Baxter	**POLÍTICA CORPORATIVA** **Política de Segurança das Informações de Terceiros**	
ÁREA FUNCIONAL: **Diretoria Baxter Hospitalar Ltda.**	**DATA DE EMISSÃO:** **18 de setembro 2020**	**DOCUMENTO Nº:** **03/2020**
PROPRIETÁRIO DA POLÍTICA: **Diretor Presidente, Diretor Juridico, Diretoria de Tecnologia da Informação**	**DATA DE VIGÊNCIA:** **18 de setembro 2020**	**VERSÃO:** 1
ESPECIALISTAS NO ASSUNTO: **Diretor Presidente, Diretor Juridico, Diretor TI, DPO**	**PRÓXIMA DATA DE REVISÃO AGENDADA:** **01 de agosto de 2021**	

Política de Segurança das Informações de Terceiros

Esta política está em conformidade com as políticas globais da **Baxter International Inc.**, a **Baxter Healthcare Corporation** e suas subsidiárias e afiliadas, incluindo a **Baxter Hospitalar Limitada** ("**Baxter**") e estabelece os requerimentos de segurança das informações da Baxter e suas afiliadas aplicáveis a fornecedores/prestadores de serviços ("**Terceiros**") com relação à confidencialidade, integridade e disponibilidade de "Informações", conforme definidas abaixo ("**Política de Segurança das Informações**" ou "**Política**").

A. OBJETIVO

O objetivo da Política de Segurança das Informações é:

1. Fornecer um conjunto claro e abrangente de requisitos para que os Terceiros evitem perdas, danos, roubo e acesso não autorizado aos recursos e Informações da Baxter;

2. Definir o comportamento ético e lícito dos Terceiros que manuseiam e interagem com os recursos e Informações da Baxter;

3. Aumentar a consciência da segurança das informações entre os Terceiros; e

4. Estabelecer responsabilidades e declarar claramente as consequências do uso inadequado das Informações e/ou recursos da Baxter**.**

B. ESCOPO E APLICABILIDADE

Esta Política de Segurança das Informações se aplica a todos os Terceiros e qualquer outra pessoa física ou jurídica contratada da Baxter que usa ou acessa os recursos e Informações da Baxter. Esta Política deve estar disponível e comunicada a todas as pessoas que usam e acessam Informações e recursos da Baxter. Esta Política abrange todos os recursos e Informações eletrônicos da Baxter dentro de locais pertencentes e não pertencentes à Baxter.

C. DEFINIÇÕES

Nesta Política de Segurança das Informações, sempre que iniciados em letras maiúsculas, além dos termos expressamente definidos ao longo deste documento, os termos e expressões abaixo indicados, no singular ou no plural e independentemente do gênero, terão os seguintes significados e definições:

"**Dados Pessoais**" tem o significado a ele atribuído na Política de Proteção de Dados para Fornecedores e inclui Dado Pessoal Sensível.

"**Disponibilidade**" significa garantir que usuários autorizados de Terceiros tenham acesso às Informações e aos sistemas de tratamento associados, quando necessário.

"**Informação**" significa quaisquer Informações Confidenciais e Dados Pessoais utilizados com propósitos comerciais pela Baxter.

"**Informações Confidenciais**" significa qualquer informação confidencial ou exclusiva, conforme definida em qualquer acordo por escrito entre o Terceiro e a Baxter.

"**Integridade**" tem o condão de proteger a precisão e integridade das Informações e seus métodos de Tratamento associados.

"**Registro**" é a Informação que tem valor comercial, legal, operacional, de conformidade ou histórico contínuo e que a organização é obrigada por lei a reter ou pretende reter como comprovação de seu negócio por um período específico.

