados, seguindo o mesmo princípio. Portanto, o tempo de retenção de dados BPx, de acordo com a legislação aplicável, deve considerar todas as etapas envolvidas na fabricação do produto final, sendo que esses dados devem ser armazenados de forma que a integridade e a rastreabilidade sejam asseguradas.

11.2.4. Segurança do banco de dados

Conforme já citado, todos os dados BPx relevantes devem ser armazenados e a segurança do banco de dados é outro ponto de atenção.

O ideal é que esses bancos de dados se encontrem em salas dedicadas, com restrição de acesso apenas às pessoas autorizadas, fortalecendo a confiabilidade dos dados, evitando danos acidentais ou intencionais.

11.2.5. Trilha de Auditoria (*Audit Trail)*

A trilha de auditoria nada mais é que um compilado de alguns metadados, que fornece informações críticas de um dado BPx. Portanto, é necessário que esse arquivo seja armazenado e mantido íntegro, até que não seja mais necessário se manter o histórico referente ao dado BPx, de acordo com o

tempo de retenção predeterminado. Por exemplo, a deleção de uma receita de operação de um sistema vinculado a um equipamento produtivo: este deve possuir o registro de data, hora e responsável pela ação. Além disso, é recomendável que se tenha uma justificativa vinculada à deleção, para se manter o histórico do ocorrido, detalhado e robusto, em relação à alteração referente a um dado BPx realizado dento do sistema.

A trilha de auditoria pode servir como prova do que foi criado, alterado ou excluído dentro da rotina, podendo essa servir como evidência de eventuais manutenções, desvios e controles de mudanças. Além disso, pode ser um meio para detectar possíveis erros e ações fora da rotina de operação, colaborando na tomada de decisão sobre as ações corretivas/preventivas necessárias. Portanto, é recomendado que se tenha a preocupação em revisar a trilha de auditoria ao longo do uso do sistema, conferindo as ações ali registradas.

É uma boa prática que se tenha procedimento(s) descrevendo o processo de revisão e aprovação de dados a serem utilizados. A revisão deve incluir dados brutos, metadados relevantes (incluindo a trilha de auditoria) e deve ser documentada.

Esse(s) procedimento(s) deve(m) descrever as ações a serem tomadas em caso de detecção de erros ou omissões notados ao longo da revisão dos dados. É de suma importância que trilhas de auditoria não sejam geradas ou extraídas em arquivos editáveis, podendo ainda, em alguns casos, ter sua consulta restrita apenas à determinados níveis de acesso.

Em casos de trilhas de auditoria que não registrem ações de BPx, por exemplo em sistemas legados ou planilhas, deve-se adotar mitigações e/ou controles técnicos de acordo com o resultado da Análise de Riscos elaborada por equipe multidisciplinar.

11.2.6. Migração de dados

Por se tratar de sistemas computadorizados e sabendo que as tecnologias se atualizam rapidamente, em algumas situações é necessário descontinuar um sistema, substituindo-o por outro. Porém, não se pode esquecer que para cada sistema há dados vinculados, que, tratando-se de dados BPx, não podem apenas ser desconsiderados.

Portanto, em casos que ocorrem essa necessidade, é preciso planejar de que forma será realizada a migração dos dados do sistema anterior para o novo. Quando da substituição apenas de versão de sistemas, normalmente os dados anteriores conseguem ser lidos pelo novo sem problemas de incompatibilidade. Porém, há situações em que os dados armazenados estão salvos em extensão da qual o novo sistema não consegue realizar a leitura. Dessa forma, recomenda-se Análise de Riscos detalhada sobre como os dados anteriores continuarão disponíveis, mesmo que apenas para consulta.

Caso os registros eletrônicos do sistema que será descontinuado não possam ser migrados, pode-se levar em consideração mantê-lo ainda instalado, mesmo que não seja mais utilizado para operações, porém, esse permanece como "banco de dados".

Quando houver incompatibilidade entre os dados gerados pelo sistema anterior

e o novo, essa deve ser tratada com cautela, sendo indicado que todo o racional seja formalizado e apoiado por controle de mudança e Análise de Riscos.

11.3. Controle de acesso

Para manutenção da integridade dos dados, é necessário que somente pessoas autorizadas tenham acesso aos sistemas, cujos dados eletrônicos são críticos.

Dentro do conceito de controle de acesso, existem pontos em que é preciso mais atenção, pois estão diretamente ligados a controles que garantem a integridade de dados. Abaixo estão citados os principais itens a serem considerados, sendo que outros podem ser levantados, de acordo com as políticas de segurança da informação da empresa.

11.3.1. Configurações e permissões de acesso

As legislações e guias existentes possuem requerimentos em relação às políticas de controle de acesso. Recomenda-se que todo acesso seja realizado sob regras de controle de acesso, para garantir que pessoas tenham acesso apenas às funcionalidades apropriadas a seu trabalho e que essas ações estejam atribuídas a indivíduos específicos. As empresas devem ser capazes de provar/demonstrar os níveis de acesso cedidos a um funcionário e garantir que o histórico de informações relativo ao acesso desse também esteja disponível. Uma forma de se garantir que isso aconteça é adotando procedimento descrevendo a relação entre nível de acesso e permissões que esse possui.

Usuários compartilhados ou genéricos não devem ser utilizados. Quando o sistema computadorizado permitir acesso individual, este deve ser utilizado, podendo impactar na necessidade de compra de licenças adicionais.

O acesso para perfil administrador deve estar restrito ao mínimo de pessoas possíveis, não sendo permitido uso de usuários genéricos. O funcionário, ao utilizar o sistema com acesso único, permite que as ações na trilha de auditoria também sejam únicas, sendo atribuídas a indivíduos específicos.

Recomenda-se que as permissões concedidas aos administradores do sistema (como deleção ou alteração de dados ou ainda alteração de configurações do sistema) não sejam atribuídas a funcionários que possuam ligação direta com os dados em questão (geração/revisão dos dados ou aprovação destes).

