| Assunto: | Funcionários afetados: | Política nº | Rev. |
|---|---|---|---|
| SEGURANÇA DA INFORMAÇÃO | TODOS | HREW | 2 |

## FINALIDADE

A finalidade desta política é estabelecer e comunicar aos funcionários o direcionamento geral das iniciativas de segurança da informação na Cleveland Clinic, no que concerne à proteção de todas as informações confidenciais, privadas e restritas de acesso não autorizado (seja intencional ou acidental), divulgação, modificação ou destruição, independentemente do formato (papel, eletrônico/digital, etc.). Esta política é suplementada por políticas, normas, procedimentos e diretrizes encontrados no Manual de Segurança e Privacidade On-line da Cleveland Clinic e em publicações, lembretes e/ou manuais departamentais de Segurança da Informação e Privacidade da Cleveland Clinic.

Todas as políticas, normas e procedimentos da Segurança da Informação são regidos por regulamentos/leis federais/estaduais, obrigação contratual, agências terceirizadas ou fazem parte de uma abordagem com boas práticas do setor no que diz respeito à segurança da informação.

## POLÍTICA

Esta política de Segurança da Informação aplica-se a todos os computadores, sistemas de rede e informações eletrônicas de propriedade e/ou administradas pela Cleveland e/ou todos os sistemas de computador conectados a redes da Cleveland Clinic. Similarmente, esta política aplica-se a todas as plataformas (sistemas operacionais), todos os tamanhos de computador (computadores portáteis usando um computador principal) e sistemas de software (sejam desenvolvidos dentro da empresa ou adquiridos de terceiros). A política aborda informações tratadas por computadores e/ou rede de computadores. Apesar de este documento incluir voz e papel, ele não trata diretamente da segurança da informação nesses formatos. Para informações sobre a proteção de informações no formato de papel, consulte a política 905 Classificação de Sistemas e Informações.

## FUNÇÕES E RESPONSABILIDADES

**Funções dos usuários**: todas as informações eletrônicas ou em papel que são armazenadas ou transmitidas por meio dos sistemas de computador da Cleveland Clinic são de propriedade da Cleveland Clinic e devem ser protegidas contra acesso não autorizado, divulgação, concessão ou destruição. Todas as pessoas associadas à Cleveland Clinic, independentemente do status (médico, funcionário, prestador de serviço, consultor, funcionário temporário, parceiro de negócios, voluntário, etc.), que tiverem contato com informações ou sistemas de informação da Cleveland Clinic, devem cumprir as políticas de Segurança da Informação encontradas neste documento e políticas, normas, procedimentos e diretrizes relacionadas à Privacidade e/ou Segurança da Informação.

**Funções dos departamentos**: Cada departamento da Cleveland Clinic é responsável por implementar esta política e políticas relacionadas usando processos, normas e diretrizes estabelecidos pelo Departamento de Segurança da Informação da Cleveland Clinic.
As responsabilidades incluem:

- Manter registros dos cumprimentos da segurança da informação e das áreas que precisam melhorar;

- Auxiliar na identificação, classificação e proteção de informações confidenciais e restritas.
- Estabelecer processos para orientar, treinar e atualizar os funcionários departamentais sobre os requisitos desta política e de políticas relacionadas
- Fornecer informações a respeito de segurança da informação, confidencialidade e violações de privacidade dentro do departamento para os Departamentos de Privacidade e Segurança da Cleveland Clinic

**Função do Departamento de Segurança da Informação**

O Departamento de Segurança da Informação da Cleveland Clinic ("O Departamento") é responsável por estabelecer e manter políticas, normas, procedimentos e diretrizes de segurança da informação em toda a empresa. O Departamento fornece o direcionamento e a experiência técnica para oferecer garantia razoável de que as informações da Cleveland Clinic estão protegidas adequadamente.

O Departamento age como uma conexão entre todos os departamentos, divisões e institutos da Cleveland Clinic para assuntos de segurança da informação e é ponto focal de todas as atividades concernentes à segurança da informação na Cleveland Clinic. O Departamento realiza avaliações de riscos, prepara planos de ação, avalia produtos de fornecedor, participa em projetos de desenvolvimento, auxilia na implementação de controle, coordena atividades de Recuperação de Desastres de TI e investiga as violações de segurança da informação.

Todas as questões e/ou problemas da segurança da informação devem ser direcionados para o Departamento da Segurança da Informação. O uso de consultores externos, equipes externas de respostas à segurança de computadores ou outros profissionais externos é estritamente proibido, a menos que isso seja aprovado pelo Departamento.

