FRESENIUS KABI

Separador AMICUS

Suplemento de segurança cibernética

SW v. 6.0 e 6.1

REF 4R4580
4R4580R
4R4580TH
6R4580
6R4590
6R4590TH-M
6R4590TH-T

Rx Only MD

471916330 (PTBR) [A] 2023/01

Sumário

Esta página foi deixada em branco intencionalmente.

Registro do status da revisão

Número de controle do documento	Data da revisão	Número da versão do software	Revisado	Assinatura e data

Esta página foi deixada em branco intencionalmente.

Seção 1.0 Introdução

Este suplemento oferece uma visão geral das informações sobre segurança cibernética do sistema Separador AMICUS. O objetivo deste documento é detalhar como as práticas de segurança e privacidade da Fresenius Kabi foram aplicadas ao sistema Separador AMICUS, o que o usuário deve saber sobre a manutenção da segurança deste produto e como a parceria da Fresenius Kabi com o usuário pode garantir a segurança em todo o ciclo de vida do produto.

Este suplemento deve ser usado em conjunto com o Manual do Operador do Separador AMICUS e o Suplemento de gerenciamento de dados.

Seção 2.0 Responsabilidade conjunta

A segurança cibernética de dispositivos médicos é uma responsabilidade compartilhada, e isso inclui a Fresenius Kabi, o pessoal do usuário responsável pela instalação e implantação e os usuários do dispositivo. É responsabilidade do pessoal do usuário responsável pela instalação e implantação do sistema Separador AMICUS avaliar o nível razoável de segurança para o ambiente operacional, integrar o sistema ao ambiente operacional, fornecer a documentação e o treinamento necessários aos operadores e oferecer apoio para o tratamento de incidentes de segurança. É responsabilidade dos usuários do sistema Separador AMICUS seguir as instruções de uso quando utilizarem o sistema Separador AMICUS, garantir que o nível de segurança exigido seja mantido (incluindo a prevenção de acesso físico ao dispositivo a usuários não autorizados) e garantir que a manutenção e as atualizações de software sejam realizadas de acordo com as recomendações da Fresenius Kabi.

A proteção abrangente do sistema Separador AMICUS contra ameaças à segurança cibernética depende não apenas das proteções integradas ao sistema Separador AMICUS, mas também da proteção e segurança da rede do usuário e do ambiente de instalação. Se um ambiente de implantação seguro e protegido não puder ser fornecido, o usuário deverá informar seu representante de conta da Fresenius Kabi para desativar os recursos de conectividade do sistema Separador AMICUS até que os requisitos contidos neste suplemento possam ser atendidos. As medidas de proteção instaladas no próprio dispositivo (conforme detalhado neste suplemento) representam proteções administrativas, técnicas e físicas razoáveis para proteger o Sistema Separador AMICUS contra os eventos mais prováveis de invasão e uso indevido.

À medida que os sistemas e ameaças evoluem, nenhum sistema pode ser protegido contra todas as vulnerabilidades e a Fresenius Kabi considera seus clientes os parceiros mais importantes na manutenção das proteções de segurança e privacidade. Caso tenha alguma dúvida, a Fresenius Kabi pede que todas as questões sejam trazidas ao seu conhecimento para que a empresa possa investigá-las. Quando apropriado, a Fresenius Kabi resolverá os problemas com alterações de produto, boletins técnicos e/ou divulgações responsáveis para clientes e autoridades. A Fresenius Kabi se esforça continuamente para melhorar a segurança e a privacidade em todo o ciclo de vida do produto.

Se um usuário quiser relatar um problema de privacidade ou segurança em potencial relacionado ao produto (incidente, violação ou vulnerabilidade), entre em contato com a Fresenius Kabi:

Endereço: Else-Kröner-Str. 1
61352 Bad Homburg
Germany

Telefone internacional.: +49 (0) 61 72 / 686-0

Telefone para os EUA: 1-800-933-6925

Site: www.fresenius-kabi.com

Seção 3.0 Descrição do produto

O sistema Separador AMICUS mostrado na Figura 1 é um separador de células sanguíneas automatizado, destinado para uso na coleta de componentes sanguíneos e células mononucleadas.

O sistema Separador AMICUS é um separador de células sanguíneas automatizado, destinado ao uso em aplicações terapêuticas de aférese e pode ser utilizado para realizar a troca terapêutica de plasma (TPT).

O sistema Separador AMICUS é um separador de componentes sanguíneos automatizado, destinado para uso em aplicações terapêuticas de aférese e pode ser usado para realizar procedimentos de troca de hemácias, depleção e depleção/troca (RBCX).

O sistema Separador AMICUS é um separador de componente sanguíneo automatizado, destinado para uso em aplicações terapêuticas de aférese e pode ser usado para a administração de Fotoferese Extracorpórea (ECP). O separador pode ser configurado por um representante de atendimento qualificado para realizar procedimentos de ECP, se autorizado pelas agências locais de regulamentação apropriadas. O uso de procedimentos de ECP não é autorizado nos EUA.

Figura 1: Sistema Separador AMICUS

Funcionários de hemocentros ou de hospitais treinados para operar o dispositivo AMICUS são os principais usuários do sistema. O grupo de usuários de suporte inclui engenheiros de serviço de campo (FSEs) e administradores de TI, que são profissionais treinados nas áreas de engenharia ou tecnologia da informação.

O Separador AMICUS fornece interfaces de rede sem fio e com fio que são usadas para se comunicar com um sistema de gerenciamento de dados. Um sistema de gerenciamento de dados é um software que faz interface com o Separador AMICUS e permite a geração de relatórios de aumento de produtividade, upload de parâmetros do doador/paciente e troca de informações do doador/paciente e do procedimento. O Separador AMICUS pode exportar dados do procedimento e do doador/paciente que foram inseridos ou gerados durante o procedimento. Os dados exportados do Separador AMICUS podem ser:

- Usado para relatórios de qualidade
- Enviados para BECS (Blood Establishment Computer Software, Softwares para banco de sangue) ou um sistema de registro médico eletrônico

- Usado na criação de registros do procedimento
- Usado para eficiências operacionais

Esses dados poderão ser usados como um registro eletrônico, no lugar de determinada documentação manual, e poderão ser usados para a tomada de decisões-médicas. Como alternativa, os dados poderão ser usados como dados focados operacionalmente para auxiliar nas atividades de negócios, como melhorar o desempenho ou a eficiência operacional. O Separador AMICUS também pode ser configurado para suportar a configuração de procedimento remoto onde as informações do doador/paciente são enviadas e exibidas no Separador AMICUS específico.

