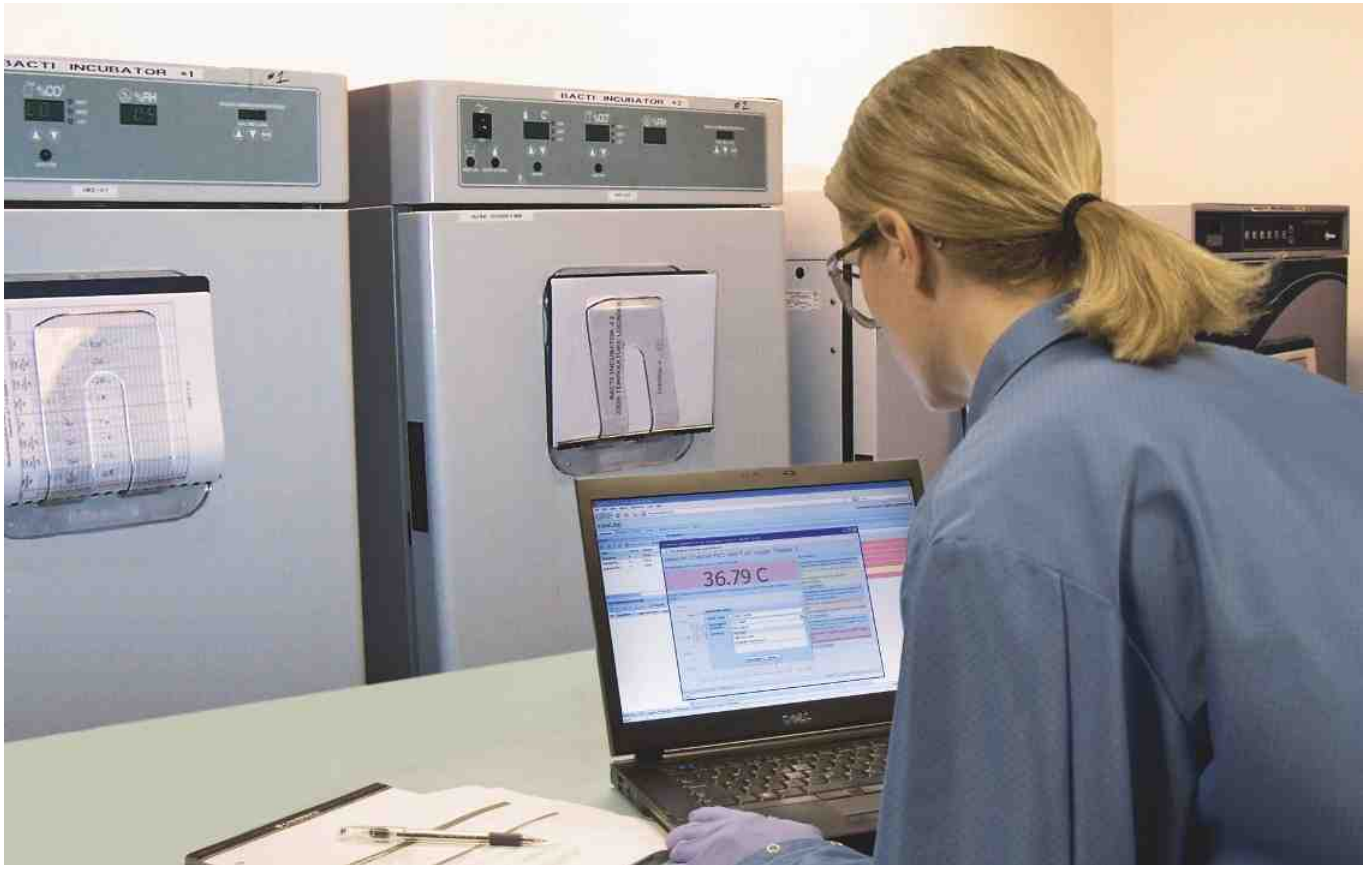
VAISALA / WHITE PAPER

Como o Sistema de Monitoramento Contínuo da Vaisala Ajuda na Conformidade com o CFR Parte 11 do Título 21 e Anexo 11 do EU GMP