**Coordenação de Atividades Descentralizadas**

A Administração da Segurança na Cleveland Clinic é um esforço tanto centralizado quanto descentralizado; dependendo do site, da plataforma e/ou do aplicativo, a responsabilidade pela administração da segurança pode ser centralizada, descentralizada ou ambas. Espera-se que os indivíduos e/ou grupos responsáveis pela administração ou suporte descentralizado do(s) sistema(s) ou aplicativo(s) de um computador trabalhem em colaboração com o Departamento de Segurança da Informação para a finalidade de alinhamento de políticas, normas, procedimentos e diretrizes, além do aprimoramento dos níveis de segurança e privacidade.

**CLÁUSULAS GERAIS**

**Princípio da Segurança da Informação**

A informação é um ativo que, como outros ativos comerciais importantes, tem valor para uma organização e deve ser protegido de forma adequada. A Segurança da Informação protege informações de uma ampla variedade de ameaças para que seja possível impedir violações

de regulamentos de paciente, garantir continuidade do negócio, minimizar danos comerciais e maximizar o retorno sobre o investimento e as oportunidades de negócio. As informações, incluindo, mas não se limitando a, dados impressos, escritos, eletrônicos, em vídeo e em áudio, só devem ser compartilhadas, armazenadas e protegidas pelo uso dos meios de proteção adequados.

**Meios de Proteção Razoáveis e Adequados**

A Segurança da Informação é alcançada pela implementação de um conjunto razoável e adequado de controles administrativos, físicos e técnicos, que inclui políticas, práticas, procedimentos, estruturas organizacionais, funções de software e mais. Esses controles são estabelecidos para garantir que os objetivos de segurança específicos da organização sejam alcançados.

**Propriedade das Informações e Direitos de Acesso**

Todos os aplicativos e informações de computadores são desenvolvidos por unidades de trabalho designadas pela Cleveland Clinic.
As unidades de trabalho da Cleveland Clinic (p. ex: seção, departamento, divisão e instituto) são “Proprietários de Dados” para todos os aplicativos e informações de computador que são desenvolvidos para suas unidades. Os Proprietários de Dados são responsáveis por assegurar a integridade das informações e determinar quem é autorizado a acessar os dados. As unidades podem atribuir funcionários específicos para trabalharem como Proprietários de Dados.

**Gerenciamento de Informações**

O cuidado e a proteção (“Gerenciamento”) de todas as Informações da Cleveland Clinic são de responsabilidade do funcionário ou da pessoa autorizada que possuir ou estiver usando as informações em um dado momento. Independentemente de quem é o Proprietário de Dados ou dos meios pelos quais as informações foram obtidas (download, upload, acesso normal on-line, etc.), o usuário ou portador das Informações da Cleveland Clinic é pessoalmente responsável pela segurança delas, de acordo com esta política.

**Classificação das Informações**

Para dar suporte ao princípio de acesso das informações na base do “precisa saber”, a Cleveland segue um sistema de classificação de informações. Esse sistema de classificação existe não apenas para proteger informações que são críticas para os pacientes e a Cleveland Clinic, mas, também, para ajudar a determinar “quem” pode ter acesso a “quais” dados dentro da estrutura da Cleveland Clinic. Para obter mais informações, consulte a Política de Classificação de Dados 801CCHS.

**Controles de Acesso Obrigatórios**

Os controles de acesso a seguir devem ser aplicados a cada computador e sistema de computação da Cleveland Clinic.

- **Somente usuários autorizados** — todos os PCSs não públicos estão reservados para

acesso somente pelos usuários autorizados da Cleveland Clinic. O uso não autorizado é estritamente proibido.