Modelos 4R4580 e 6R4580 e seus acessórios

Para os modelos 4R4580 e 6R4580 mostrados na Figura 2, a funcionalidade oferecida exige que o sistema inclua as seguintes interfaces:

- Interface de rede sem fio/com fio usando o acessório adaptador de rede Lantronix
- Interface do usuário com tela de toque
- Interface de comunicação de porta serial
- Interface de porta serial para diagnóstico
- Interface de porta serial para leitor de código de barras

As interfaces fornecidas permitem que o Separador AMICUS tenha conectividade com os seguintes acessórios opcionais:

- Servidor de Aplicação de Gerenciamento de Dados DXT, que faz interface com o Sistema de Gerenciamento de Doadores via interface de rede
- Dispositivo de fotoativação Phelix via interface de comunicação de porta serial

Observação: O Phelix é usado em conjunto com o AMICUS para realizar Fotoferese Extracorpórea (ECP) nas localidades onde é aprovado. O Phelix e a fotoferese extracorpórea não são aprovados para uso nos Estados Unidos.

- Terminal de diagnóstico via interface de porta serial
- Leitor de código de barras via interface de porta serial para leitor de código de barras

A interface do usuário da tela de toque implementa interface humano-máquina em todas as interações com usuários do Separador AMICUS.

Além disso, o uso do dispositivo AMICUS no ambiente de uso pretendido não requer operação 24 horas por dia, 7 dias por semana, portanto, o dispositivo é ligado e desligado diariamente.

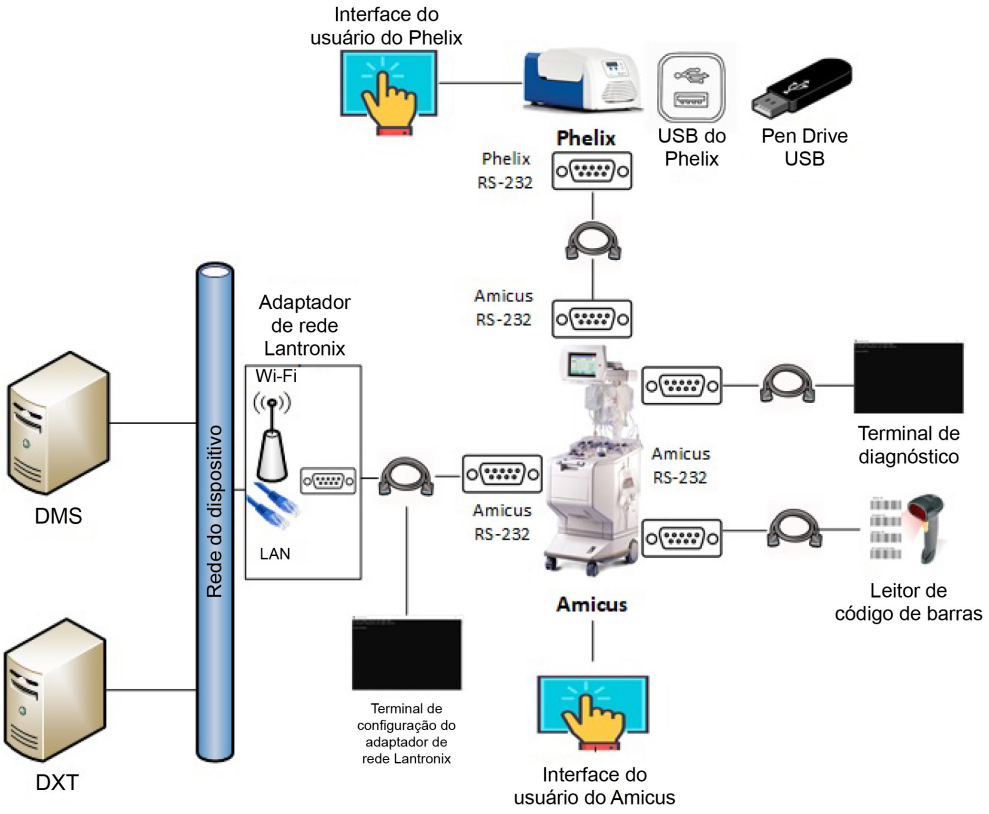

Figura 2: Modelos 4R4580 e 6R4580 e seus acessórios

Ao isolar os recursos computacionais e os processos de doação dos processos de comunicação, as funcionalidades críticas do processamento seguro do sangue foram separadas. Um ataque de segurança cibernética aos recursos de rede do Separador AMICUS não afetaria a integridade ou disponibilidade do procedimento. A separação razoável, lógica e física dos processos de interface do usuário (UI) (por exemplo, o sistema de tela de toque) dos recursos de rede também foram implementados.

Além disso, as funções que usam interfaces externas (por exemplo, RS-232) são projetadas para exigir a confirmação da ação do operador na interface do usuário do sistema de aférese AMICUS. Por fim, as interfaces de rede podem ser totalmente desabilitadas para isolar o dispositivo de qualquer conectividade remota, sem qualquer impacto sobre as funções críticas de processamento de sangue. Embora a proteção completa contra todas as ameaças à segurança cibernética não seja possível sem a implementação adequada pelo cliente de uma rede e ambiente seguros e protegidos, essas medidas de isolamento oferecem proteção razoável contra as intrusões e usos indevidos mais prováveis.

Modelos 6R4590 e seus acessórios

Para os modelos 6R4590 mostrados na Figura 3, a funcionalidade oferecida exige que o sistema inclua as seguintes interfaces:

- Interfaces de rede com e sem fio
- Interface do usuário (UI) com tela de toque
- Interface de comunicação de porta serial
- Interface de porta USB para diagnóstico e manutenção
- Interface de porta USB para leitor de código de barras

As interfaces fornecidas permitem que o Separador AMICUS inclua conectividade com os seguintes acessórios opcionais:

- Servidor de Aplicação de Gerenciamento de Dados DXT, que faz interface com o Sistema de Gerenciamento de Doadores via interface de rede
- Dispositivo de fotoativação Phelix via interface de comunicação de porta serial

Observação: O Phelix é usado em conjunto com o AMICUS para realizar Fotoferese Extracorpórea (ECP) nas localidades onde é aprovado. O Phelix e a fotorese extracorpórea não são aprovados para uso nos Estados Unidos.