Introdução

As duas principais diretrizes regulamentares que descrevem o uso adequado de sistemas informatizados para realização de atividades relacionadas com as GMP são a CFR, Parte 11 do Título 21 da FDA e a EU GMP "Anexo 11: Sistemas Informatizados" publicado pela Comissão Europeia como parte da EudraLex. Este white paper analisa os requisitos da Parte 11 e o Anexo 11, aplicáveis à validação e monitoramento ambiental, e descreve como o softwares viewLinc do sistema de monitoramento contínuo Vaisala ajuda as empresas a cumprir tais exigências.

Escopo e Princípios

O alcance geográfico do CFR 21, Parte 11 e Anexo 11 conforme se segue: A Parte 11 aplica-se aos fabricantes que buscam a aprovação da FDA para comercialização de produtos farmacêuticos, biológicos, nutracêuticos e dispositivos médicos nos Estados Unidos. O Anexo 11, entretanto, aplica-se a processos de fabricação que visam distribuir os mesmos produtos na União Europeia. Tanto a Parte 11 como o Anexo 11 descrevem amplos controles técnicos e procedimentos que podem ser usados na criação e armazenando de dados eletrônicos utilizados em registros necessários às GMPs. O Anexo 11 é um dos dezenove requisitos complementares da guia de GMP da UE. As revisões do Anexo 11 de 2011 alinham as GMPs da UE com as diretrizes de qualidade Q8-10 (publicadas pela Conferência Internacional para a Harmonização de Requisitos Técnicos de Registo dos Medicamentos para Uso Humano). Essas alterações se refletem no presente white paper.

A Parte 11 aplica-se à criação, modificação, arquivamento, recuperação e transmissão de quaisquer registros eletrônicos exigidos por regras estabelecidas da FDA. O Anexo 11 é um pouco mais amplo e aborda os princípios e o uso adequado de sistemas computacionais aplicados na execução de tarefas necessárias às GMPs. O CFR 21, Parte 11 declara que a opinião da FDA é de que os riscos de falsificação, má interpretação e alteração (sem deixar provas) no âmbito das GMPs, são maiores com registros eletrônicos do que os registros em papel e, portanto, requerem controles específicos. Por comparação, o Anexo 11 alude mais à automação de processos com sistemas informatizados. Tanto a Parte 11 quanto o Anexo 11 visam reduzir os riscos à qualidade de produtos que poderiam resultar da automação em ambientes de fabricação.

De acordo com o CFR 21, Parte 11, Subparte A, Seção 11.1 – Escopo:

> (a) Os regulamentos nesta parte estabelecem os critérios sob os quais a Agência considera registros eletrônicos, assinaturas electrónicas e assinaturas manuscritas executadas por registros eletrônicos confiáveis, e geralmente equivalentes a registros em papel e assinaturas manuscritas executadas em papel.[1]

O escopo da Parte 11 abrange qualquer registro eletrônico criado em conformidade com os regulamentos da FDA. A Parte 11 também se aplica aos registros eletrônicos submetidos à Agência em conformidade com as leis Federais de Alimentos, Medicamentos e Cosméticos e de Serviços de Saúde Pública. Aplicável neste escopo são "… tais registros [que] não são especificamente identificados nos regulamentos das agências. No entanto, esta parte não se aplica aos registros em papel que são ou foram transmitidos por via eletrônica."2 Isto significa que, embora os documentos devam cumprir com a Parte 11, eles não precisam serem especificamente mencionados em qualquer orientação ou regulamento GMP. Se o registro existir primeiro no formato de papel impresso, não é considerado um "documento eletrônico." A transmissão eletrônica da versão em papel, por e-mail em cópia escaneada ou um PDF não substitui o registro em papel, nem o torna "eletrônico."[3]

Uma diferença fundamental entre o CFR 21 Parte 11 e o Anexo 11 é que a Parte 11, em sua maioria, diz respeito aos registros eletrônicos e assinaturas eletrônicas (ERES); e o Anexo 11 não aborda as assinaturas eletrônicas em detalhe.

