DMF MEDICAL

OPERANDO SOLUÇÕES

Política de Segurança da Informação (ISO 27001) e Privacidade de Dados(LGPD)

Abril / 2023

OBJETIVO

Estabelecer diretrizes para estruturar um sistema normativo e de práticas de Proteção de Dados Pessoais e Sensíveis, visando garantir a privacidade e proteção dos dados de terceiros que a Medic® ofereça tratamento.

ABRANGÊNCIA

A privacidade de dados é de extrema relevância para a Medic®, de forma que desenvolvemos essa política para demonstrarmos todas nossas práticas para o Tratamento e Proteção de Dados Pessoais.
É missão da Medic® cumprir o estipulado nesta Política, bem como, na Lei Geral de Proteção de Dados e demais instrumentos legais ou infralegais relacionados ao tema, garantindo a adequada proteção a Dados Pessoais.
A Medic® compromete-se a divulgar em seu sítio eletrônico a versão mais recente deste documento e comunicar aos colaboradores, prestadores de serviços e parceiros.

CONCEITOS

Os termos e expressões a seguir, quando escritos em letras maiúsculas, deverão ter os seguintes significados, conforme definido abaixo:

DPO (“Data Protection Officer”): pessoa que na Medic® é o responsável por coordenar e por assegurar a conformidade com a Política de Proteção de Dados e requisitos legais/ regulamentares locais aplicáveis, também, atuará como o canal com os Titulares dos Dados e a Autoridade Nacional de Proteção de Dados.

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem decisões referentes ao tratamento de dados pessoais ou sensíveis.

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais ou sensíveis em nome do Controlador.

Autoridade Nacional de Proteção de Dados ou ANPD: autoridade administrativa encarregada da Proteção de Dados Pessoais é um órgão da administração pública nacional responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados em todo o território brasileiro.

Titular dos Dados: qualquer pessoa natural que possa ser identificada, direta ou indiretamente, através de meios que provavelmente serão usados por qualquer pessoa física ou jurídica, em particular em relação a um número de identificação, dados de localização, identificador online ou um ou mais fatores específicos da identidade física. Pode ser por exemplo, um cliente, um funcionário, um fornecedor.

Dados Pessoais: quaisquer dados relacionados a um indivíduo (pessoa natural) que é ou possa ser identificada a partir dos dados em conjunto com outras informações, inclusive dados eletrônicos e virtuais.

Dados Sensíveis: os dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Tratamento: qualquer ação tomada tendo por base dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Acesso – Ato de ingressar, transitar, conhecer ou consultar a informação, seja local, ou remotamente, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade. Ativos de Informação – Os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso.

Credenciais ou Contas de Acesso – Identificações concedidas após o processo de credenciamento de acesso, que permitam habilitar determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão, credencial biométrica ou lógica como identificação de usuário e senha.

LGPD: Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709 de 14 de agosto de 2018.

POLÍTICA DE TRATAMENTO DE DADOS

Como Operador atuando em nome de Controladores, a Medic® garantirá que os dados recebidos serão tratados e mantidos em sigilo e utilizados apenas para o propósito específico de sua captação.

A coleta e o tratamento de Dados Pessoais ou Sensíveis pela Medic® são feitos usualmente para a execução de um contrato ou para o cumprimento de uma obrigação legal à qual estejamos sujeitos, respeitando a informação mínima necessária a cada finalidade.

A Medic® poderá divulgar os Dados Pessoais nas situações exigidas para a execução do contrato, sempre dentro dos limites exigidos e autorizados pela Lei.

Nas hipóteses de compartilhamento de Dados Pessoais com terceiros a Medic® se responsabiliza pelo uso dos Dados Pessoais de maneira consistente e de acordo com os propósitos para os quais foram coletados e sempre de acordo com esta Política.

Quando necessário em decorrência de obrigação legal, determinação de autoridade competente, ou decisão judicial, nos limites da respectiva decisão, a Medic® cientificará os Controladores ou os proprietários dos Dados Pessoais ou Sensíveis, quando for o caso, sobre as eventuais demandas legais que resultem na divulgação de informações pessoais, exceto se tal cientificação seja vedada por lei ou proibida por mandado judicial.

Mantemos os Dados Pessoais ou Sensíveis pelo tempo necessário para as finalidades para as quais são tratados ou até a respectiva solicitação de exclusão, a qual será atendida nos termos solicitados, desde que, não infrinja quaisquer preceitos legais, ordens judiciais ou sejam necessários para resolver disputas, manter a segurança, evitar fraudes e abuso e garantir o cumprimento de contratos.

No caso de transferência internacional dos Dados Pessoais ou Sensíveis, a Medic® buscará o consentimento específico do Titular dos Dados ou do Controlador para a respectiva transferência.

No caso de Tratamento de Dados de menores de idade, a Medic® buscará o consentimento específico de pelo menos um dos pais ou pelo responsável legal, sendo certo que, realizará todos os esforços razoáveis para verificar que o consentimento foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.