11.3.2. Assinatura eletrônica

Quando se utiliza assinaturas eletrônicas, deve-se ter em mente que essa é equivalente à assinatura manuscrita, rubrica ou qualquer outro formato adotado como assinatura requerida (por exemplo para aprovação, revisão ou verificação de documentos).

Ao longo de guias e normas, é possível encontrar algumas recomendações para sistemas não biométricos:

- utilizar pelo menos dois componentes de identificação distintos, como por exemplo código de identificação e senha, sendo que quando um indivíduo

executar uma série de assinaturas, durante um único e contínuo período de acesso, a primeira inserção de assinatura eletrônica deve requerer esta de forma completa, com todos seus componentes. As assinaturas subsequentes podem ser executadas utilizando apenas um destes componentes, desde que individuais;

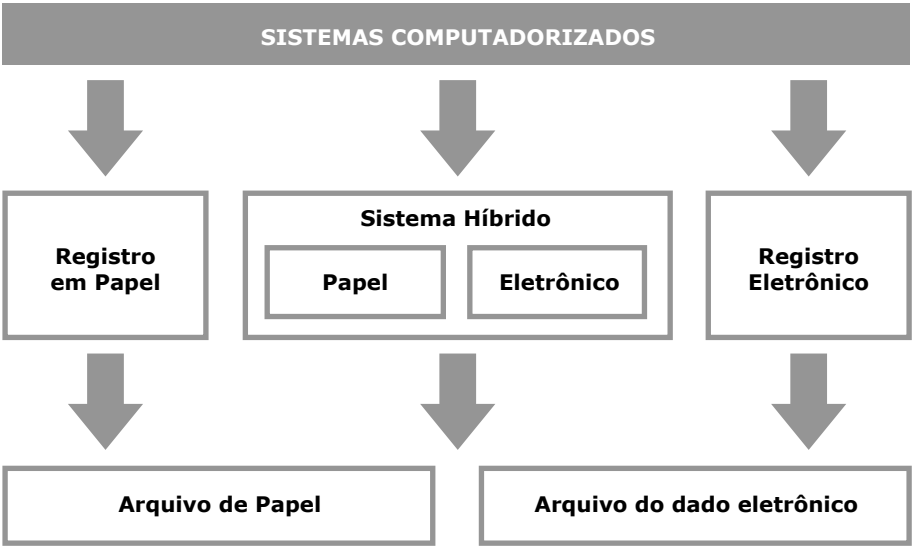
- Quando a série de assinaturas não for durante um único e contínuo período de acesso, para cada assinatura, o sistema deve requerer todos os componentes da assinatura eletrônica;
- As assinaturas eletrônicas devem ser utilizadas exclusivamente por seus proprietários e serem administradas e executadas para garantir que tentativas de uso por indivíduos que não sejam seu verdadeiro proprietário.

11.3.3. Revisão dos dados de *audit log*

Seguindo a mesma lógica de revisão de trilha de auditoria, também é recomendado que se tenha na rotina de operação a preocupação em revisar os dados de login, para que acessos fora do comum sejam detectados, sendo possível tomar as ações corretivas/preventivas necessárias.

11.4. Sistemas Híbridos

São considerados sistemas híbridos aqueles que possuem sua operação baseada em gerar registros em papel e em registros eletrônicos, de forma sincronizada (figura a seguir), por exemplo, controle de treinamento realizado por sistema, entretanto as evidências dos treinamentos possuem registro e assinatura manual.



Fonte: *Data Integrity in the FDA – Regulated Laboratory – April 2014 – tradução livre*

É um enorme desafio garantir a integridade de dados destes sistemas, pois são necessários procedimentos que sustentem o registro e armazenamento, tanto dos dados em papel quanto os dados eletrônicos. Portanto, para esse tipo de sistema são necessários os cuidados dedicados tanto à integridade dos dados em papel como para os dedicados à integridade dos dados eletrônicos (conforme orientado neste guia).

Para os sistemas híbridos deve-se ter particular atenção à inserção de dados críticos de forma manual, devido a problemas já citados, como erro de digitação ou falsificação no momento da inserção dos dados no sistema. Em sua maioria, os dados manuais têm parte na geração dos dados eletrônicos, de forma que se alterados resultam na geração de dados eletrônicos com valores diferentes e não reais pelo sistema.

Uma forma de mitigar esse problema é implementar a dupla verificação, garantindo que os dados eletrônicos obtidos, provenientes dos dados inseridos manualmente, são verdadeiros e confiáveis.

11.5. Validação de sistemas computadorizados

Se necessário, revisão, aprovação ou verificação de uma entrada de dados ou atividade concluída ou tarefa, essa deve ser executada por uma segunda pessoa diferente da pessoa que realizou a entrada ou completado a tarefa. A conferência deve ser feita no momento em que a ação ocorreu. Todos os itens críticos devem ser submetidos à dupla checagem no ato da operação. No caso de sistemas eletrônicos, essa conferência pode eventualmente ser substituída por um sistema validado operado por uma pessoa qualificada, quando algum tipo de *check* é feito pelo sistema. Nesse caso, a Análise de Riscos deve incluir o cenário de armazenamento de dados críticos, incluindo a definição de quais são os parâmetros críticos do sistema.

Em relação aos temas de integridade de dados, todos os conceitos apresentados neste guia devem ser comprovados através de validação.

Terceirização da Infraestrutura de Tecnologia da Informação e Cadeia de Abastecimento

12. Terceirização da Infraestrutura de Tecnologia da Informação e Cadeia de Abastecimento

A política de integridade de dados de um contratado, tanto para serviços de terceirização da infraestrutura de tecnologia da informação quanto para etapas da cadeia de fornecimento, possui um papel crucial na manutenção das medidas de governança de dados adotadas pela empresa contratante. É importante ressaltar que há limitações, por parte do contratante, em obter informações acerca das medidas de integridade dos dados adotadas pelo contratado, bem como a dificuldade de realizar uma supervisão remota do cumprimento desses princípios. As limitações supracitadas ocorrem, principalmente, porque a comunicação entre contratados e contratantes acontece por meio de cópias/impressões ou relatórios.