D. USO PESSOAL DOS RECURSOS DA BAXTER

Os recursos da Baxter são fornecidos para fins comerciais. Os Terceiros são responsáveis pelo uso por seus funcionários, gerentes, diretores, administradores, consultores e colaboradores dos recursos da Baxter de maneira profissional, ética e legal em todos os momentos. O uso pessoal incidental é permitido, mas não deve:

1. Interferir na produtividade e desempenho de trabalho do Terceiro ou de qualquer outra pessoa;

2. Impactar negativamente a disponibilidade e o desempenho dos recursos da Baxter; ou

3. Violar qualquer outra disposição desta ou de qualquer outra política da Baxter, inclusive a Política de Proteção de Dados para Fornecedores.

E. USO INACEITÁVEL DE RECURSOS ELETRÔNICOS

As seguintes atividades são estritamente proibidas:

1. Tentar aproveitar os direitos de acesso existentes para ler, alterar ou copiar Informações sem autorização;

2. Tentar "hackear" ou contornar os controles de segurança para obter acesso às Informações ou recursos da Baxter;

3. Tentar alterar ou modificar as configurações de segurança estabelecidas de quaisquer recursos atribuídos da Baxter (por exemplo, computador, laptop, telefones celulares e dispositivos), independentemente de ser para fins comerciais legítimos;

4. Desativar qualquer software de segurança (ou seja, antivírus ou firewall) em qualquer recurso gerenciado ou de propriedade da Baxter;

5. Instalar hardware na rede ou sistemas da Baxter (por exemplo, switch de rede, ponto de acesso sem fio);

6. Instalar qualquer software ou executar qualquer arquivo executável não pré-aprovado pelo Suporte Técnico da Baxter;

7. Conectar à rede da Baxter (à exceção da Rede de Convidados da Baxter) computadores ou dispositivos não emitidos pela Baxter;

8. Transferir ou armazenar informações da Baxter para computadores, dispositivos ou recursos de colaboração não emitidos pela Baxter, incluindo: computador pessoal, tablets, telefones celulares, dispositivos de armazenamento, contas de e-mail não pertencentes à Baxter e outros sites de armazenamento ou aplicativos não pertencentes à Baxter baseados na nuvem/Internet (por exemplo, Box, Dropbox, Google Drive; OneDrive);

9. Baixar, instalar, armazenar, transmitir ou distribuir músicas, filmes, software ou jogos não licenciados ou protegidos por direitos autorais da Internet ou qualquer outra coisa que viole o Código de Ética da Baxter ou as leis locais/do país; e

10. Baixar, visualizar ou distribuir material de natureza discriminatória, assediadora, ameaçadora, sexual, pornográfica, racista, sexista, difamatória ou de outra forma ofensiva.

F. COMUNICAÇÕES ELETRÔNICAS

Deverá haver discrição e respeito às leis aplicáveis (como Lei Geral de Proteção de Dados) ao comunicar qualquer Informação em qualquer sistema eletrônico, como e-mail, aplicativos de mensagens instantâneas, salas de bate-papo e grupos de notícias.

Essas Informações não devem ser transmitidas para outros, a menos que esteja em conformidade com o contrato celebrado com a Baxter e a lei aplicável. Se autorizados, os usuários devem tomar cuidado especial para garantir que tais Informações sejam devidamente protegidas durante a comunicação (ou seja, criptografadas) e enviadas apenas para aqueles autorizados a receber tais informações (consulte “Segurança de Dados” a seguir para obter instruções sobre como proteger as comunicações eletrônicas).

As comunicações e mensagens eletrônicas não devem conter conteúdo que possa ser considerado ofensivo, perturbador, difamatório ou depreciativo, incluindo, entre outros, comentários ou imagens sexuais, calúnias raciais ou outros comentários ou imagens que ofendam alguém com base em sua raça, nacionalidade, sexo, orientação sexual, religião, convicções políticas, deficiência ou outra situação legalmente protegida.

Os usuários de Terceiros que encontrarem ou receberem material questionável devem relatar imediatamente o incidente ao Help Desk Global, Segurança Global das Informações, Recursos Humanos ou Segurança Corporativa.