- Pen Drive via Interface de porta USB para diagnóstico e manutenção
- Leitor de código de barras via interface de porta USB para leitor de código de barras

A interface da tela de toque implementa interface homem máquina para todas as interações com usuários do Separador AMICUS. Além disso, o uso do dispositivo AMICUS no ambiente de uso pretendido não requer operação 24 horas por dia, 7 dias por semana, portanto, o dispositivo é ligado e desligado diariamente.

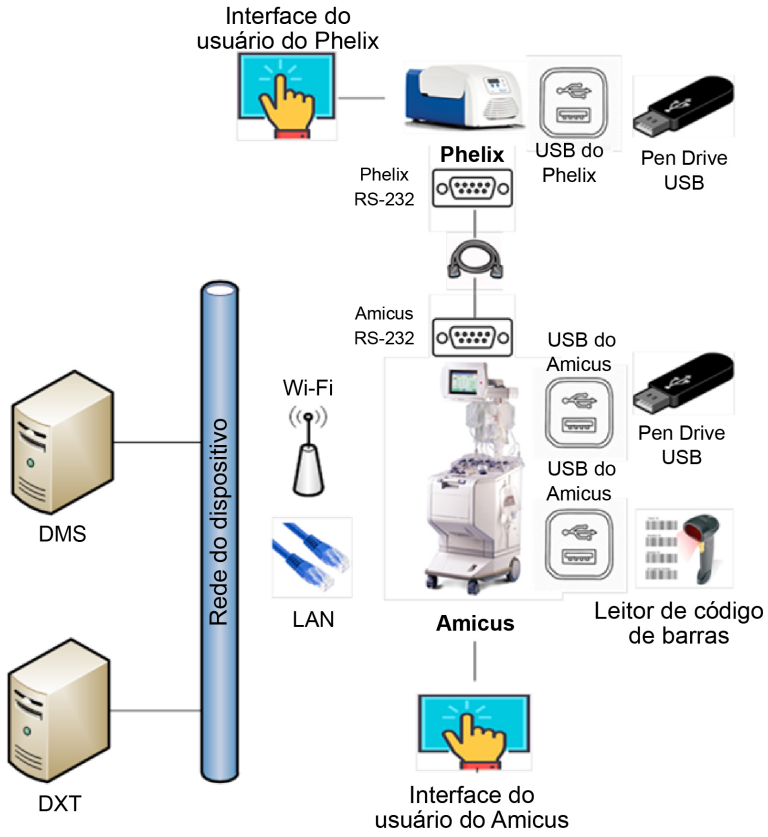

Figura 3: Produtos e accessórios para o modelo 6R4590

Ao isolar os recursos de computação e processos de doação dos processos de comunicação de rede, separamos as funcionalidades críticas do processamento seguro do sangue. Um ataque de segurança cibernética aos recursos de rede do Separador AMICUS não afetaria a integridade ou disponibilidade do procedimento. A separação razoável, lógica e física dos processos de interface do usuário (por exemplo, a tela de toque) dos recursos de rede também foram implementados.

Além disso, as funções que usam interfaces externas (por exemplo, LAN ou USB) são projetadas para exigir a confirmação da ação do operador na interface do usuário do Separador AMICUS. Por fim, as interfaces de rede podem ser totalmente desativadas para isolar o dispositivo de qualquer conectividade remota, sem afetar em nada as funções críticas do processamento de sangue. Embora a proteção completa contra todas as ameaças à segurança cibernética não seja possível sem a implementação adequada pelo clientede uma rede e ambiente seguros e protegidos, essas medidas de isolamento oferecem proteção razoável contra as intrusões e usos indevidos mais prováveis.

Seção 4.0 Especificações de hardware

As funções de computação e conectividade do Separador AMICUS são implementadas com um computador de placa única (SBC), um sistema embarcado fechado. O uso de um SBC em dispositivos como o Separador AMICUS melhora muito a qualidade geral da plataforma computacional, pois o design e os componentes do SBC são validados em uma escala muito maior do que o hardware de propriedade dos fabricantes de dispositivos de baixo volume. A funcionalidade do Separador AMICUS é compatível com as interfaces listadas nas tabelas a seguir:

Tabela 1: Interfaces de hardware para os modelos 4R4580 e 6R4580

Interface	Especificações	Descrição
Rede	RS-232 IEEE 802.11, IEEE 802.3	Adaptador de rede serial Lantronix (Wi-Fi, LAN)
Leitor de código de barras	RS-232	Interface serial para leitores de código de barras compatíveis
Terminal de diagnóstico	RS-232	Interface serial para terminal de diagnóstico
Phelix	RS-232	Interface serial exclusiva para o acessório de fotoferese

Tabela 2: Interfaces de hardware para os modelos 6R4590

Interface	Especificações	Descrição
Rede com fio	IEEE 802.3	Controlador de LAN integrado
Rede sem fio	IEEE 802.11	Adaptador de rede Ethernet para Wi-Fi Lantronix
Leitor de código de barras	USB 2.0	Interface USB para leitores de código de barras compatíveis
Pen Drive	USB 2.0	Interface USB para Pen Drives compatíveis
Phelix	RS-232	Interface serial exclusiva para o acessório de fotoferese

Lista de materiais de segurança cibernética (CBOM)

Consulte as notas de lançamento para obter a CBOM para a versão de software instalada no sistema Separador AMICUS.

Seção 5.0 Portas e serviços de rede

Para os modelos 4R4580 e 6R4580

O Separador AMICUS não inclui uma interface de rede nativa.
A conectividade de rede sem fio ou com fio é fornecida pelo adaptador de rede serial Lantronix.