Nesse sentido, o contratante deve assegurar que o contratado sempre disponibilize "cópias verdadeiras" dos dados, tanto para documentos físicos quanto para documentos eletrônicos. As "cópias verdadeiras" de arquivos físicos devem assegurar, principalmente, a autenticidade do documento, bem como que não haja informações ausentes. As "cópias verdadeiras" de documentos virtuais devem incluir, além dos dados brutos, os respectivos metadados.

A aprovação de contratados, bem como a aceitação de dados de qualidade fornecidos por estes, deve ser precedida por uma qualificação dele, a fim de assegurar a confiabilidade na obtenção, geração e transmissão desses dados. Além disso, em função da inviabilidade de o contratante verificar os dados brutos de todos os relatórios recebidos do contratado, é essencial que o contratante realize uma qualificação robusta do fornecedor, considerando aspectos chave no que diz respeito à integridade de dados.

12.1. Acordos de qualidade/contratos

As responsabilidades e políticas de cada uma das partes, a respeito do tema integridade de dados, devem estar presentes nos acordos de qualidade ou contratos firmados entre contratado e contratante, bem como as consequências, caso o contratado recuse ou limite o acesso aos dados do contratante. De maneira geral, o contratado deve aplicar níveis de medidas equivalentes às adotadas pelo contratante.

Uma análise de competência e conformidade deve ser realizada antes do acordo ser firmado, sendo que a qualificação e requalificação do fornecedor devem levar em consideração as definições e limitações de responsabilidades definidas neste documento. Dessa forma, a fim de permitir ao contratante a auditoria do contratado, o acordo de qualidade deve definir que o contratante tenha acesso a todas as informações relevantes ao produto ou serviço contratado, assim como seus registros. Deve ser assegurado ainda que o contratante tenha acesso aos registros eletrônicos, sistemas computadorizados, documentos impressos e outros registros impressos e eletrônicos relevantes.

12.2. Qualificações dos contratados

No intuito de assegurar que os princípios de integridade de dados estão sendo

adequadamente gerenciados pelos contratados, qualificações iniciais e periódicas são uma ferramenta eficaz para assegurar a confiabilidade nos dados fornecidos, desde que as qualificações incluam no escopo verificações relacionadas ao tema. Os contratantes são os responsáveis finais pelas decisões baseadas em dados de BPx relevantes, incluindo aqueles baseados nos dados fornecidos pelo contratado. Daí a importância da qualificação dos contratantes no intuito de assegurar a veracidade, integridade e confiabilidade dos dados fornecidos. A periodicidade e abordagem da qualificação no contratado devem ser baseadas em análise de risco e, dessa forma, é fundamental que as pessoas responsáveis possuam a devida qualificação, competência, experiência e treinamento para avaliar o sistema de governança de dados do contratado.

O escopo das qualificações dos contratantes deve incluir aspectos chave e essenciais para garantir a integridade dos dados gerados e transferidos. Uma das maneiras de verificação do cumprimento dos princípios de integridade de dados pelo contratante é, durante a qualificação, confrontar relatórios sumários recebidos, tais como certificados de análise, com os dados brutos que geraram estes relatórios. Devem ser verificados, ainda, se o contratante possui uma governança de dados definida e implementada, se os sistemas computadorizados que geram dados BPx relevantes são validados, se existe a ferramenta "trilha de auditoria" presente e habilitada, se as auditorias internas incluem aspectos relevantes à integridade de dados, se existe uma política para geração de "cópias verdadeiras", entre outros aspectos.

Laboratórios de controle de qualidade têm demonstrado grandes problemas relacionados à integridade de dados e, portanto, qualificações dessa classe de contratante devem ser robustas o suficiente para assegurar confiabilidade dos dados fornecidos. Os laboratórios de microbiologia, tradicionalmente, utilizam técnicas manuais de teste e registro, prática esta que pode resultar em diversos problemas de integridade de dados. Os principais problemas relacionados a laboratórios de controle de microbiológicos são falsificação de dados, principalmente registros de valores menores do que os obtidos. Devido ao imediato descarte das amostras de microbiologia, falsificações são difíceis de serem verificadas. A verificação das amostras físicas nos incubadores, quando confrontadas com as tendências dos relatórios anteriores, podem ser indícios de falsificação. Nos laboratórios de controle de qualidade físico-química, estes erros incluem, principalmente, ausência ou desabilitação da "trilha de auditoria", ausência de níveis de acesso a sistemas informatizados, utilização de usuários únicos, injeções não oficiais antes do início do teste em métodos de cromatografia e até mesmo falta de controle sobre as modificações nos dados do sistema computadorizado.

Quando da contratação de banco de dados, importância especial deve ser dada à recuperação dos dados, bem como a localização geográfica dos dados e as leis aplicáveis àquela localização geográfica. No caso de contratação de serviços de nuvens, deve ser assegurado que o contratado seja devidamente treinado e qualificado no gerenciamento de dados e conceitos de integridade de dados.

Ações Regulatórias

13. Ações Regulatórias

O assunto Integridade de Dados é tratado em algumas normas da Anvisa, que citam a necessidade e obrigatoriedade de atendimento aos princípios da integridade dos dados, contudo, não a nomeiam desta forma. A abordagem é feita através do registro dos dados, do preenchimento da documentação e identificação dos responsáveis por cada operação ou através da intervenção na produção e controle de qualidade. A seguir alguns casos presentes na nossa legislação.

RDC nº 17/2010:

Art. 13. Boas Práticas de Fabricação é a parte da Garantia da Qualidade que assegura que os produtos são consistentemente produzidos e controlados, com padrões de qualidade apropriados para o uso pretendido e requerido pelo registro.