As seguintes atividades específicas envolvendo comunicações eletrônicas são proibidas:

1. Comunicar ou transmitir Registros e Informações por meio de canais de comunicação não aprovados;

2. Enviar cartas em corrente, e-mails indesejados e mensagens de e-mail em massa não autorizadas dentro ou fora da Baxter;

3. Enviar ou encaminhar spam de qualquer conta de e-mail da Baxter ou por meio do uso de qualquer ativo do sistema de informações da Baxter;

4. Enviar e-mails e mensagens “falsificados” (ou seja, modificar o campo “De” ou qualquer outra informação do remetente para fazer com que um e-mail pareça ter vindo de outra pessoa);

5. Listar endereços de e-mail privados (ou outros que não sejam o endereço de e-mail atribuído à Baxter – @baxter.com ou ao domínio do Terceiro) como um ponto de contato comercial. Isso inclui a listagem de endereços de e-mail privados não aprovados em qualquer cartão de visita, papel timbrado, material promocional ou mensagem de correio de voz da Baxter ou do Terceiro;

6. Usar uma cópia eletrônica da assinatura de outra pessoa sem a permissão do titular da assinatura. Observe que o envio de e-mails em nome de outra pessoa (por exemplo, um Assistente Administrativo enviando um e-mail em nome de um Executivo), quando autorizado e indicado no e-mail, é aceitável;

7. Usar computadores ou dispositivos da Baxter para participar de fóruns públicos ou privados online, blogs, wikis ou outros sites para qualquer fim que não seja o uso comercial permitido; e

8. Usar contas de e-mail pessoais ou mídia social para negócios da Baxter ou quaisquer contas de e-mail ou mídia social que não sejam de propriedade, aprovadas ou autorizadas para uso pela Segurança Global das Informações para uso na condução de negócios da Baxter.

G. PRIVACIDADE, DIREITO DE MONITORAMENTO E INVESTIGAÇÕES

Os recursos eletrônicos da Baxter que são distribuídos e fornecidos a empregados, contratados e Terceiros são destinados ao uso comercial da Baxter. Na medida em que seja consistente com as leis locais pertinentes, a Baxter reserva-se o direito de inserir, acessar, digitalizar, monitorar e registrar quaisquer recursos de propriedade da Baxter ou não pertencentes à Baxter conectados à rede da Baxter para garantir a produtividade, comportamento ético e conformidade com as políticas de segurança e padrões pertinentes da Baxter, assim como com as leis aplicáveis. Isso inclui, entre outros:

1. Monitoramento de sites visitados;

2. Monitoramento e revisão do material baixado ou carregado na Internet;

3. Revisão de comunicações eletrônicas enviadas e recebidas por usuários da Baxter (por exemplo, e-mail ou aplicativos de mensagens instantâneas);

4. Monitoramento do tráfego e atividade da rede de propriedade da Baxter; e

5. Digitalização de conteúdo eletrônico de sistemas da Baxter.

As investigações de suposto uso impróprio, crime ou outra ofensa ou violação das políticas da Baxter podem ser realizadas por pessoal apropriado. Os usuários sendo investigados normalmente não serão informados de que estão sendo investigados. Os resultados de tais investigações serão informados à administração da Baxter apropriada para ações futuras. A Baxter pode permitir o acesso de organizações de aplicação da lei com relação a qualquer investigação ou processo de qualquer ação relacionada ao acesso não autorizado ou uso impróprio de sistemas de informações da Baxter.

H. CONFORMIDADE

O não cumprimento ou violação desta Política pode resultar em rescisão do contrato e, inclusive, em medidas administrativas e judiciais adicionais.

Todos os Terceiros devem cumprir e fazer com que seus funcionários, gerentes, diretores, administradores, consultores e colaboradores cumpram todas as leis e regulamentos locais relevantes, os quais prevalecerão em caso de conflito com esta Política e políticas relacionadas.

Em raras circunstâncias, pode ser permitido solicitar uma exceção a esta Política. O Diretor Global de Privacidade (ou designado) e/ou Diretor de Segurança das Informações (ou designado) deve aprovar as exceções de conformidade.

Exceções a esta Política somente serão consideradas se circunstâncias especiais não permitirem a implementação prática de uma exigência e se houver controles de compensação em vigor para mitigar o risco de segurança das Informações. Esses itens serão tratados e considerados caso a caso.

