DIÁRIO OFICIAL DA UNIÃO

Publicado em: 22/08/2019 | Edição: 162 | Seção: 1 | Página: 89

Órgão: Ministério da Saúde/Agência Nacional de Vigilância Sanitária/Diretoria Colegiada

INSTRUÇÃO NORMATIVA - IN Nº 43, DE 21 DE AGOSTO DE 2019

Dispõe sobre as Boas Práticas de Fabricação complementares aos sistemas computadorizados utilizados na fabricação de Medicamentos.

A Diretoria Colegiada da Agência Nacional de Vigilância Sanitária, no uso das atribuições que lhe confere o art. 15, III e IV, aliado ao art. 7º, III e IV da Lei nº 9.782, de 26 de janeiro de 1999, e ao art. 53, VI, §§ 1º e 3º do Regimento Interno aprovado pela Resolução da Diretoria Colegiada - RDC n˚ 255, de 10 de dezembro de 2018, em reunião realizada em 20 de agosto de 2019, resolve:

CAPÍTULO I

DAS DISPOSIÇÕES INICIAIS

Seção I

Do objetivo

Art. 1º Esta Instrução Normativa possui o objetivo de adotar as diretrizes de Boas Práticas de Fabricação relacionadas aos sistemas computadorizados do Esquema de Cooperação em Inspeção Farmacêutica, PIC/S, como requisitos complementares a serem seguidos na fabricação de medicamentos em adição às Diretrizes Gerais de Boas Práticas de Fabricação de Medicamentos.

Seção II

Da abrangência

Art. 2º Esta Instrução Normativa se aplica a todas as formas de sistemas computadorizados utilizados como parte de atividades reguladas pelas Boas Práticas de Fabricação de medicamentos, incluindo os medicamentos experimentais.

Seção III

Das definições

Art. 3º Para efeito desta Instrução Normativa, são adotadas as seguintes definições:

I - aplicativo: Software instalado em uma plataforma/hardware definida, fornecendo uma funcionalidade específica;

II - ciclo de vida: Todas as fases da vida do sistema, desde os requisitos iniciais até a desativação, incluindo projeto, especificação, programação, teste, instalação, operação e manutenção;

III - infraestrutura de TI: O hardware e o software, como software de rede e sistemas operacionais, que tornam possível o aplicativo funcionar;

IV - negócio: objeto a ser estudado na validação, compreende gerenciamento de dados e materiais, atividades analíticas, processo produtivo etc.;

V - proprietário do processo: A pessoa responsável pelo processo do negócio;

VI - proprietário do sistema: A pessoa responsável pela disponibilização e manutenção de um sistema computadorizado e pela segurança dos dados que residem nesse sistema;

VII - sistema computadorizado personalizado ou sob medida: Um sistema computadorizado projetado individualmente para se adequar a um processo de negócios específico;

VIII - software comercial pronto para uso: Software comercialmente disponível, cuja adequação para uso é demonstrada por um amplo conjunto de usuários;

IX - terceiro: Partes não administradas diretamente pelo titular da autorização de fabricação ou de importação.

CAPÍTULO II

DAS DISPOSIÇÕES GERAIS

Seção I

Da introdução

Art. 4º Um sistema computadorizado é um conjunto de software e componentes de hardware que, juntos, cumprem certas funcionalidades.

Art. 5º A aplicação deve ser validada.

Art. 6º A infraestrutura de tecnologia da informação deve ser qualificada.

Art. 7º Sempre que um sistema computadorizado substitui uma operação manual, não deve haver diminuição na qualidade do produto, controle de processo, garantia da qualidade ou um aumento do risco geral para o processo.

Seção II

Da gestão de riscos

Art. 8º A gestão de riscos deve ser aplicada durante todo o ciclo de vida do sistema computadorizado, levando em consideração a segurança do paciente, a integridade dos dados e a qualidade do produto.

Art. 9º As decisões sobre a extensão da validação e controle de integridade de dados devem ser baseadas e justificadas em avaliações de risco documentadas do sistema computadorizado.

Seção III

Do pessoal

Art. 10. O Proprietário do Processo, Proprietário do Sistema, Pessoas Autorizadas, TI e as demais áreas e demais pessoas relevantes devem ter qualificações adequadas, nível de acesso e responsabilidades definidas para desempenhar as suas atribuições.

Seção IV

Dos fornecedores e prestadores de serviços

Art. 11. Quando fornecedores, prestadores de serviços ou outros terceiros são usados para fornecer, instalar, configurar, integrar, validar, manter, modificar ou armazenar um sistema computadorizado ou serviço relacionado, ou para fins de processamento de dados, devem existir contratos entre o fabricante e quaisquer terceiros, em que constem declarações claras das responsabilidades do terceiro.