§ 3º As BPF determinam que:

> VI - devam ser feitos registros (manualmente e/ou por meio de instrumentos de registro) durante a produção para demonstrar que todas as etapas constantes nos procedimentos e instruções foram seguidas e que a quantidade e a qualidade do produto obtido estejam em conformidade com o esperado. Quaisquer desvios significativos devem ser registrados e investigados;
>
> VII - os registros referentes à fabricação e distribuição, que possibilitam o rastreamento completo de um lote, sejam arquivados de maneira organizada e de fácil acesso;

Art. 202. Quando os documentos exigirem a entrada de dados, estes devem ser claros, legíveis e indeléveis.

Art. 203. Toda alteração efetuada em qualquer documento deve ser assinada, datada e possibilitar a leitura da informação original.

Art. 205. Os dados podem ser registrados por meio de sistema de processamento eletrônico, por meios fotográficos ou outros meios confiáveis.

§ 1º As fórmulas mestras/fórmulas padrão e os Procedimentos Operacionais Padrão relativos ao sistema em uso devem estar disponíveis e a exatidão dos dados registrados deve ser verificada.

§ 2º Se o registro dos dados for feito por meio de processamento eletrônico, somente pessoas designadas podem modificar os dados contidos nos computadores.

§ 3º Deve haver registro das alterações realizadas.

§ 5º A entrada de dados considerados críticos, quando inserida manualmente em um sistema, deve ser conferida por outra pessoa designada.

§ 6º Os registros eletrônicos dos dados dos lotes devem ser protegidos por meio de cópias em fita magnética, microfilme, impressão em papel ou outros meios.

§ 7º Durante o período de retenção, os dados devem estar prontamente disponíveis.

Guias Garantia de Qualidade - ANVISA – 31/10/2006

Nos referidos Guias, existem algumas informações relativas ao correto gerenciamento da integridade de dados em documentos de produção. Alguns exemplos foram retirados do guia e reproduzidos a seguir.

Ordem de Produção

Deve existir uma ordem de produção para cada tamanho de lote, que seja cópia fiel da fórmula padrão/mestre;

Deve haver registro da data de ocorrência de cada etapa e dos tempos de execução, quando este puder influenciar a qualidade do produto;

Cada etapa deve ser registrada na Ordem de Produção de maneira imediata ou concomitante à obtenção dos dados ou execução das atividades; os registros não devem ser executados em momento posterior à execução das atividades;

As operações desempenhadas no processo de produção devem seguir com exatidão o determinado na Ordem de Produção;

As Ordens de Produção devem ser preenchidas à tinta e não devem conter rasuras;

Caso sejam necessárias correções, não devem ser utilizadas tintas corretivas, mas a informação errada deve ser anulada com um único risco e em seguida retificada. A pessoa que alterou as informações deve rubricar ao lado da alteração efetuada. As Ordens de Produção devem ser preparadas de forma a que evitem erros de transcrição;

Deve haver registro de verificações realizadas. Estas deverão ser efetuadas por pessoa ou sistema diferente da que realizou as atividades.

Procedimentos de Inspeção Anvisa: Pop-O-SNVS-014 Revisão: 0 Vigência: 21/07/2014

O POP–O-SNVS-014 utilizado pelo Sistema Nacional de Vigilância Sanitária (ANVISA, VISAs Estaduais e VISAs Municipais) descreve os exemplos de não conformidades que podem ser encontradas durante as inspeções, assim como, o seu grau de criticidade, que é classificado como maior, menor e crítico.

A seguir são listadas as principais não conformidades presentes neste documento, que se relacionam com integridade de dados.

Reclamações/devoluções/recolhimento

Ausência de registro, avaliação ou investigação de reclamação relacionada à qualidade, segurança e eficácia de produtos (Maior).

Testes em matérias-primas e intermediários

Evidência de falsificação ou adulteração de resultados analíticos (Crítica).

Os dados brutos não permitem a rastreabilidade de reagentes, substâncias químicas de referência, equipamentos, métodos, procedimentos de preparo e registros de cada análise (Maior).

Evidência de falsificação ou adulteração de dados de estabilidade (Crítica).

Falsificação de certificado de análise (Crítica).

Equipamentos

Ausência de registros de uso de equipamento (Maior).

Treinamento

Registros de treinamento inadequados (Menor).

Registros

Há evidência de falsificação ou adulteração de registros ou dados (Crítica).

Ausência ou não apresentação em tempo adequado de documentação de fornecedores (Maior).

Inexistência ou registros incompletos de comercialização (Maior).

Tempo de guarda insuficiente de documentos e registros (Menor).

Registros relativos a documentos de BPF incompletos ou não mantidos (Maior).

Estas são as informações concretas da Anvisa sobre integridade de dados para orientar as empresas; elas nos dão uma noção correta daquilo que a agência exige e a forma como ela classifica tais não conformidades. Adicionalmente é importante relatar que os auditores dos órgãos reguladores estão cada vez mais atentos aos registros apontados pelas empresas em documentos, bem como aos dados brutos e sua respectiva rastreabilidade. Significa dizer que as empresas devem manter esses dados de forma bem clara, coerente, organizada e acessível, para que seja possível resgatá-los a qualquer momento, bem como responder a todo tipo de questionamento feito pelo auditor sobre sua origem, destino e guarda.

Principais não conformidades encontradas

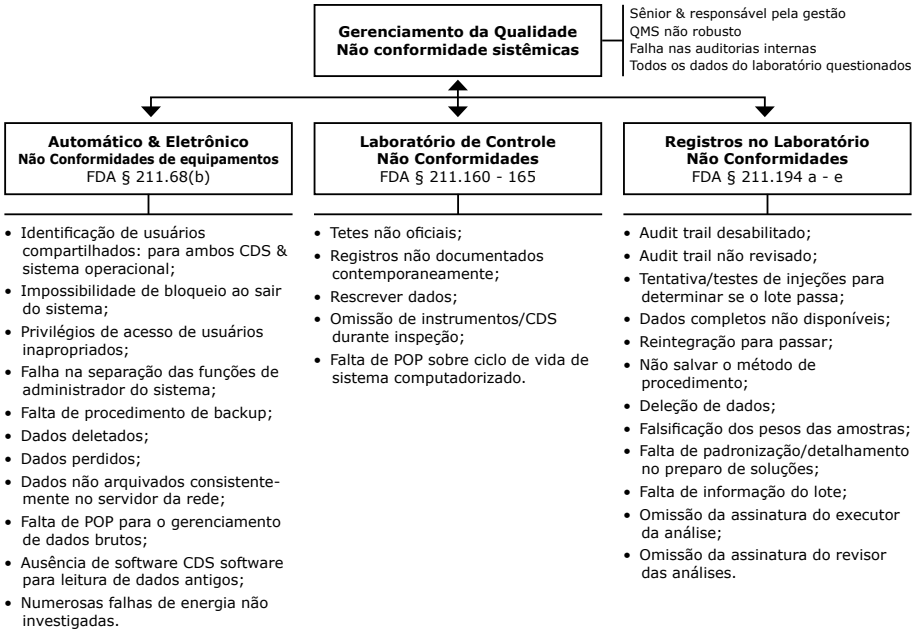
14. Principais não conformidades encontradas