I. RESPONSABILIDADES DO TERCEIRO

Os recursos da Baxter estão disponíveis para permitir e aprimorar a capacidade de cada usuário de conduzir negócios. Todos os usuários compartilham a responsabilidade de proteger os recursos, Registros e Informações da Baxter. As seguintes responsabilidades específicas do usuário final devem ser seguidas para garantir uma postura de segurança forte:

1. GESTÃO DE ATIVOS

Tomar medidas razoáveis para proteger fisicamente os ativos, inclusive aqueles atribuídos à Baxter (por exemplo, laptops, telefones, tablets, dispositivos de armazenamento) e garantir que os ativos sejam protegidos contra perda ou roubo, incluindo:

- ✓ Usar um cabo de segurança, se disponível, para manter os laptops atribuídos bloqueados;
- ✓ Não deixar ativos em um carro por longos períodos. Se for necessário deixá-los por um curto período de tempo, guardá-los no porta-malas ou certificar-se de que não estejam visíveis e trancar o carro;
- ✓ Não despachar bagagem contendo laptops ou outros dispositivos atribuídos;
- ✓ Verificar se os documentos impressos que contêm Informações Confidenciais e/ou Dados Pessoais estão protegidos em contêineres ou salas trancados quando não estiverem em uso para evitar divulgação não autorizada;

- ✓ Devolver todos os ativos da Baxter após a rescisão do contrato/obrigação contratual; e

- ✓ Comunicar imediatamente qualquer dispositivo (atribuído à Baxter) perdido ou roubado a: Help Desk Global da Baxter, Segurança Global das Informações ou Segurança Corporativa.

2. IDS DA CONTA E SENHAS

Os Terceiros são responsáveis por manter a integridade de suas contas, protegendo todas as credenciais de acesso (por exemplo, IDs da conta e senhas). Como tal, os Terceiros são responsáveis por qualquer atividade que ocorra com sua ID da conta e senha. Para proteger as senhas, os Terceiros:

- ✓ Não devem usar, para contas Baxter, a mesma senha usada para qualquer outra conta que não seja da Baxter;

- ✓ Podem usar software de gestão de senha pré-aprovado;

- ✓ Não devem armazenar sua senha no computador ou próxima a ele;

- ✓ Não devem compartilhar suas senhas com ninguém;

- ✓ Não devem fazer login em um sistema com IDs da conta e/ou senha de outra pessoa;

- ✓ Devem manter Histórico e expiração periódica;

- ✓ Possuir comunicação segura de senhas temporárias e solicitação de alteração após o primeiro uso;

- ✓ Providenciar alteração imediata das senhas quando houver motivos para acreditar que uma conta foi comprometida;

- ✓ Providenciar alteração das senhas das contas de sistemas, serviços e sistemas compartilhados quando qualquer pessoa que conheça a senha for desligada ou mudar para uma posição diferente que não exija mais o acesso;

- ✓ Providenciar verificação da identidade do usuário antes da redefinição de senha;

- ✓ Providenciar alteração de todas as senhas padrão a partir da definição de novos valores padrão; e

- ✓ Os requisitos de força da senha devem atender à extensão padrão (i.e. ISO e NIST) e à complexidade comum de segurança.

3. CONECTIVIDADE

A conectividade com os dispositivos da Baxter deve ser protegida quando fora das instalações da Baxter e/ou do Terceiro.

Os usuários do Terceiro devem:

- ✓ Usar a transmissão protegida aprovada pela Baxter, como Zscaler ou outras Redes Privadas Virtuais (“VPN”) fornecidas pela Baxter ou pelo Terceiro;

- ✓ Desconectar as conexões de transmissão protegidas aprovadas pela Baxter e/ou do Terceiro quando não estiverem em uso; e

- ✓ Desativar a conexão sem fio em laptops quando não estiverem em uso.