Parágrafo único. Os departamentos de tecnologia de informação do contratante e do contratado devem ser considerados análogos.

Art. 12. A competência e a confiabilidade de um fornecedor são consideradas elementos essenciais durante a seleção do produto ou do prestador de serviço, onde a determinação destas por meio de uma auditoria deve ter a necessidade estabelecida por uma avaliação de risco documentada.

Art. 13. A documentação fornecida com softwares comerciais prontos para uso deve ser revisada por usuários qualificados para verificar se os requerimentos do usuário são atendidos.

Art. 14. Informações sobre os sistemas de gestão da qualidade e sobre auditorias realizadas em fornecedores ou desenvolvedores de software e sistemas implantados devem ser disponibilizados aos inspetores sempre que solicitadas.

CAPÍTULO III

DAS DISPOSIÇÕES ESPECÍFICAS

Seção I

Da validação da fase de projeto

Art. 15. Os documentos e relatórios de validação devem abranger as etapas relevantes do ciclo de vida.

Art. 16. Os fabricantes devem justificar seus padrões, protocolos, critérios de aceitação, procedimentos e registros com base em sua avaliação de risco.

Art. 17. A documentação de validação deve incluir os registros dos controles de mudança e os relatórios de investigação de quaisquer desvios observados.

Art. 18. Um inventário de todos os sistemas relevantes e as funcionalidades relacionadas às Boas Práticas de Fabricação deve ser mantido pela empresa e disponibilizada sempre que solicitado.

Art. 19. Devem estar disponíveis descrições atualizadas dos sistemas críticos que detalhem os arranjos físicos e lógicos, fluxos de dados e interfaces com outros sistemas ou processos, quaisquer pré-requisitos de hardware e software e medidas de segurança.

Art. 20. As especificações dos requerimentos dos usuários devem descrever as funções requeridas ao sistema computadorizado e se basearem em uma avaliação de risco documentada e no impacto às boas práticas de fabricação.

Parágrafo único. Os requisitos do usuário devem ser rastreáveis durante todo o ciclo de vida.

Art. 21. O usuário deve tomar as medidas pertinentes para garantir que o sistema foi desenvolvido de acordo com um sistema de gestão da qualidade apropriado.

Parágrafo único. O fornecedor deve ser avaliado de forma adequada.

Art. 22. Para a validação de sistemas computadorizados personalizados, ou sob medida, deve haver um processo que garanta a avaliação formal e o registro das medidas de qualidade e de desempenho para todos os estágios do ciclo de vida do sistema.

Art. 23. Devem ser demonstradas as evidências dos métodos e cenários de testes apropriados.

§1ºAs evidências previstas no caput devem incluir os limites de parâmetros do sistema (processo), limites de dados e tratamento de erros.

§2ºFerramentas de teste automatizadas e ambientes de teste devem ter avaliações documentadas de sua adequação.

Art. 24. Caso os dados sejam transferidos para outro formato ou sistema de dados, a validação deve incluir verificações de que os dados não foram alterados em valor ou significado durante este processo de migração.

Seção II

Da fase operacional

Subseção I

Dos dados

Art. 25. A troca de dados eletrônicos de sistemas computadorizados com outros sistemas devem possuir verificações acopladas apropriadas para a alimentação e o processamento correto e seguro dos dados, a fim de minimizar os riscos.

Subseção II

Das verificações de exatidão

Art. 26. Para dados críticos inseridos manualmente, deve haver uma verificação adicional da exatidão dos dados.

§1ºEssa verificação pode ser feita por um segundo operador ou por um meio eletrônico validado.

§2ºA criticidade e as consequências potenciais de dados errados ou incorretamente inseridos em um sistema devem ser cobertas pela avaliação de risco.

Subseção III

Do armazenamento dos dados

Art. 27. Os dados devem ser protegidos por meios físicos e eletrônicos contra danos.

Art. 28. Os dados armazenados devem ser verificados quanto à acessibilidade, legibilidade e exatidão.

Art. 29. O acesso aos dados armazenados deve ser garantido durante todo o período de armazenamento.

Art. 30. Devem ser feitos backups de todos os dados relevantes.

Parágrafo único. A integridade e a exatidão dos dados de backup e a capacidade de restaurar os dados devem ser verificadas durante a validação e monitoradas periodicamente.

Subseção IV

Das impressões

Art. 31. Os dados armazenados eletronicamente devem possibilitar a geração de cópias impressas claras.

Art. 32. Para os registros que dão suporte à liberação dos lotes, deve ser possível gerar impressões indicando se algum dos dados foi alterado desde a sua inserção original.