- **Identificação e autenticação** — todos os usuários devem ter uma ID exclusiva de usuário e senhas para ganhar acesso a redes, sistemas e/ou aplicativos da Cleveland Clinic
- **IDs e senhas seguras de usuário** — as IDs e senhas de usuário devem ser mantidas em sigilo e de conhecimento apenas pelo usuário; as senhas devem ser mantidas em sigilo e de conhecimento apenas pelo usuário; as senhas devem ter um comprimento significativo e serem difíceis de adivinhar.
- **Administração da conta** — apenas funcionários autorizados com responsabilidade de segurança podem ter a função de atribuir e manter contas de login e privilégios associados.
- **Acesso privilegiado** — o acesso privilegiado, de alto nível, como “raiz”, “superusuário” ou “administrador” é reservado estritamente para administradores de sistemas.
- **Acesso por não funcionários da Cleveland Clinic** — prestadores de serviço, consultores, fornecedores, etc. devem assinar um Contrato de Não Divulgação e devem ter o acesso autorizado adequadamente pela administração da Cleveland Clinic.
- **Acesso remoto** — o acesso remoto será concedido a funcionários e outras pessoas com uma necessidade comercial válida, após autorização apropriada. Até o limite possível, o acesso será concedido apenas aos recursos necessários. Todos os usuários remotos seguirão todos os procedimentos e políticas de acesso remoto.
- **Computadores desacompanhados** — todas as estações de trabalho localizadas em áreas de acesso público, ou que contenham dados confidenciais, devem ser configurados para fazer logoff automático após um período de tempo razoável e pré-determinado (uma proteção de tela autorizada é uma alternativa aceitável).
- **Computadores não autorizados** — computadores de propriedade privada trazidos para as instalações da Cleveland Clinic devem seguir as políticas de uso e conectividade da Cleveland Clinic. Todos esses computadores devem ter os mesmos níveis de controles técnicos instalados (configurações, gerenciamento de patch e antivírus).
- **Conexões fora da rede (modem ou sem fio)** — conexões diretas a computadores da Cleveland Clinic por conexões sem fio ou modems que contornam a conectividade e a segurança da rede são proibidas.
- **Rede com fio ou sem fio** — a instalação de pontos de acesso e sistemas sem fio nas instalações da Cleveland Clinic sem autorização adequada é estritamente proibida. O uso não autorizado de pontos de acesso sem fio e sistemas sem fio para transpor ou compartilhar redes da Cleveland Clinic também é estritamente proibido.

**Conformidade de Fornecedor**

Os funcionários da Cleveland Clinic devem realizar esforços razoáveis para informar os

fornecedores sobre esta política de Segurança da Informação da Cleveland Clinic e exigir que eles cumpram todos os procedimentos e políticas que englobam a Segurança da Informação da Cleveland Clinic.

**Segurança da Informação Considerada em Avaliações de Desempenho de Funcionários**

A conformidade com os procedimentos e as políticas de segurança da informação é uma consideração feita em todas as avaliações pertinentes de desempenho de funcionários (Avaliação de Nova Contratação, Avaliação de Meio do Ano, Avaliação Anual de Desempenho).

**Monitoramento, Investigação e Ação Disciplinar**

O monitoramento de conformidade será realizado periodicamente para fornecer garantias razoáveis de que as unidades organizacionais estejam operando de maneira consistente com os requisitos definidos nesta e em outras políticas relacionadas à segurança da informação. Aquisição, divulgação ou discussão não autorizada de informações relacionadas a atividades comerciais da Cleveland Clinic, informações médicas de pacientes, funcionários atuais ou antigos e candidatos a uma vaga. Todos os atos maliciosos que destroem ou comprometem qualquer tipo de dados é um assunto sério que levará a uma ação corretiva, podendo incluir demissão e possíveis imputações criminais. As questões disciplinares resultantes dos requisitos da segurança da informação serão tratadas pelos gerentes que trabalham em conjunto com o Recursos Humanos.

**Informações de Contato**

Todas as questões e preocupações relacionadas à segurança da informação da Cleveland Clinic devem ser direcionadas a um dos seguintes:

- Diretor do Departamento de Segurança da Informação da Cleveland Clinic: 216-738-4307
- Gerente do Departamento de Segurança da Cleveland Clinic: 216-738-4320
- Assistência Técnica de TI da Cleveland Clinic: 216-738-4357

**DEPARTAMENTO DE EMISSÃO**

Departamento de Segurança da Informação e Relações com Funcionários, Recursos Humanos

**REFERÊNCIAS DA POLÍTICA**

Ação corretiva
Segurança da Informação Geral — 900
Classificação de Sistemas e Informações — 905
Controle de Acesso — 925
Informações Aceitáveis de Uso — 935

| Assunto: | Funcionários afetados: | Política nº | Rev. |
|---|---|---|---|
| SEGURANÇA DA INFORMAÇÃO | TODOS | HREW | 2 |

**CITAÇÕES**

- 45 CFR Section 142.308(a)(10)
- 45 CFR Section 142.3088(a)(7)
- 45 CFR Section 142.308(a)(12)