Todas as portas TCP e UDP estão permanentemente fechadas no adaptador de rede Lantronix, exceto a porta listada abaixo, que é usada para se comunicar com o Servidor de Aplicação de Gerenciamento de Dados DXT:

Tabela 3: Portas e serviços de rede para os modelos 4R4580 e 6R4580

Porta	Protocolo	Nome do serviço	Descrição do serviço	Criptografado	Aberta/ Fechada
10000 - 49100	Intercâmbio eletrônico de dados (EDI) proprietário sobre TCP/IP	DXT Interface	Interface de comunicação com o Servidor de Aplicação de Gerenciamento de Dados DXT para transmitir resultados do procedimento e receber parâmetros de configuração do procedimento	Sim	Aberta

Para os modelos 6R4590

Todas as portas TCP e UDP estão permanentemente fechadas no dispositivo, com exceção das 2 portas listadas abaixo. Não há interface fornecida para abrir portas adicionais:

Tabela 4: Portas e serviços de rede para os modelos 6R4590

Porta	Protocolo	Nome do serviço	Descrição do serviço	Criptografado	Aberta/ Fechada
10000 - 49100	Intercâmbio eletrônico de dados (EDI) proprietário sobre TCP/IP	DXT Interface	Interface de comunicação com gerenciamento de dados DXT servidor de aplicação para relatar resultados do procedimento e receber parâmetros de configuração de procedimentos	Sim	Aberta
49101	Atraso pós-discagem (PDD) proprietário sobre TCP/IP	Dados periódicos Exibir	Dados de diagnóstico interface de saída para assistência técnica de campo engenharia Equipe	Não	Aberta

Seção 6.0 Dados confidenciais transmitidos

O Separador AMICUS recebe do servidor de aplicação de gerenciamento de dados DXT e transmite para ele dois conjuntos principais de informações:

- Parâmetros do procedimento
- Registros do procedimento

Os parâmetros do procedimento são usados para configuração do procedimento. O registro do procedimento contém os resultados do procedimento. Alguns dos elementos de dados incluídos nos parâmetros do procedimento ou registro do procedimento são:

- Identificador do procedimento/doação
- Identificador do doador/paciente
- Peso do doador/paciente
- Altura do doador/paciente
- Contagem de hematócrito do doador/paciente
- Contagem de plaquetas do doador (apenas para procedimentos envolvendo plaquetas)

Embora esses elementos de dados possam ser usados para caracterizar o doador/paciente, eles não são capazes de identificar um indivíduo no sistema AMICUS. Nenhum dos elementos de dados transmitidos tem a intenção de identificar indivíduos. Portanto, os elementos de dados transmitidos não se enquadram na categoria de dados confidenciais.

Dados confidenciais armazenados para os modelos 4R4580 e 6R4580

O Separador AMICUS exige que as credenciais da rede sem fio sejam armazenadas no adaptador de rede Lantronix se a conectividade com a rede for estabelecida usando a interface Wi-Fi do dispositivo. As credenciais da rede Wi-Fi são consideradas dados confidenciais, pois sua exposição não intencional pode levar a acesso não autorizado à rede sem fio. O acesso às credenciais de rede armazenadas só é possível quando um usuário tem acesso físico ao adaptador de rede Lantronix.

Dados confidenciais armazenados para os modelos 6R4590

O Separador AMICUS exige que as credenciais da rede sem fio sejam armazenadas, se a conectividade com a rede for estabelecida usando a interface Wi-Fi do dispositivo. As credenciais da rede Wi-Fi são consideradas dados confidenciais, pois sua exposição não intencional pode levar a acesso não autorizado à rede sem fio. Proteções razoáveis

foram implementadas para limitar o acesso às credenciais de rede armazenadas. Essas proteções incluem a solicitação de entrada da interface do usuário por parte de administradores autenticados (o que, em circunstâncias normais, exige a presença física na frente do dispositivo) para acessar essas informações confidenciais.

Diagrama de fluxo de dados e rede

O ambiente de implantação de rede recomendado, conforme mostrado na Figura 4 e na Figura 5, deve incluir (no mínimo) a implementação da segurança de perímetro de rede com um firewall e a separação de redes locais em uma VLAN dedicada, onde os Separadores AMICUS são instalados. Se configurado corretamente, esse particionamento da rede pode proporcionar proteção contra ameaças externas e reforço no caso de comprometimento da rede corporativa.