Subseção V

Das trilhas de auditoria

Art. 33. Baseada em análise de risco, deve ser considerada a construção de um sistema de trilha de auditoria de todas as deleções ou alterações relevantes às Boas Práticas.

§1ºPara alteração ou exclusão de dados relevantes para as Boas Práticas de Fabricação, a razão deve ser documentada.

§2ºAs trilhas de auditoria devem estar disponíveis e devem ser passíveis de serem apresentadas em um formato compreensível quando disponibilizadas.

§3ºAs trilhas de auditoria devem ser revisadas regularmente.

Subseção VI

Do gerenciamento de mudanças e do gerenciamento de configurações

Art. 34. Quaisquer alterações em um sistema computadorizado, incluindo configurações do sistema, devem ser feitas de maneira controlada, de acordo com um procedimento definido.

Subseção VII

Da avaliação periódica

Art. 35. Sistemas computadorizados devem ser periodicamente avaliados para confirmação de que permanecem validados e em conformidade com as Boas Práticas de Fabricação.

Parágrafo único. Essas avaliações devem incluir, quando apropriado, o conjunto atual de funcionalidades, registros de desvio, incidentes, problemas, histórico de atualização, desempenho, confiabilidade, segurança e relatórios de situação de validação.

Subseção VIII

Da segurança

Art. 36. Devem existir controles físicos ou lógicos que assegurem que o acesso ao sistema computadorizado é permitido apenas às pessoas autorizadas.

Parágrafo único. Os métodos adequados para impedir o acesso não autorizado ao sistema podem incluir o uso de chaves, cartões de acesso, códigos pessoais com senhas, dados biométricos, acesso restrito a equipamentos de informática e áreas de armazenamento de dados.

Art. 37. A extensão dos controles de segurança deve ser determinada de acordo com uma avaliação da criticidade do sistema computadorizado.

Art. 38. A criação, alteração e cancelamento de autorizações de acesso devem ser registradas.

Art. 39. Sistemas de gestão de dados e de documentos devem ser projetados para registrar a identidade dos usuários que inserem, alteram, confirmam ou excluem dados, incluindo data e hora.

Subseção IX

Da gestão de incidentes

Art. 40. Todos os incidentes, não apenas falhas de sistema e erros de dados, devem ser registrados e avaliados.

Parágrafo único. A causa raiz dos incidentes críticos deve ser identificada e integrar a base das ações corretivas e preventivas adotadas.

Subseção X

Da assinatura eletrônica

Art. 41. Registros eletrônicos podem ser assinados eletronicamente.

Art. 42. As assinaturas eletrônicas devem:

I - ter o mesmo impacto que as assinaturas manuscritas dentro dos limites da empresa;

II - ligar-se permanentemente ao seu respectivo registro;

III - incluir a hora e a data em que foram aplicadas;

IV - para os registros utilizados externamente, a assinatura eletrônica deve atender as diretrizes de certificação digital aplicáveis localmente.

Subseção XI

Da liberação de lotes

Art. 43. Quando um sistema computadorizado for usado para liberação de lotes, deve ser assegurado que apenas Pessoa Delegada pelo Sistema de Qualidade Farmacêutica tenha permissão a essa funcionalidade.

§1ºUm registro especificando a pessoa responsável pela liberação deve estar disponível.

§2ºA identificação e o registro da pessoa responsável devem ser realizados por meio de assinatura eletrônica.

Subseção XII

Da continuidade do negócio

Art. 44. Devem existir medidas que garantam a continuidade dos processos críticos em caso de falhas dos sistemas computadorizados que lhes dão suporte, tais como sistemas alternativos ou registros manuais.

§1ºO tempo necessário para se pôr em prática as medidas alternativas deve ser baseado no risco, bem como ser adequado a um determinado sistema e ao processo comercial apoiado.

§2ºEssas medidas alternativas devem ser adequadamente documentadas e testadas.

Subseção XIII

Do arquivamento

Art. 45. Os dados podem ser arquivados desde que permaneçam acessíveis, legíveis e íntegros.

Parágrafo único. Se forem necessárias alterações relevantes no sistema, a capacidade de recuperar os dados deve ser assegurada e testada.

CAPÍTULO IV

DAS DISPOSIÇÕES FINAIS

Art. 46. O descumprimento das disposições contidas nesta Instrução Normativa constitui infração sanitária, nos termos da Lei nº. 6.437, de 20 de agosto de 1977, sem prejuízo das responsabilidades civil, administrativa e penal cabíveis.

Art. 47. Esta Instrução Normativa entra em vigor 45 (quarenta e cinco) dias após sua publicação.

WILLIAM DIB
Diretor-Presidente