4. SEGURANÇA DE DADOS

É imperativo proteger as Informações e Registros da Baxter, de nossos clientes, pacientes, profissionais da saúde e empregados contra divulgação não autorizada ou acidental. Portanto, os Terceiros devem garantir e assegurar que os seus usuários finais:

- ✓ Sempre que possível, devem armazenar informações classificadas como Restritas, Altamente Restritas ou Propriedade Intelectual no armazenamento pré-aprovado e seguro de acordo com as melhores práticas do mercado (por exemplo, OneDrive, SharePoint, Teams), em vez de laptops/estações de trabalho locais. Se tais recursos estiverem indisponíveis, como em um voo, as informações salvas em dispositivos locais devem ser movidas para o armazenamento pré-aprovado quando disponível;

- ✓ Devem garantir a destruição imediata de Informações dos dispositivos após a conclusão da necessidade do negócio;

- ✓ Devem compartilhar Informações apenas com as partes internas e externas que estão autorizadas a recebê-los. Se você não tiver certeza se eles estão autorizados, entre em contato com a Segurança de TI do Terceiro e/ou da Baxter; e

- ✓ Criptografar as Informações que contêm Informações antes de enviar pela Internet ou para uma pessoa física ou jurídica que não seja da Baxter ou do Terceiro.

5. GESTÃO DE ACESSO

Os usuários dos Terceiros devem apenas obter o acesso mínimo necessário para o usuário desempenhar sua função de trabalho, e devem garantir que o acesso solicitado não entre em conflito com os direitos de acesso existentes e a segregação de funções. Os gerentes também são obrigados a alterar ou revogar em tempo hábil o acesso que não seja necessário.

Para garantir que o acesso apropriado seja mantido, os gerentes devem revisar o acesso do usuário final pelo menos uma vez por ano ou com mais frequência, quando o nível de risco ou criticidade de um sistema justificar maior supervisão.

6. RELATANDO INCIDENTES DE SEGURANÇA E ATIVIDADE SUSPEITA

Os usuários finais são a primeira linha de defesa na proteção da Informação, seus recursos e dados. Portanto, todos os usuários devem relatar quaisquer incidentes de segurança ou atividades suspeitas para investigação o mais rápido possível para o setor responsável no Terceiro ou na Baxter (para: Help Desk Global da Baxter, Segurança Global das

Informações ou Segurança Corporativa), conforme o caso. Deixar de relatar incidentes de segurança ou atividades suspeitas em tempo hábil pode resultar em rescisão do contrato imediatamente e eventuais medidas administrativas e judiciais.

As informações de contato para relatar um incidente de segurança ou atividade suspeita podem ser encontradas na aba *Cybersecurity* no site da Baxter: https://worksites.baxter.com/sites/cybersecurity.

Os incidentes de segurança incluem:

- ✓ Dispositivos perdidos ou roubados;
- ✓ Informações/dados perdidos ou roubados, independentemente de estarem impressos ou em mídia/dispositivos eletrônicos;
- ✓ Informações enviadas intencionalmente ou acidentalmente ao destinatário errado;
- ✓ Clicar no link de um e-mail suspeito;
- ✓ Baixar software e/ou arquivos não autorizados da Internet para um dispositivo da Baxter ou do Terceiro;
- ✓ Compartilhar contas de usuário e senhas;
- ✓ Comprometimento da senha do usuário usada em outra conta que não seja da Baxter; e
- ✓ Ativos de acesso físico perdidos.

Atividades suspeitas podem incluir:

- ✓ Atividade ou mensagens estranhas/anormais em uma estação de trabalho ou laptop;
- ✓ Pop-ups e/ou outras evidências de malware, vírus e spyware; e
- ✓ Qualquer tentativa inadequada de danificar, interromper, acessar, copiar e/ou transmitir recursos e informações.

J. TREINAMENTO

Empregados, colaboradores, prestadores de serviços, diretores, gerentes e consultores à serviço do Terceiro devem realizar e concluir treinamento de segurança de informações, que contenha requisitos para proteção e tratamento seguro das Informações. Um relatório contendo um resumo do treinamento concluído deverá ser disponibilizado mediante solicitação da Baxter.