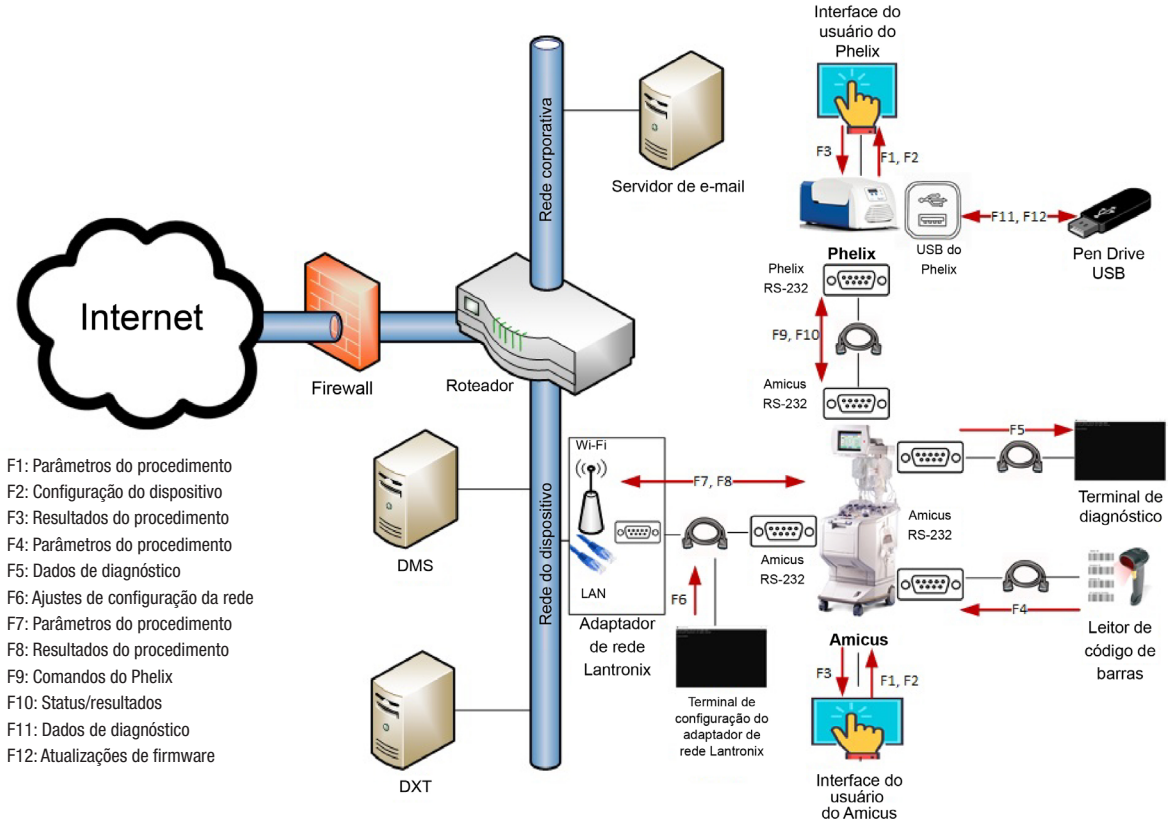

Figura 4: Diagrama de instalação recomendado para os modelos 4R4580 e 6R4580

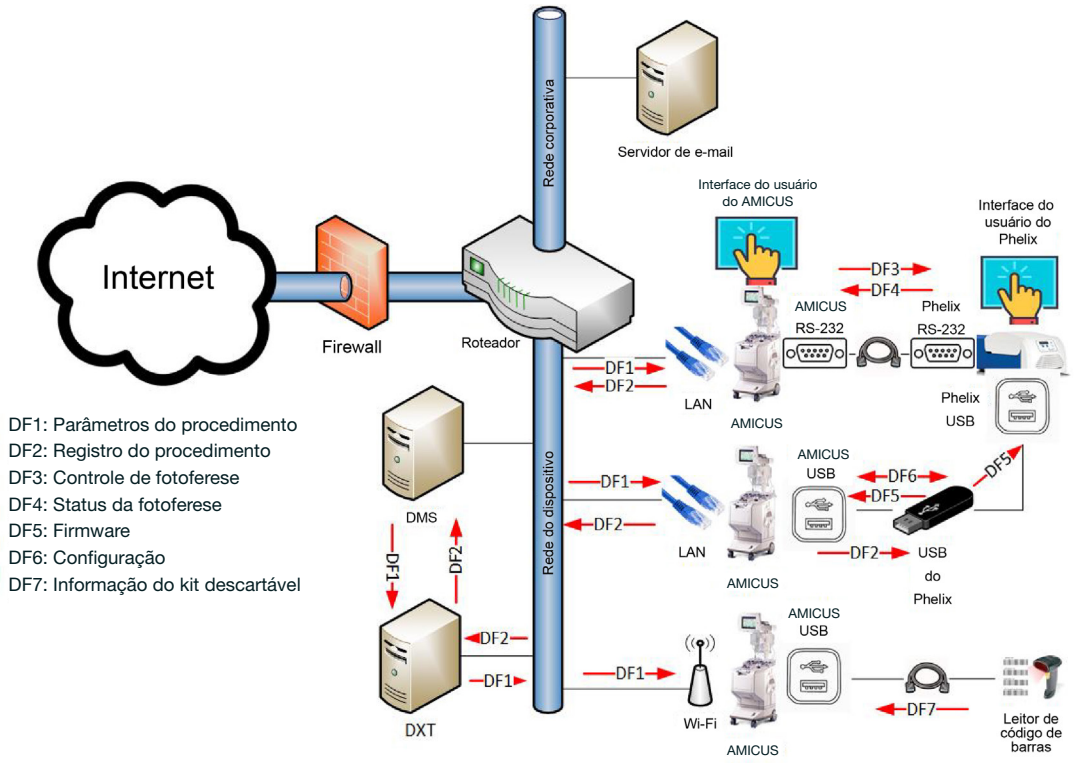

Figura 5: Diagrama de instalação recomendado para os modelos 6R4590

Seção 7.0 Proteção contra malware

Durante o autoteste de inicialização, o Separador AMICUS executa verificações de integridade do sistema contra corrupção, incluindo aquelas que podem ser causadas por malware. Nos modelos 6R4590, medidas adicionais, tais como restrições rigorosas do sistema de arquivos, estão em vigor para proteger o ambiente operacional do software do dispositivo. Como parte da responsabilidade compartilhada do cliente pela proteção da segurança cibernética, um software comercial de proteção antimalware/antivírus deve ser instalado na rede do Separador AMICUS e no ambiente em que está instalado.

Seção 8.0 Autenticação e autorização

Existem três funções de usuário definidas para a operação do Separador AMICUS:

- Operador
- Administrador
- Assistência técnica

A função/conta de operador é usada para executar funções relacionadas ao uso pretendido dos dispositivos. A função de operador não inclui senha. A função pode ser configurada para inserir o identificador do operador em diferentes momentos durante o procedimento. No entanto, por padrão, essa configuração está DESATIVADA para melhorar a usabilidade.

A função/conta de administrador é usada para ajustar as configurações definidas por usuários do dispositivo, como limites e padrões de parâmetros do procedimento e configuração de rede. A função de administrador pode ser configurada para exigir uma senha configurável pelo usuário para acessar as funções autorizadas de administrador.

A função/conta de assistência técnica é usada para executar a manutenção de rotina e os reparos necessários do dispositivo. Nos modelos 4R4580 e 6R4580, o acesso à função de assistência técnica exige acesso ao hardware interno do Separador AMICUS. Nos modelo 6R4590, o acesso à função de assistência técnica é protegido por senha.

Observação: Nenhuma das funções mencionadas pode usar conexão remota para acessar a funcionalidade autorizada para a função. O acesso aos funcionalidade autorizada para a função exige interação com o Separador AMICUS por meio da tela de toque dedicada com interface homem máquina.

Seção 9.0 Controles de rede para os modelos 4R4580 e 6R4580

Os controles de rede são de responsabilidade do administrador do ambiente de instalação, de acordo com as respectivas políticas de TI do usuário. Os controles devem ser avaliados para verificar se atendem às normas pertinentes de gerenciamento de risco de segurança de redes, como a ISO/IEC 80001. As medidas de proteção padrão, como firewall e segmentação de rede, devem estar implementadas antes da instalação

dos dispositivos na rede do usuário. Medidas adicionais, como filtragem MAC, são altamente recomendadas, mas não são obrigatórias.

Atenção: O Separador AMICUS e o sistema de gerenciamento de dados devem ser instalados em um perímetro de rede seguro para evitar o acesso de sistemas externos não autorizados.