14.1. No Controle da Qualidade

14.1.1. *Warning Letters - FDA*

A "*Warning Letter*" é uma notificação oficial da agência de vigilância sanitária americana *FDA* para a violação de alguma norma/regra em atividade regulada documentada durante inspeções ou investigações.

Em seguida, o resumo de algumas citações de *Warning Letters* específicas da área de Integridade de Dados em laboratórios de Controle de Qualidade:



Fonte: *Analytical Quality Control Working Group – IT Compliance Group – ECA Academy – tradução livre*

14.1.2. Más práticas *versus* Falsificação

A maioria das não conformidades de integridades de dados registradas pelos órgãos reguladores são relacionadas com Controle da Qualidade, porém aproximadamente 5% delas tem relação com falsificação de dados. As demais notificações são relacionadas com más práticas de gerenciamento de dados.

Fonte: *Analytical Quality Control Working Group – IT Compliance Group – ECA Academy*

14.1.3. Falsificação de Dados

Empresas que cometem fraudes intencionais, no geral, trabalham para trazer resultados fora de especificação para dentro de especificação, visando a liberar produto. Nesse tipo de caso, normalmente a equipe está ciente dos requisitos, operadores são treinados, mas violam a integridade para atender a empresa. A falsificação de dados é essencialmente executar testes fraudulentos, tendo objetivo de aprovar matérias-primas e lotes de produtos acabados com resultados dentro da especificação. Os órgãos reguladores já sabem que no geral, as práticas de falsificação de dados consistem em:

a) Registrar os resultados no papel sem evidência documental que sustentem tais registros;

b) Persistir com os testes até obter resultados satisfatórios. Essa prática pode ser acompanhada de deleção dos dados anteriores ou uso de amostras no lugar do padrão para injeções *SST (system suitability test)*, desta forma obtém-se uma curva de calibração falsificada de forma superficial;

   Nota: *a funcionalidade SST é utilizada para verificar resolução, eficiência da coluna e repetibilidade com padrão antes de executar análises com as amostras.*

c) Copiar um arquivo de resultado aprovado de um lote para dentro de um novo lote sem executar as análises verdadeiras;

d) Executar uma análise e calcular qual deveria ser o peso da amostra e então "fabricar" os dados da balança de forma que fiquem coerentes;

e) Executar análise cromatográfica sem nenhum cromatograma gerado, meramente reintegrando dados de lotes anteriores e imprimindo o mesmo conjunto de dados utilizando o *CDS (Chromatography Data System)*;

f) Integração manual de cromatogramas reais gerados amenizando ou aumentando picos de cromatogramas padrões, mas não das amostras ou vice-versa.

14.1.4. Más Práticas de Gerenciamento

Os restantes 95% das citações de integridade de dados são relacionadas com más práticas de gerenciamento. No geral são empresas que não estão cientes dos requisitos e possuem treinamento e procedimentos insuficientes. Alguns exemplos:

a) Ausência de qualificação de fornecedor de serviços de nuvem, incluindo impacto na integridade de dados armazenados pelo fornecedor deste tipo de serviço;

b) Área usuária ter acesso diretamente ao banco de dados ou arquivos editáveis, podendo violar e alterar os dados diretamente no banco;

c) Falta de dados completos (dados brutos + metadados);

d) Falha na assinatura dos resultados como executor do teste;

e) Falha na revisão e assinatura do revisor no pacote de documentos que expressam os resultados;

f) Usar uma balança analítica sem impressora acoplada e somente registrar os resultados manualmente;

g) Economizar dinheiro nas licenças dos usuários compartilhando contas que deveriam ser individuais de forma que o autor das análises não possa ser identificado;

h) Uso de contas de usuários genéricas;

i) Definir o dado bruto como papel quando é possível utilizar os dados do sistema computadorizado;

j) Usar estações que não são conectadas à rede;

k) Falha no backup dos registros eletrônicos;

l) Deleção de registros eletrônicos;

m) Falha para identificar o método utilizado – não são bem vistos backup em mídias móveis e CDs executados diretamente pelos usuários finais;

n) Falha no registro do peso das amostras utilizadas nas análises;

o) Registros de testes, logbooks entre outros em folhas soltas sem encadernação ou controle de cópias;

p) Os dados brutos não permitem a rastreabilidade de reagentes, substâncias químicas de referência, equipamentos, métodos, procedimentos de preparo e registros de cada análise (Maior).