Em vez disso, o Anexo 11 trata dos sistemas informatizados, incluindo componentes de hardware e software que contribuem para realização de atividades em ambientes GMP. Esses aplicativos devem ser validados mediante processos de qualificação. Além disso, o Anexo 11 estipula que sistemas informatizados que substituem operações manuais não deverão resultar na diminuição da qualidade do produto, controle de processo ou garantia de qualidade. Nem o um aumento de risco em um processo onde os sistemas informatizados são utilizados.[4]

O software viewLinc do sistema de monitoramento contínuo da Vaisala é um "sistema híbrido", pois utiliza registros eletrônicos com a expectativa de que ao solicitar-se uma assinatura, o registro será impresso e assinado. Os registros impressos a partir do viewLinc são gerados em PDF, para que possam ser importados a um sistema que visa implementar assinaturas eletrônicas. Visto que o viewLinc não utiliza assinaturas eletrônicas, discutiremos a questão ainda no presente artigo.

Os dados ambientais coletados pelo viewLinc são armazenados como registros eletrônicos que podem ser usados como evidência de que os produtos regulamentados foram armazenados respeitando os devidos intervalos de vários parâmetros ambientais (e.g. temperatura, umidade, CO_2, pressão diferencial, etc.).

Note-se que, embora, o software viewLinc ajude os usuários a cumprir os requisitos do CFR 21 Parte 11 e do Anexo 11, a responsabilidade final pelo cumprimento é dos responsáveis pelo conteúdo dos registros eletrônicos, bem como os responsáveis pelo uso dos sistemas informatizados. Da mesma forma, a responsabilidade pelo cumprimento das exigências de registros em papel é do responsável pelo conteúdo dos registros.

Inspeções Regulatórias

Tanto a Parte 11 quanto o Anexo 11 estipulam que os sistemas e componentes usados para gerar registros eletrônicos devem ser disponibilizados para inspeção regulamentar. De acordo com a Parte 11, "os sistemas computacionais (incluindo hardware e software), controles e documentação relacionada mantida conforme a referida Parte devem estar prontamente disponíveis e sujeitas à inspeção da FDA." Da Mesma Forma, no Anexo 11: "O sistema de qualidade e informações de auditorias relativas a fornecedores ou desenvolvedores de software e sistemas implementados devem ser disponibilizado aos inspetores mediante solicitação."[5]

No aplicativo, significa que os registros eletrônicos gerados pelo viewLinc devem ser copiados e mantidos, como qualquer sistema automatizado. Para garantir que nenhum dado histórico seja perdido quando os usuários do sistema atualizarem o viewLinc, a Vaisala mantém compatibilidade com as versões anteriores do software. No entanto, sugerimos que, como prática recomendada, as empresas arquivem uma cópia da versão usada para criar os registros eletrônicos como referência de backup.

Controles de Sistema & Segurança I

Anexo 11

Nos termos do Anexo 11, existem três seções que dão ênfase aos controles de sistema e segurança. Essencialmente, a integridade de dados é parte da gestão de riscos e, como tal, os controles destinados a garantir a correção dos dados devem ser implementados. Os controles incluem: verificações de dados internos (dentro do software e/ou com procedimento manual) e acesso autorizado pelo usuário apenas para pessoal designado. Na terminologia do Anexo 11, o software viewLinc CMS da Vaisala constitui um aplicativo instalado na plataforma de um proprietário de sistema, tornando a Vaisala um "terceiro fornecedor de software disponível comercialmente."