O Terceiro deve ter um *Data Privacy Officer* (Encarregado) ou, caso a autoridade nacional de proteção de dados o dispense, então o Terceiro deve, no mínimo, ter um representante como ponto de contato para todos os itens relacionados à segurança da Informação. Além disso, o Terceiro deverá ter um responsável por supervisionar o cumprimento desta Política de Segurança das Informações.

K. PRÁTICAS DE SEGURANÇA DE RECURSOS HUMANOS

Acordos de confidencialidade, termos de consentimento, notificação de privacidade e/ou documentos semelhantes e equivalentes devem estar vigentes para todos os funcionários e devem incluir:

- ✓ Obrigações de confidencialidade durante e após o emprego;
- ✓ Disposições regendo o uso aceitável de recursos eletrônicos, incluindo, entre outros, o uso de recursos eletrônicos de maneira profissional, legal e ética; e
- ✓ Notificação de Privacidade, por meio da qual manterá sigiloso os dados Tratados e consentirá com o Tratamento dos seus Dados Pessoais para fins de eventual relação contratual, legítimo interesse e/ou cumprimento de obrigação legal pela Baxter.

Deve haver procedimento ou política vigentes para identificar e coletar ativos (físicos e eletrônicos) dos indivíduos que se desligarem ou deixarem o Terceiro ou para aqueles que não precisam mais de acesso às Informações.

L. LOG-IN E MONITORAMENTO

As atividades de log-in devem ser documentadas, processadas e monitoradas de acordo com os padrões comuns de segurança (i.e. ISO, NIST).

M. GESTÃO DE ATIVOS

O Terceiro deve manter um inventário de ativos, incluindo sistemas, dispositivos, hardwares e ativos de software quando possuir Informações pertencentes ou confiadas pela Baxter localizadas fora do ambiente desta e/ou quando possuir uma conexão de acesso remoto ao ambiente do Terceiro.

O Terceiro deve ter controles de descarte de ativos em vigor para garantir que as Informações (impressas e eletrônicas) sejam descartadas de acordo com padrões comuns de segurança (i.e., ISO, NIST) quando não forem mais necessárias, bem como deve manter evidências documentadas do descarte adequado, sem prejuízo das medidas e controles para apagamento e destruição das Informações armazenadas nestes ativos de acordo com essa Política de Segurança das Informações.

N. TRATAMENTO DE INFORMAÇÕES:

O Terceiro deve garantir a separação das Informações da Baxter das de outros clientes quando possuir Informações pertencentes ou confiadas pela Baxter localizadas fora do ambiente desta e/ou quando tiver uma conexão de acesso remoto ao ambiente da Baxter.

As comunicações entre a Baxter e o Terceiro (incluindo e-mail, transferência de arquivos, conectividade remota, pastas compartilhadas, etc.) devem ser protegidas usando os serviços fornecidos pela Baxter.

Processos e ferramentas devem ser usados para evitar, detectar e responder à perda de Informações.

As Informações não devem ser armazenadas ou transferidas usando dispositivos de armazenamento removíveis sem a aprovação documentada do Diretor de Segurança das Informações, se tal procedimento for permitido pelas normas de segurança da informação. Sendo tal procedimento autorizado, se tais dispositivos forem usados, todas as informações neles armazenadas devem ser criptografadas.

O. REFERÊNCIAS E DOCUMENTOS ASSOCIADOS

Esta Política deve ser lida em conjunto com outras políticas e recursos corporativos que estabelecem as expectativas da Baxter referentes ao comportamento de conselheiros, diretores, funcionários, agentes e contratados. Essas políticas incluem o seguinte:

- Código de Conduta da Baxter
- Política Global de Privacidade
- Política Global de Proteção de Informações
- LGPD
- Sharepointlink:https://worksites.baxter.com/sites/LGPD_Brasil/Documentos%20Compartilhados/Forms/AllItems.aspx.

P. ANEXOS

N/A

Q. ALTERAÇÃO DE HISTÓRICO

VERSÃO	ALTERAÇÃO	DATA(s)