O Separador AMICUS e o sistema de gerenciamento de dados devem ser instalados em um perímetro de rede seguro com as seguintes características de TI:

- Compatível com Ethernet 10/100 BASET com fio IEEE 802.3
- Compatível com LAN sem fio (consulte a tabela de configuração do adaptador de rede na seção a seguir para especificações sem fio específicas)
- Logicamente isolado e protegido de redes não confiáveis, como a Internet, ou de domínios menos confiáveis, como e-mail corporativo, por meio de dispositivos de proteção de limite (perímetro), como firewall de inspeção de estados
- Redes devidamente segmentadas, por exemplo, rede corporativa segregada (e-mail, etc.) da rede do dispositivo
- Comunicação sem fio criptografada e com integridade protegida
- Capaz de rastrear e monitorar trilhas de auditoria

Observação: Os dispositivos de proteção de limite controlam o fluxo de informações entre domínios de segurança interconectados. Eles normalmente incluem gateways, roteadores, firewalls, sistemas de análise e virtualização de código malicioso baseados em rede, túneis de intrusão, interfaces gerenciadas, gateways de mensagem e gateways unidirecionais (por exemplo, díodos de dados).

A funcionalidade sem fio faz referência e usa os seguintes protocolos e normas do setor:

- 802.11a/b/g/n/ac são padrões de rede sem fio desenvolvidos pelo Institute of Electrical and Electronics Engineers (IEEE). Consulte as normas ISO/IEC 8802-11 para as redes locais e de áreas metropolitanas para obter mais informações.
- WPA2/802.11i (acesso protegido à rede) é um protocolo de segurança opcional para redes sem fio. Consulte a IEEE 802.11i para obter mais informações.

Atenção: O uso de protocolos de segurança sem fio obsoletos pode aumentar os riscos de segurança cibernética associados à tentativa de um invasor de acessar ou modificar o tráfego da rede. A Fresenius Kabi recomenda o uso dos protocolos WPA2/802.11i.

- O TCP/IP (Protocolo de Controle de Transmissão/Protocolo de Internet) é um protocolo padrão de transporte de dados usado para a Internet e outras redes semelhantes. Consulte RFC 1122 para obter mais informações.

Criptografia

Mesmo que o Separador AMICUS não transmita dados confidenciais, a criptografia do tráfego de rede pode ser ativada, se necessário. A criptografia pode ser habilitada para parâmetros de procedimento e partes do registro do procedimento que incluem elementos de dados considerados características do procedimento de doação. Quando ativada, a criptografia usa um algoritmo com chave de criptografia de 40 bits.

Como o acesso às credenciais de rede armazenadas só é possível com a conexão física ao adaptador de rede Lantronix, as credenciais de rede não são criptografadas.

Seção 10.0 Controles de rede para modelos 6R4590

Os controles de rede são de responsabilidade do administrador do ambiente de instalação, de acordo com as respectivas políticas de TI do usuário. Os controles devem ser avaliados para verificar se atendem às normas pertinentes de gerenciamento de risco de segurança de redes, como a ISO/IEC 80001. As medidas de proteção padrão, como firewall e segmentação de rede, devem estar implementadas antes da instalação dos dispositivos na rede do usuário. Medidas adicionais, como filtragem MAC, são altamente recomendadas, mas não são obrigatórias. Embora o Separador AMICUS tenha proteções rigorosas com foco na conformidade com as normas de segurança aplicáveis, como a NIST, por exemplo, usá-lo em total conformidade com essas normas exige que o cliente forneça uma rede e um ambiente de instalação que também estejam em conformidade.

O Separador AMICUS não permite conectividade de entrada, com exceção das duas portas identificadas na seção Portas e serviços de rede.

Atenção: O Separador AMICUS e o sistema de gerenciamento de dados devem ser implantados em um perímetro de rede seguro para evitar o acesso de sistemas externos não autorizados.

O Separador AMICUS e o sistema de gerenciamento de dados devem ser implantados em um perímetro de rede seguro com as seguintes características de rede de TI:

- Compatível com Ethernet 10/100 BASE-T IEEE802.3 com fio
- Compatível com LAN sem fio (consulte a tabela de configuração do adaptador de rede na seção a seguir para especificações sem fio específicas)
- Logicamente isolado e protegido de redes não confiáveis, como a Internet, ou de domínios menos confiáveis, como e-mail corporativo, por meio de dispositivos de proteção de limite (perímetro), como firewall de inspeção com estado
- Redes devidamente segmentadas, por exemplo, rede corporativa segregada (e-mail, etc.) da rede do dispositivo
- Comunicação sem fio criptografada e com integridade protegida
- Capaz de rastrear e monitorar trilhas de auditoria

Observação: Os dispositivos de proteção de limite controlam o fluxo de informações entre domínios de segurança interconectados. Eles normalmente incluem gateways, roteadores, firewalls, análise de código malicioso baseado em rede e sistemas de virtualização, túneis de intrusão, interfaces gerenciadas, gateways de correio e gateways unidirecionais (por exemplo, diodos de dados).

Esta funcionalidade sem fio faz referência e usa os seguintes protocolos e normas do setor:

- 802.11a/b/g/n/ac são padrões de rede wireless desenvolvidos pelo Institute of Electrical and Electronics Engineers (IEEE). Consulte as normas ISO/IEC 8802-11 para as redes locais e de áreas metropolitanas para obter mais informações.
- WPA2/802.11i (acesso protegido à rede) é um protocolo de segurança opcional para redes wireless. Consulte IEEE 802.11i para obter mais informações.

Atenção: O uso de protocolos de segurança sem fio obsoletos pode aumentar os riscos de segurança cibernética associados à tentativa de um invasor de acessar ou modificar o tráfego da rede. A Fresenius Kabi recomenda o uso dos protocolos WPA2/802.11i.

- TCP/IP (Protocolo de Controle de Transmissão/Protocolo de Internet) é um protocolo padrão de transporte de dados usado para a Internet e outras redes semelhantes. Consulte RFC 1122 para obter mais informações.

- EDI é o protocolo de comunicação proprietário do fabricante do instrumento baseado nos padrões da American Society for Testing and Materials (ASTM E 1394-97). O protocolo EDI fornece comunicação na camada de aplicação.

Criptografia

Mesmo que o Separador AMICUS não transmita dados de identificação pessoal conforme tratado na Seção 5 deste suplemento, o sistema pode ser configurado para criptografar dados de EDI transmitidos pela interface de rede. O algoritmo usado por esse recurso apresenta força de chave de criptografia de 56 bits para criptografar o registro do procedimento.

Atenção: Deixar de ativar a criptografia dos parâmetros do procedimento pode aumentar os riscos de segurança cibernética associados à tentativa de um invasor de acessar ou modificar os dados de EDI. Enquanto outros controles de defesa profunda estão em vigor para mitigar esses riscos, a Fresenius Kabi recomenda a ativação da criptografia dos parâmetros do procedimento.