Nota: *A má prática sem intenção de fraude também gera o registro de não conformidades pelo órgão regulador.*

14.2. Na Empresa

Algumas não conformidades relacionadas à integridade de dados:

a) Evidência de falsificação ou adulteração nos documentos de fabricação e embalagem (Crítica).

b) Evidência de falsificação, adulteração ou fraude em documentos relevantes as BPF (Crítica).

c) Senhas compartilhas e informadas na proteção de tela ou coladas na parede, no monitor ou ainda em notas adesivas;

d) Ausência de verificações rotineiras de dispositivos de medida ou ausência de registros de verificações (Maior).

e) Ausência de programa, de registros, ou execução incorreta da calibração de equipamentos/instrumentos críticos automáticos, mecânicos, eletrônicos ou de medição (Maior).

f) Ausência de programa ou de registros de manutenção preventiva de equipamentos críticos (Maior).

g) Requisitos inadequados de saúde dos operadores e/ou de programa de higiene (Maior).

h) Liberação de produtos aprovados pela Garantia da Qualidade sem verificação adequada da documentação/registros de fabricação e embalagem (Maior).

i) Documentos mestres de produção em desacordo com o Registro do Produto (Maior).

j) Informações imprecisas ou incompletas em documentos de lotes de fabricação ou embalagem (Maior).

k) Ausência de registros ou execução incorreta da calibração de equipamentos/instrumentos não críticos automáticos, mecânicos, eletrônicos ou de medição (Menor).

l) Registros de treinamento inadequados (Menor).

m) Documentos mestres de produção com ausência de informações relevantes (Menor).

14.3. Ações e ferramentas para mitigar riscos de falhas na integridade de dados

O projeto de adequação para mitigar riscos e falhas na integridade de dados deve se estender, pelo menos, para:

a) Pesquisa e Desenvolvimento;
b) Estudos clínicos;
c) Pesquisa clínica;
d) SAC e Farmacovigilância;
e) Assuntos regulatórios;
f) Todo site fabril, incluindo Controle e Garantia da Qualidade.

14.4. No Controle da Qualidade

14.4.1. Dados Brutos

Cópias impressas de cromatogramas geralmente não incluem registros, por exemplo, de sequência de injeção, método do instrumento, método de integração, audit trail, os quais são utilizados para criar o cromatograma e estão associados com a sua validade. Portanto, a maioria dos cromatogramas impressos não atendem os requisitos de integridade de dados e segurança da informação.

O dado bruto geralmente é extremamente importante para interpretação do resultado real da análise, e deve ser protegido como um dado crítico.

14.4.2. System Suitability Test

Todas as injeções devem fazer parte do SST e da sequência de análise.

14.5. Na Empresa

14.5.1. Definir os Dados Críticos

A maioria dos guias internacionais e nacional de validação de sistemas computadorizados orienta que os dados BPx (impacto em boas práticas) relevantes ou GxP (*impact in good practices*) são definidos pelos seguintes critérios:

a) Saúde do paciente;

b) Qualidade do produto;

c) Integridade de dados.

Os critérios acima descritos norteiam a Análise de Riscos Funcional, que definirá quais funcionalidades e itens do sistema merecem a devida atenção relacionada aos controles mitigatórios, documentais e técnicos. Na integridade de dados, utilizamos o mesmo racional analisando a criticidade dos dados gerados na empresa que se torna o caminho viável para implementação do projeto de adequação de *Data Integrity*. A definição deve responder quais dados devem ter sua integridade protegida.

De acordo com o FDA, tanto os dados gerados para atender requisitos de boas práticas quanto quaisquer dados que o setor de Qualidade avalie como críticos para liberação de produtos devem ser considerados no projeto de Integridade de Dados. Se o departamento de Qualidade determinar que um dado não é relevante para boas práticas, essa decisão deve ser documentada com justificativa técnica para sua exclusão. Isso deve se aplicar para registros eletrônicos assim como para registros em papel.

Alguns exemplos de dados que normalmente têm a integridade protegida, mas não limitados a:

d) Fotografias que acompanham reclamações sobre produtos;

e) Registros de monitoramento ambiental;

f) Registros de Qualificação e Calibração de equipamentos;

g) Registros de limpeza e manutenção de equipamentos;

h) Registros de produção de lotes;

i) Transcrições manuais de displays de equipamentos (ex: pesagem em balanças);

j) Cromatogramas de HPLC (pode ser em vários formatos);

k) Registros de inventário;

l) Registros de treinamento.

Importante registrar a avaliação de todos os registros BPx relevantes.

14.5.2. Data Integrity Assessment

Geralmente é difícil dimensionar o grau de adequação que um site exige para

as práticas de integridade de dados, portanto é interessante que a empresa se organize para fazer um levantamento e aplicar alguns questionamentos para os sistemas que geram dados críticos.

O *assessment* (análise) deve contemplar os seguintes temas macros:

a) ALCOA +;

b) Tratamento dos dados;

c) Controle de acesso;

d) Dados críticos;

e) Data Owner e *Data Steward*;

f) Backup e recuperação.

14.5.3. Mitigações

Alguns exemplos, mas não limitados à:

a) Identificação e capacitar os *Data Owners* (Donos dos Dados) e *Data Stewards* (Administradores dos Dados);

b) Treinar os funcionários para lidar de maneira apropriada com dados BPx relevantes e relatórios, treinar permanentemente a conscientização e escopo de *Data Integrity*;

c) Assegurar a veracidade dos dados reportados;

d) Enfatizar que todos os funcionários da companhia são responsáveis pela integridade de cada dado gerado na sua área e/ou etapa de produção ou análise ao qual participa;

e) Assegurar controle de acesso individual limitado e autorizado de forma a se prevenir alterações inadequadas;

f) Definir claramente os perfis de acesso;

g) Definir claramente os registros completos de cada dado crítico;

h) Implementar, controlar e revisar *audit trail* antes da liberação do produto;

i) Backup regular dos dados e da aplicação, apoiado por procedimento aprovado e usuários treinados;

j) Testes regulares de recuperação de sistema (dados e aplicação) apoiado por procedimento (incluso no processo de revisão periódica do sistema, por ex);

k) Incluir funcionalidades de segurança da informação, controle de acesso e integridade de dados no escopo da validação de sistemas;

l) Dados eletrônicos que são automaticamente salvos em memórias temporárias não atendem requisitos de Boas Práticas e de Retenção e deve ser adequado;

m) Aquisição automática de dados ou impressoras conectadas diretamente a equipamentos (ex: balanças);

n) Profissionais que realizam atividades de revisão devem ter fácil acesso a dados brutos;

o) Implementação de dupla conferência para casos de registro de dados críticos manuais;

p) Implementação de medidas de controle para evitar o acesso de profissionais de automação industrial diretamente nas portas de comunicação dos PLCs (controladores lógicos programáveis) sem prévia aprovação do Controle de Mudanças;

q) No processo documentado de descontinuidade de sistemas, prever acesso adequado e integridade de dados pelo tempo de guarda determinado pela regra regulatória do negócio.