Ao abordar as características de segurança e procedimentos que tornam um software comercialmente disponível, compatível com os requisitos do Anexo 11, a EMA assume uma abordagem com base em riscos e espera que as empresas averiguem tanto a integridade dos dados quanto a segurança do sistema

em termos de riscos associados a processos executados por sistemas informatizados. As seções a seguir do Anexo 11 ilustram o equilíbrio que deve ser encontrado entre o esforço dedicado para garantir que controles de sistema sejam implementados e o nível de risco que um determinado sistema destina-se a atenuar.

> "Os sistemas informatizados que compartilham dados eletronicamente com outros sistemas devem incluir verificações internas adequadas para a correta e segura entrada e processamento de dados, a fim de minimizar os riscos…
>
> "Os controlos físicos e/ou lógicos devem ser implementados para restringir o acesso ao sistema informatizado a pessoas autorizadas…
>
> "A extensão dos controles de segurança depende da criticidade do sistema informatizado."[6]

No Anexo 11, a segurança do sistema, os dados e o controle de acesso de operadores é abordada nas seguintes passagens:

> "Os dados só devem ser inseridos ou alterados por pessoas autorizadas. Deve-se dispor de um procedimento definido para a emissão, cancelamento e alteração de autorização para acessar e alterar os dados, incluindo a mudança de senhas pessoais.
>
> "Quando os dados críticos forem inseridos manualmente ... deverá ser feita uma verificação adicional quanto à precisão do registro efetuado.
>
> "O sistema deve registrar a identidade dos operadores que acessam ou confirmam os dados críticos...
>
> "Qualquer alteração a uma entrada de dados críticos deve ser autorizada e registrada e incluindo a razão da mudança. Deve-se levar em conta o desenvolvimento de um registro completo no sistema de todas as entradas e alterações (uma "trilha de auditoria")."[7]

Alinhado a estas orientações, o viewLinc software do CMS gera arquivos em formato proprietário usando a técnica checksum, que detecta registros inválidos ou alterados. Além disso, o software utiliza várias camadas de controle de acesso, incluindo a autenticação interna do sistema operacional Windows. Todos os dados gravados por dispositivos que se conectam ao viewLinc são capturados no arquivo do registrador de dados. Os usuários

com nível de acesso de administrador de sistema nunca podem desativar ou modificar o conteúdo, nem a forma como os dados são gravados no registro eletrônico. Assim que os dados são gravados pelo dispositivo (e durante a gravação), os arquivos não podem ser editados ou apagados. Além disso, todas as alterações feitas nos parâmetros de funcionamento do registrador de dados no meio de uma sessão de gravação resulta na criação um registro eletrônico completamente novo.

Controles de Sistema & Segurança II

CFR 21 Parte 11

Em relação ao CFR 21 Parte 11, a segurança de dados é parcialmente abordada nas seções que descrevem o que o FDA denomina de "sistemas fechados" e "sistemas abertos."
O termo "sistema fechado" tem diferentes significados conforme o contexto. Para efeitos da Parte 11, um sistema fechado é "um ambiente no qual o acesso ao sistema é controlado por pessoas responsáveis pelo conteúdo dos registros eletrônicos no sistema." O software viewLinc é um

"sistema fechado", pois os arquivos de dados não podem ser modificados sob quaisquer circunstâncias, e somente pessoas autorizadas podem obter acesso ao sistema. Todos os arquivos criados pelo viewLinc são seguros, e qualquer tentativa de alterá-los seria registrada pela trilha de auditoria do sistema, que capta todas as interações com o sistema, incluindo a limpeza da memória em um dispositivo de gravação.