Uma vez que o acesso a credenciais de rede armazenadas exige entrada da interface do usuário por parte de administradores autenticados (o que, em circunstâncias normais, exige a presença física na frente do dispositivo), o dispositivo não criptografa essas informações armazenadas.

Seção 11.0 Registro de auditoria

O sistema Separador AMICUS armazena todos os registros internamente em seu cartão de memória flash compacto. Os registros implementados incluem:

- Registro de eventos do sistema
- Registros do procedimento
- Registros de dados do procedimento
- Registros de execução do sistema

O acesso aos registros é limitado e depende da função do usuário. Por exemplo:

- O operador não tem acesso aos registros.
- Nos modelos 6R4590, o administrador pode apenas exportar os registros do procedimento para um Pen Drive USB.

- Nos modelos 6R4590, os usuários de assistência técnica podem exportar todos os registros para um Pen Drive USB, visualizar os registros de eventos do sistema na tela do AMICUS ou excluir todos os registros do sistema.

- Nos modelos 4R4580 e 6R4580, os usuários de assistência técnica podem exportar todos os registros substituindo o cartão de armazenamento compacto, visualizar os registros de eventos do sistema na tela do AMICUS ou excluir todos os registros do sistema.

Para os modelos 6R4590, consulte o Volume 1, Capítulo 3 do Manual do Operador AMICUS para mais instruções sobre como exportar relatórios do procedimento.

Os registros do procedimento são apresentados no formato de arquivo de texto. Eles são criados quando o operador inicia um procedimento. Os registros contêm dados do procedimento, entradas do operador, número do operador, todos os eventos relacionados ao procedimento (com o progresso do procedimento no momento do evento) e resultados do procedimento. Nos modelos 6R4590, os registros do procedimento exportados para um Pen Drive USB não são criptografados.

O registro de eventos do sistema é um arquivo binário cíclico para registrar os principais eventos do sistema, como inicialização, mudança de estado de segurança e eventos do início de procedimento. É possível apresentar o conteúdo desse arquivo para o usuário de assistência técnica na tela do AMICUS.

Seção 12.0 Detecção e resposta

Nos casos em que um evento de segurança interrompe um procedimento disparando um alerta de procedimento, o protocolo de segurança correto é executado e a notificação normalmente é exibida na interface do usuário do dispositivo.

Em todos os casos de violação de segurança, é aconselhável que o cliente isole o dispositivo comprometido de acordo com suas políticas de segurança de TI e entre em contato com a Fresenius Kabi para obter mais ajuda com o incidente.

Observação: Nos modelos 4R4580 e 6R4580, a senha do Wi-Fi deve ser atualizada periodicamente de acordo com as políticas de TI do ambiente de instalação.

Observação: Nos modelos 4R4580 e 6R4580, a senha do Wi-Fi deve ser atualizada imediatamente após a detecção de intrusão não autorizada na rede de instalação.

Observação: Nos modelos 4R4580 e 6R5480, a interface serial entre o Separador AMICUS e o adaptador de rede Lantronix deve ser desconectada em caso de violação confirmada de segurança da rede de instalação e deve permanecer desconectada até que a segurança da rede seja restaurada.

Seção 13.0 Backup e restauração

Nos modelos 4R4580 e 6R4580, o sistema Separador AMICUS não oferece a funcionalidade de backup ou restauração.

Para os modelos 6R4590, o Separador AMICUS oferece funcionalidade de importação/exportação da configuração e dados do dispositivo via interface USB que pode ser usada para arquivamento, retenção e restauração de componentes essenciais do dispositivo. O cliente pode implementar procedimentos de backup e restauração da configuração e dados do dispositivo usando esta funcionalidade para fazer backup com segurança dos componentes desejados do dispositivo e reter essas informações em caso de procedimentos de recuperação de desastres.

Seção 14.0 Conectividade remota

Conforme explicado anteriormente, a proteção abrangente das funções de conectividade do Separador AMICUS contra ameaças à segurança cibernética depende não apenas das proteções integradas ao sistema Separador AMICUS, mas também da proteção e segurança da rede do cliente e do ambiente de instalação.

O Separador AMICUS não oferece o tipo tradicional de conectividade remota, como desktop remoto, que permite o controle direto do dispositivo a partir de um aplicativo remoto. No entanto, o Separador AMICUS fornece uma interface para o servidor de aplicação de gerenciamento de dados DXT para receber parâmetros do procedimento de um sistema externo de gerenciamento de doadores. Isso permite a substituição da entrada manual de parâmetros pelo método eletrônico, o que reduz os erros decorrentes da entrada manual de dados.

A interface com o servidor de aplicação de gerenciamento de dados DXT também é usada para relatar os resultados do procedimento após sua conclusão. Os relatórios do procedimento podem ser usados para que a funcionalidade de eficiência operacional ative o registro de tendências de diferentes aspectos do procedimento, para identificar áreas de melhoria na forma como o dispositivo é operado no ambiente do usuário final.

Os relatórios de procedimento também podem ser usados na funcionalidade de registro eletrônico para complementar o perfil do doador mantido pelo sistema de gerenciamento de doadores. Essa conectividade é oferecida na interface definida anteriormente na seção Portas e serviços de rede.

Seção 15.0 Tratamento de assistência técnica

A manutenção de rotina inclui calibração do dispositivo e download do Relatório de informações do sistema. Os relatórios do procedimento são recuperados do dispositivo apenas se houver um relatório indicando perda de dados ou mau funcionamento do dispositivo durante um procedimento. Nenhuma das tarefas de manutenção de rotina pode ser realizada remotamente, pois exigem a presença física do engenheiro de serviço de campo junto ao instrumento.

Fim da vida útil e fim do período de suporte

Atualmente não há ciclo de fim de vida útil ou fim de período de suporte para o Separador AMICUS.

Quando uma data de fim de vida útil for determinada para este dispositivo ou versão de software, uma comunicação será enviada aos clientes afetados.

Padrões de codificação segura

O firmware do Separador AMICUS é desenvolvido usando padrões de codificação patenteados para desenvolvimento em linguagem C com base nas práticas recomendadas de engenharia de software. É importante salientar que o Separador AMICUS passa por rigorosos processos de revisão de código e análise estática.

Padrões de reforço do sistema

Nenhum padrão de reforço foi implementado para o Separador AMICUS.