14.5.4. Planilhas Eletrônicas

Geralmente as planilhas eletrônicas são muito fáceis de serem geradas e funcionam bem – uma vez as fórmulas inseridas com sucesso, dificilmente vemos casos de a planilha errar o cálculo. O problema é que as planilhas elaboradas em softwares de mercado (prateleira) não possuem funcionalidades de segurança da informação, controle de acesso e acabam potencializando as não conformidades nas auditorias que focam este tema.

Os órgãos reguladores esperam as seguintes ações quanto a este tema:

a) Inventário de planilhas eletrônicas críticas utilizadas em toda empresa (geralmente, há planilhas críticas no Desenvolvimento, Pesquisa Clínica, Controle da Qualidade, Garantia da Qualidade, Planejamento e Produção);

b) Validação das planilhas baseada em Análise de Riscos com o máximo de restrição possível na edição das fórmulas e nos acessos a elas. Não focar somente na validação das fórmulas e sim na proteção da planilha como um todo;

c) Substituição das planilhas pelo aumento no escopo dos sistemas que circundam as aplicações, como: inclusão dos cálculos mais comuns necessários no CQ, nos CDS (*Chromatography Data System*), *LIMS (Laboratory Information Management System)* ou *ERPs (Enterprise Resource Planning)*, *MES (Manufacturing Execution System)* ou até *BI (Business Intelligence*) para consolidação de dados;

d) Caso algumas planilhas ainda não possam ser substituídas, espera-se a inclusão das mesmas em softwares repositórios específicos que controlam o acesso e auditam a operação das células no interior da planilha – detalhes que os *GEDs* no geral não cobrem – a decisão deve ser baseada em risco.

14.5.5. Sistemas Híbridos

É chamado de sistemas híbrido, aquele sistema que gera e armazena o dado eletrônico, mas por algum motivo, o dado impresso é o dado oficial.

Recomenda-se que sistemas eletrônicos que geram e armazenam dados eletrônicos e atendem o requisito de assinatura eletrônica tenham os seus dados definidos como eletrônicos, ou seja, sistema sem papel (*paperless*), no qual a comprovação da análise ou dado, revisão e a aprovação dos dados ocorre no próprio sistema utilizando assinatura eletrônica (diferente de assinatura digital, que exige certificadoras digitais externas para autenticação – não aplicável para este tema).

A tendência no mercado mundial é, com o passar dos anos, que haja maior aderência aos sites fabris *paperless*, atualmente possível tecnologicamente, porém as questões culturais ainda fazem muitas indústrias permanecerem e optarem por dados no papel, o que dificulta a consolidação dos dados até para os indicadores de qualidade e melhoria contínua. Quanto mais os dados forem integrados e mais rápido ocorrer o acesso ao dado pelas pessoas designadas, maior a detectabilidade de tendência fora de especificação, evitando riscos à qualidade dos produtos, à saúde do paciente, ao negócio e à imagem da empresa. Esta abordagem ainda diminui a ocorrência de desvios nos lotes de produção (quanto mais etapas manuais, maiores as chances de problemas).

É interessante a utilização do sistema híbrido quando o sistema atende os requisitos de segurança da informação e integridade de dados, incluindo audit trail, porém não contempla unicamente a funcionalidade de assinatura eletrônica. Nesse caso, pode ser definido que os dados completos sejam impressos e a comprovação da análise, revisão e a aprovação dos dados ocorre manualmente no impresso, sendo esse definido como registro crítico oficial. No caso de sistema híbrido, o controle de reimpressão deve ser aplicável e/ou nova comprovação da análise, revisão e a aprovação dos dados ocorre manualmente no impresso – desde que durante a validação, for comprovado que não é possível violar os dados brutos e metadados antes da impressão.

14.5.6. Provedores de Serviços de Nuvem

Tendência mundial de tecnologia, os provedores de serviços de nuvem geram muitas dúvidas nos profissionais de validação e qualificação. Aqui seguem algumas dicas para assegurar a integridade de dados hospedados por provedores desse tipo de serviço, no mínimo:

a) Qualificar e auditar o fornecedor do serviço – a maioria dos grandes e bons provedores de soluções já possuem algumas menções de certificações que podem ajudar a definir a abordagem de auditoria (se possível) e itens a serem abordados;

b) Ao mover um sistema BPx para um provedor de serviços em nuvem, a responsabilidade regulatória permanece com a empresa farmacêutica e este processo deve ser validado – Migração de Dados com verificação qualitativa e quantitativa;

c) Criar um POP para definir os passos para escolher os provedores de serviços de nuvem;

d) Definir os papéis e responsabilidades para gerenciar um provedor de serviços de nuvem;

e) Estabelecer qual será o procedimento a ser seguido na ocorrência de atualizações ou versionamentos do sistema ou serviço;

f) Definir um plano de continuidade do negócio em caso de indisponibilidade do sistema;

g) Definir procedimento de recuperação do sistema e testar periodicamente;

h) Validar o sistema;

i) Monitorar os logs de backups.