De acordo com a Parte 11, a Subparte B "Seção 11.10 Controles para sistemas fechados" procedimentos e controles devem ser implementados de forma a garantir a "autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos." Os registros precisam ser protegidos de retração ou falsificação. Os controles podem incluir:

- Validação de sistema para indicar a função esperada
- A capacidade de gerar cópias completas
- Proteção de registro para fins de recuperação
- Acesso limitado aos registros
- Trilhas de auditoria com registro de data e hora inalteráveis e disponíveis para análise
- Gravação sequencial linear, inalterável e completa
- Pessoal autorizado verifica o acesso e assinaturas
- Dispositivos infalsificáveis para garantir a validade dos dados
- capacitação adequada do pessoal envolvido em tarefas relacionadas à Parte 11
- Políticas escritas que incluem os responsáveis que usam assinaturas eletrônicas.

Além destes exemplos de controles para sistemas fechados, deve haver um controlo sobre a documentação do sistema que inclui a distribuição de registros, o uso de documentação operacional do sistema e procedimentos de controle de mudança.

Dentro do viewLinc, as cópias dos dados registrados pelos dispositivos equipados com sensor são disponibilizadas ao copiar os arquivos de dados brutos ou pela criação de um “impressão PDF” para exportar gráficos em PDF (é necessário o Adobe Acrobat ou uma impressora de formato de documento portátil similar). Dado que o viewLinc é um sistema híbrido, os registros eletrônicos gerados por ele devem ser impressos e assinados. Os registros são eletrônicos, mas a assinatura é manual (daí o termo "híbrido"). Os registros são protegidos para recuperação com as funções do viewLinc de relatórios e exportação, e o software não permite a modificação de registros em qualquer circunstância, por qualquer pessoa, autorizada ou não, incluindo sequência das etapas por um usuário. O acesso aos registros é limitado pela controle de acesso do software, que como já foi afirmado, usa o método de autenticação interna do sistema operacional Windows.

Trilhas de Auditoria

Em resposta aos requisitos da Parte 11 para gravação sequencial, o viewLinc cria uma trilha de auditoria que inclui todos os dados registrados nos dispositivos CMS. O sistema aplica uma função de soma de verificação para todos os arquivos gerados pelo sistema para garantir a integridade dos dados. Além disso, qual alteração feita nos parâmetros de funcionamento do registrador em atividade resulta na criação de um registro eletrônico completamente novo.

Cada dispositivo CMS (e.g: registrador de dados, transmissor) contém dados eletrônicos em memória EEPROM não volátil. Assim que os dados forem transferidos do dispositivo para o software, a mídia em que está armazenado, a estratégia de backup e os procedimentos de recuperação são de responsabilidade dos usuários do sistema.

O CMS Vaisala é um sistema comercial pronto baseado na criação de arquivos de banco de dados seguros, que não podem ser modificados sem tornar o banco de dados completamente inutilizável. Seus dispositivos também são fisicamente invioláveis. O software segue um protocolo propietário de comunicação com os dispositivos, e identifica de forma positiva cada dispositivo, determinando a integridade dos dados como parte de seu processo. Além disso, os arquivos históricos são criptografados.

Validação

Parte 11:

As orientações relativas à validação constam do CFR 21 Parte 11 e do Anexo 11, (“Seção 11.10 Controles para sistemas fechados", e "Fase e Validação de Projetos", respectivamente). Como qualquer procedimento de validação, a intenção é mostrar que o sistema funcione conforme o previsto. A FDA considera a validação de um controle de procedimento para garantir que o sistema fechado possa gerar registros precisos, com confidencialidade quando exigido pelas GMPs.

> “As pessoas que utilizam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles que visem garantir autenticidade, integridade e, quando necessário, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não rejeite imediatamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte:
>
> (a) Validação de sistemas para assegurar a exatidão, confiabilidade, desempenho consistente e pretendido e a capacidade de discernir os registros inválidos ou alterados.”[8]

No seu documento intitulado: “Parte 11, Registros Eletrônicos; Assinaturas Eletrônicas – Escopo e Aplicação”9 a FDA define sua estratégia de cumprimento sobre validação nos termos da Parte 11, e sugere que os requisitos estabelecidos orientem as decisões das empresas sobre o grau de seus esforços de validação.10 Basicamente, o efeito que um sistema tem sobre a capacidade da empresa de cumprir os requisitos das GMPs deve corresponder com a validação desse sistema. Como todos os dados pertinentes aos requisitos estabelecidos, a "precisão, confiabilidade, integridade, disponibilidade e autenticidade" dos registros devem ser verificadas de acordo não só com a regra, mas também às exigências e parâmetros de sua aplicação. Recomendamos um documento de avaliação de risco que pode servir como justificativa para o âmbito e a profundidade dos procedimentos de validação.