Seção 16.0 Upgrade de firmware

As atualizações de firmware só podem ser aplicadas pelo pessoal de assistência técnica da Fresenius Kabi ou por indivíduos treinados e certificados pela Fresenius Kabi de acordo com os respectivos Boletins de Serviço Técnico. O usuário deve entrar em contato com seu representante da conta da Fresenius Kabi para receber atualizações de firmware para o AMICUS.

Seção 17.0 Resumo de riscos

Operação fora do ambiente de instalação pretendido

Não instalar o sistema de aférese AMICUS em um ambiente seguro pode aumentar a probabilidade das seguintes situações de risco:

- Uma rede de TI inadequadamente segmentada ou segregada pode tornar ineficazes os controles de segurança existentes e sofrer ataques cibernéticos, tais como os ataques “Denial-of-Service” ou “Man-in-the-Middle”.

- A falta de dispositivos de proteção de perímetro devidamente configurados, como um firewall, pode permitir que dados desnecessários ou mesmo dados prejudiciais (malware) sejam inseridos ou se espalhem pelas redes, o que torna os dados críticos ou confidenciais suscetíveis a monitoramento, à interceptação ou sujeitos a ataques cibernéticos.

- Não instalar um software antimalware em redes de TI pode comprometer a integridade e a disponibilidade do Separador AMICUS.

- A falta de rastreamento e monitoramento adequado das trilhas de auditoria pode resultar em incidentes indetectáveis, o que pode prejudicar os esforços de resposta e recuperação no caso de um incidente cibernético.

Os riscos residuais de um Separador AMICUS conectado estão listados na tabela a seguir, em conjunto com a justificativa para sua aceitação:

Tabela 5: Risco residual para os modelos 4R4580 e 6R4580

Riscos de segurança residuais	Justificativa para aceitação
A obtenção de informações de configuração de rede do Separador AMICUS pode permitir que um invasor se conecte à rede do ambiente de implantação e invada outros sistemas.	Os riscos podem ser gerenciados adequadamente com a implementação da devida segmentação de rede pelo cliente para segregar os separadores AMICUS de outros sistemas — além da implementação, por parte das políticas de TI adequadas, de mecanismos de autorização com o nível mais baixo de privilégio possível.
Impacto ao perfil de doadores/ pacientes no que diz respeito ao histórico de doações/tratamentos registrado no sistema de gerenciamento de doadores com base nas informações recebidas do Separador AMICUS.	Este risco pode ser gerenciado de forma adequada com a implementação de protocolos de segurança adequados que exijam a análise dos resultados do procedimento relatados no contexto da prescrição da doação/tratamento.

O ataque “Denial-of-Service” pode impedir que o sistema ofereça a funcionalidade de configuração remota do procedimento ou documentação de procedimento eletrônica.	Esse risco pode ser gerenciado adequadamente com políticas adequadas de senha e monitoramento da rede de TI. Além disso, as funcionalidades integradas de inserção manual de parâmetros de procedimento e de armazenamento temporário dos registros de procedimentos no dispositivo estão em vigor para reduzir o risco de ataques até que o perímetro da rede esteja seguro.

Tabela 6: Risco residual para os modelos 6R4590

Riscos de segurança residuais	Justificativa para aceitação
A obtenção de informações de configuração de rede do Separador AMICUS pode permitir que um invasor se conecte à rede do ambiente de implantação e invada outros sistemas.	Os riscos podem ser gerenciados adequadamente com a implementação da devida segmentação de rede pelo cliente para segregar os Separadores AMICUS de outros sistemas — além da implementação, por parte das políticas de TI adequadas, de mecanismos de autorização com o nível mais baixo de privilégio possível.
Impacto ao perfil de doadores/pacientes no que diz respeito ao histórico de doações/tratamentos registrado no sistema de gerenciamento de doadores com base nas informações recebidas do Separador AMICUS.	Este risco pode ser gerenciado de forma adequada com a implementação de protocolos de segurança adequados que exijam a análise dos resultados do procedimento relatados no contexto da prescrição da doação/tratamento.
Firmware não autorizado anula o status validado das condições operacionais do Separador AMICUS.	Como a atividade de upload de firmware exige presença física na frente do dispositivo, que deve ser colocado no modo de assistência técnica dedicado, esse risco pode ser gerenciado de forma apropriada com a implementação dos devidos protocolos de segurança e acesso físico.

Embora os riscos residuais de habilitar as funções de conectividade do dispositivo AMICUS devam ser conhecidos e reconhecidos pelo administrador do ambiente de instalação do dispositivo, os benefícios de habilitar a configuração eletrônica de procedimentos e o relatório eletrônico de resultados de procedimentos (o que praticamente elimina o problema significativo da inserção manual de dados incorretos) superam muito o riscos remanescentes, considerando os controles já existentes que estão em vigor.

Divulgação coordenada de vulnerabilidades (CVD)

A Fresenius Kabi divulgará todas as vulnerabilidades conhecidas de acordo com o processo de CVD. A Fresenius Kabi aceitará os relatórios de vulnerabilidades recentemente descobertas de acordo com o processo de CVD. Entre em contato com seu representante da Fresenius Kabi para obter acesso aos recursos de CVD.

Seção 18.0 Declaração de divulgação do fabricante para segurança de dispositivos médicos

Formulários para o Separador AMICUS podem ser fornecidos sob demanda. Entre em contato com o representante da conta da Fresenius Kabi para saber mais.

Seção 19.0 Isenção de responsabilidade

A Fresenius Kabi não promete ou garante aos clientes que qualquer um dos métodos ou sugestões descritos neste suplemento de segurança cibernética restaurará os sistemas do cliente, evitará erros de procedimento, resolverá quaisquer problemas relacionados a qualquer código malicioso ou proporcionará quaisquer outros resultados declarados ou pretendidos. O cliente assume exclusivamente todos os riscos relacionados com o uso ou não uso das orientações apresentadas neste Suplemento de segurança cibernética.

Esta página foi deixada em branco intencionalmente.

FRESENIUS KABI

Fresenius Kabi AG
Else-Kröner-Str. 1
61352 Bad Homburg
Germany
Tel.: +49 (0) 61 72 / 686-0
www.fresenius-kabi.com

Fresenius Kabi Warrendale
770 Commonwealth Dr.
Warrendale, PA 15086 USA

Para os US:
1-800-933-6925

US

CE **0123** A marcação CE não se aplica aos códigos 4R4580, 4R4580R e 4R4580TH.