14.5.6.1. Contrato dos Serviços de Nuvem

A chave do sucesso na aquisição de provedores de serviços de nuvem por empresas do meio farmacêutico é envolver a Garantia da Qualidade no conteúdo do contrato. É o documento e momento para definir níveis seguros de serviços. Veja algumas dicas:

a) Definir claramente as responsabilidades e papéis de controle de dados (cliente) e processamento de dados (fornecedor);

b) Incluir redundâncias e alta disponibilidade em sites regionais físicos distintos;

c) Contratar serviços automáticos de backup e entrada de redundância;

d) Acordar periodicidade de backup;

e) Especificar todos os documentos que o provedor de serviço deverá fornecer para o atendimento das regulamentações;

f) Especificar claramente prazo de armazenamento dos dados;

g) Especificar claramente as práticas de segurança adotadas;

h) Especificar claramente quais dados serão armazenados;

i) Especificar claramente política de backup e *restore*;

j) Certificações a serem atendidas;

k) Abertura do *vendor* para receber auditorias periódicas;

l) SLA (Acordo de Nível de Serviço), incluindo duração máxima de eventos de falha do sistema;

m) Acordo de tempo para testes de atualizações ou versionamentos do sistema ou serviço anterior à entrada em ambiente de produção;

n) Definir em quais países os dados estarão armazenados – estudar a legislação dos países informados, pois dependendo do caso, os governos locais são detentores automáticos dos dados;

o) Definir política de defesa contra softwares maliciosos, prevendo realização de testes de segurança periódicos, escaneamento com sistemas antivírus, atualizações de segurança, tratativa em caso de detecção, emissão de relatórios periódicos sobre a segurança;

p) Definir capacidade: nível de utilização adequado, limites e desempenho, o tempo de resposta frente a requisição de aumento ou redução da capacidade;

q) Definir gerenciamento de configurações, prevendo detalhamento dos elementos utilizados para a disponibilização do serviço, processo de manutenção da configuração estabelecida.

14.5.7. Diferença entre *backup* e *archiving*

Backup: garantir que as informações armazenadas possam ser recuperadas em casos de desastres, quando arquivos originais são perdidos, deletados ou estejam inacessíveis.

Archiving: garantir a preservação a longo prazo de dados, inclusive pelo tempo exigido de guarda de dados BPx relevante de acordo com a regra regulatória do negócio.

Conclusões

15. Conclusões

O texto foi escrito no sentido de esclarecer o assunto e prover exemplos práticos sobre não conformidades encontradas na rotina das empresas, bem como exemplos reais encontrados nas inspeções da Anvisa, de maneira a servir de referência para treinamentos e melhor compreensão do assunto.

Como citado anteriormente, o assunto é antigo, faz parte das BPFs e qualquer empresa deve ter a previsão de treinamento constante do assunto Integridade de Dados em seus documentos internos.

Treinamento, atenção e revisão constantes em BPF previnem e mitigam problemas relacionados com falhas em integridade de dados.

Deve-se ter consciência de que as falhas de integridade de dados podem levar a problemas com a segurança dos produtos e principalmente, do paciente. Nesse sentido, este tema também deveria ser incluído no processo de gestão de riscos das empresas.

Referências

16. Referências

1. **FDA** - Food and Drug Administration. Data Integrity and Compliance With CGMP Guidance for Industry DRAFT GUIDANCE. Center for Drug Evaluation and Research (CDER). Center for Biologics Evaluation and Research (CBER). Center for Veterinary Medicine (CVM). Rockville, MD, USA. 2016.

2. **ANVISA**. *Não conformidades em fabricantes de medicamentos*. Inspeções Nacionais. Brasília-DF, 2014.

3. **PIC/S**. Pharmaceutical Inspection Convention Co-Operation Scheme. *Draft Pic/S Guidance Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments* - Pi 041-1. 2016.

4. **EMA** -European Medicines Agency. *Questions and answers: Good manufacturing practice: Data integrity*. London, United Kingdom. 2016. Disponível em: http://www.ema.europa.eu/ema/index.jsp?curl=pages/regulation/q_and_a/q_and_a_detail_000027.jsp#section17. Acesso em 04/12/2016.

5. **EMA**– European Medicines Agency. *Records Management (section 4.3, 4.3.1], Policy/0026.*London, United Kingdom. 2014.

6. **ICH**– International Council for Harmonisation of Technical Requirements for Pharmaceuticals for *Human Use. ICH E6, Guideline for Good Clinical Practice (section 5.2.1, 8.1, 8.3.13). Current Step 4 version.* Brussels, Switzerland, 1996.

7. **FDA** – Food and Drug Administration. 21 CFR *Part 211, Code of Federal Regulations - Good Manufacturing Practices - section 211.188a, 211.194.2, 211.194.8.*Rockville, MD, USA. 2016.

8. **FDA** – Food and Drug Administration. *Part 11, Electronic Records; Electronic Signatures – Scope and Application (section C).* Rockville, MD, USA. 2003.

9. **FDA** – Food and Drug Administration. *Guidance for Industry - Electronic Source Data in Clinical Investigations (section I, II, IV).* Rockville, MD, USA. 2013.

10. **FDA** – Food and Drug Administration. *Guidance for Industry - Contract Manufacturing Arrangements for Drugs: Quality Agreements (section B1).* Rockville, MD, USA. 2016.

11. **EUROPEAN COMMISSION**. Health and Consumers Directorate-General – EudraLex. *Volume 4 – Guidelines to Good Manufacturing Practice Medicinal Products for Human and Veterinary Use, Annex 11: Computerised Systems – section 1, 7.2, 17*. Brussels, Switzerland. 2011.

12. **MHRA**– Medicines and Healthcare Products Regulatory Agency. *GMP Data Integrity Definitions and Guidance for Industry.* United Kingdom, 2015. 16p.

13. **WHO**. Guidance on Good Data and Record Management Practices. Draft document for comment. Working document QAS/15.624. Geneva, World Health Organization, 2015.

14. WHO. *Guidance on Good Data and Record Management Practices*. *Draft for comment*. Geneva, World Health Organization, 2015.

15. Fritz, Maxine K.; **Toscano**, George. *Data Integrity: Make Sure This Hot Topic Doesn't Burn You or Your Suppliers, Contract Manufacturers or Contract Laboratories.* Ann Arbor, USA: NSF Becker & Associates Consulting, 2014.

Sindicato da Indústria de Produtos Farmacêuticos do Estado de São Paulo
Rua Alvorada, 1.280 - Vila Olímpia
CEP 04550-004 - São Paulo/SP - Brasil
Fone: +55 11 3897-9779
Fax: +55 11 3845-0742

SINDUSFARMA

ISBN 978-85-60162-58-1