Anexo 11

As orientações constantes do Anexo 11 referem-se mais especificamente à validação em sua seção "Fase e Validação de Projetos.”[11] Esta descreve as expectativas de validação, incluindo o ciclo de vida dos documentos de validação, alterar registros de controle, relatórios de desvio, estoques de sistemas relacionados com as GMPs, Especificação de Requisitos de Usuários (URS), avaliação de riscos, sistemas de gestão da qualidade, avaliação de fornecedores, ambientes de teste e integridade de dados através de processos de migração. O escopo das orientações de validação do Anexo 11 excede a da Parte 11 em sua inclusão da infraestrutura de TI como elemento que requer qualificação.[12] A validação deve ainda obedecer às normas de Qualificação de Operação, devendo ser executadas no ambiente em que o sistema será usado. Isto significa que os provedores de sistema não podem oferecer sistemas previamente validados, mas podem realizar a instalação e qualificações de operação após a instalação do sistema.

Validação do Sistema de Monitoramento Contínuo da Vaisala

Apesar da validação, juntamente com todos os outros procedimentos do sistema operacional, é responsabilidade da empresa, a Vaisala oferece protocolos de validação, incluindo Instalação (QI) e Qualificação de Operação (OQ). Os referidos documentos contêm protocolos detalhados para a avaliação das funções do software viewLinc, e incluem colunas aos que executam protocolos a fim de indicar êxito ou fracasso e, assim, observar todos os desvios constatados.

Um técnico de validação da Vaisala pode realizar a execução da IQ/OQ no CMS da Vaisala. Podemos também realizar um estudo de mapeamento do ambiente em regiões selecionadas. Para obter mais informações, consulte:

Need to replace it with the Portuguese site weblink

Equipe

Parte 11:

O CFR 21 Parte 11 contém menos orientação do que o Anexo 11 sobre quem está apto para usar sistemas relacionados à GMP. Na Parte 11, as pessoas autorizadas são definidas pelo contexto; ou seja, o sistema que elas usam em vez de sua função na empresa. Em “Definições” o acesso de pessoal a um sistema, além de sua responsabilidade pelo conteúdo dos registros eletrônicos do sistema, define um Sistema Fechado. Na mesma seção "Sistemas abertos" são descritos como aqueles que não têm necessariamente controle de acesso pelo pessoal responsável pelo conteúdo dos registros eletrônicos.[13] No entanto, tanto os sistemas Abertos como os Fechados devem dispor de procedimentos que garantam "autenticidade, integridade e, conforme o caso, a confidencialidade dos registros eletrônicos.”

De acordo com os "Controles de Sistema Fechados", obtemos orientações para garantir que o pessoal tenha a habilidade necessária e acesso para realizar tarefas relacionadas com a GxP com sistema, afirmando que "os procedimentos e controles incluirão os seguintes:

(i) Determinar que as pessoas que desenvolvem, mantêm ou utilizam sistemas de registro eletrônico/assinatura eletrônica tenham a educação, capacitação e experiência para desempenhar suas tarefas atribuídas.

(j) Definir e observar as políticas escritas que atribuem a responsabilidade aos indivíduos que iniciarem ações por meio de suas assinaturas eletrônicas, a fim de impedir a falsificação de registros e assinaturas.”[14]

Anexo 11

O Anexo 11 apresenta exemplos de funcionários responsáveis: “Proprietário do Processo, Proprietário do Sistema, Pessoas Qualificadas e IT”15 Semelhante à Parte 11, o Anexo 11 também exige capacitação adequada e controles de acesso mediados por administradores de sistema.

Capacitação & Controle de Acesso do CMS da Vaisala

O software viewLinc contém dez níveis de direitos que determinam quais dados uma pessoa qualificada pode conferir e quais funções do software podem usar. O administrador do sistema também define controles de acesso ao nível dos locais monitorados. A Vaisala oferece treinamento remoto e no local aos usuários do sistema e administradores para ajudar na implantação adequada do sistema e utilização.

Conclusão

A Parte 11 e o Anexo 11 foram introduzidos para tratar das principais diferenças entre os sistemas informatizados e manuais e criar registros eletrônicos equivalentes a registros em papel, como comprovação da boa execução de tarefas relacionadas com GMP. Hoje, os sistemas de monitoramento ambiental mais usados em empresas compatíveis com o GxP são inerentemente consistentes com os requisitos dos "Onzes.” No entanto, o risco de não conformidade com as orientações regulamentares não decorrem dos próprios sistemas, mas em como são implementados, usados e mantidos.

Tanto a Parte 11 quanto o Anexo 11 fornecem ampla orientação sobre abordagens da gestão baseada em riscos de registros criados com sistemas computadorizados. Em resposta a estes requisitos, o softwares viewLinc de CMS da Vaisala permite que as empresas estejam em conformidade com amplos protocolos de validação, várias camadas de segurança, recursos de trilha de auditoria contra falhas (fail-safe) e um sistema projetado para ambientes regulamentados.

Referências

1: Cf. CFR 21, Parte 11, “Disposições Gerais, Sec. 11.1 Escopo”, http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?fr=11.1

2 Ibid.

3. Ibid. Cf.: (b) no Âmbito de Aplicação: “No entanto, esta parte não se aplica aos registros em papel que são, ou foram, transmitidos por via eletrônica.”

4. Cf. Anexo 11 “Princípio”: http://ec.europa.eu/health/files/eudralex/vol-4/annex11_01-2011_en.pdf

5. Ibid. Cf. Fornecedores e Prestadores de Serviços (3.4)

6. Ibid. Cf. Dados (5), Segurança (12.1), e (12.2)

7. Cf. Anexo 11, Eudralex Volume 4, da Comissão Europeia DGIII-E-3 (1998) http://ec.europa.eu/health/files/eudralex/vol-4/pdfs-en/anx11_en.pdf

8. Cf. CFR 21, Parte 11, Subparte B – Registros Eletrônicos, sec. 11.10 Controles para sistemas fechados http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfCFR/CFRSearch.cfm?CFRPart=11&showFR=1

9. “Parte 11, Registros Eletrônicos; Assinaturas Eletrônicas – Escopo e Aplicação” http://www.fda.gov/regulatoryinformation/guidances/ucm125067.htm

10. A Agência fornece mais orientação sobre validação nas seções 4.8 e 4.10 do presente documento: “Princípios Gerais de Validação de Software; Orientação final para a Indústrias e Funcionários da FDA” http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm085281.htm

11. Cf. Anexo 11, "Fase de Projeto, 4. Validação” http://ec.europa.eu/health/files/eudralex/vol-4/annex11_01-2011_en.pdf

12. Ibid. "Princípio"

13. CFR 21, Parte 11 “Sec. 11.3 Definições” http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfCFR/CFRSearch.cfm?CFRPart=11&showFR=1

14. Ibid. “Sec. 11.10 Controles para Sistemas Fechados”

15. Cf. Anexo 11, "General, 2. Equipe” http://ec.europa.eu/health/files/eudralex/vol-4/annex11_01-2011_en.pdf

VAISALA

www.vaisala.com

Favor contatar-nos no
br.vaisala.com/pedirinfo

Escanear o código para informações adicionais

CE