O tratamento de Dados Pessoais Sensíveis, quando o for caso, somente poderá ocorrer quando o Controlador, titular ou seu responsável legal consentir, de forma específica, desde que, destacadas também as finalidades específicas.

POLÍTICA DE RH

Na inclusão de candidato, colaborador ou prestador de serviço assim como no seu desligamento ou término das atividades, as informações pertinentes a ele serão excluídas ou mantidas de acordo com a regra da necessidade mínima mantendo-se assim somente informações necessárias para cumprimento da legislação vigente e do contrato de trabalho.

A cada inclusão ou alteração de colaborador ou prestador de serviços, os direitos de acesso são determinados pela gerência; inclusive os acessos físicos; com ajustes executados até um prazo máximo de 24 horas. Ao desligamento, encerramentos das atividades ou falta de necessidade de acesso, os direitos de acessos serão excluídos.

POLÍTICA DE ATUALIZAÇÕES

A Política de Proteção de Dados Pessoais será revisada e atualizada ao menos uma vez por ano, ou sempre que se fizer necessário.
A cada atualização ou revisão, serão comunicados: colaboradores, prestadores de serviços e parceiros.

POLÍTICA DE CONTROLE DE ACESSO

Todo o controle de acesso aos ativos de informações da Medic® é controlado através de credenciais únicas, seja no ambiente Google®, VIMAN® (Sistema de Gestão OPME) ou dependências da empresa.

Frequentemente as senhas de acesso são atualizadas e os níveis de acesso são revistos, por medida de segurança.

Toda inclusão, alteração, ou exclusão de acesso é feita mediante uma solicitação da gerência ou processo automático de exclusão após desligamento da empresa ou falta de necessidade em mantê-las, obedecendo assim o conceito de mínima necessidade.

O acesso físico à empresa é realizado por biometria.

POLÍTICA DE MESA LIMPA E TELA LIMPA

A política de mesa limpa e tela limpa se trata de garantir que informações confidenciais, tanto em formato digital quanto físico, e dispositivos eletrônicos não fiquem desprotegidos em espaços de trabalho quando não estão sendo utilizados. É uma estratégia importante para reduzir riscos de violações de segurança. Algumas práticas simples incluem o uso de armários com trancas para armazenar documentos e dispositivos, proteger as telas dos computadores de olhares curiosos, configurar proteção por senha e desligar os dispositivos ao final do dia. Restrições no uso de equipamentos de cópia e impressão também são recomendadas, assim como a adoção de uma cultura de uso mínimo de papel e o descarte adequado de informações após reuniões.

POLÍTICA DE EXCLUSÕES

A exclusão de dados é realizada sempre que o mesmo não se fizer necessário, seja para o cumprimento de um contrato ou serviço, ou até mesmo disposições legais; seguindo a tabela de prazos de exclusões abaixo:

Prazos de Eliminação dos dados tratados:

PERMANENTE	• Histórico Empresarial de Carteira de Clientes (ativo empresarial); • Rastreabilidade de produtos (vida útil destes).

10 ANOS (de acordo o Art. 205 do Código Civil)	• Dados pessoais de representantes legais de empresas que assinam um contrato com a Medic®; • Dados de Due Diligence (se os auditados assinam contrato com a empresa); • Dados de Contratos de Proctor e Patrocínio de Eventos da saúde; • Dados de Cotações de Valores e Análise Prévia de Procedimentos (se o procedimento é aprovado); • Dados de Faturamento dos Produtos médicos implantados.
7 ANOS (de acordo com o Art. 7° Inciso XXIX da Constituição Federal)	• Dados de colaboradores para cumprimento de obrigações legais, incluindo exames admissionais e dados de benefícios (Planos de Saúde, VR, VT, Contabilidade).
5 ANOS (de acordo com o Art. 150 § 4º do Código Tributário Nacional)	• Dados enviados em Despachos Aduaneiros; • Dados de Notificações de Compra e Venda de Produtos Médicos (Importação e Exportação).
3 ANOS (de acordo o Art. 206, §3°, Inciso V do Código Civil)	• Dados de Due Diligence (se os auditados não assinam contrato com a empresa); • Dados para resguardar a empresa em uma eventual reparação civil; • Dados de Cotações de Valores e Análise Prévia de Procedimentos (se o procedimento não é aprovado).

6 MESES*	• Dados de Currículos e Fichas de Emprego.
30 DIAS*	• Imagens de câmeras de segurança.

LEMBRANDO QUE TODOS OS PRAZOS CONTRATUAIS CONTAM APÓS O TÉRMINO DA RELAÇÃO CONTRATUAL ou a OCORRÊNCIA DO FATO GERADOR, COM EXCEÇÃO DOS ITENS DESTACADOS.

***Prazo contado do recolhimento**

POLÍTICA DE GESTÃO DE BACKUPS

Todos os ativos de informações da Medic® possuem backups realizados periodicamente, seja em ambiente interno ou externo à empresa, garantindo a redundância de armazenamento e segurança das informações.

Os dados pessoais e sensíveis são armazenados e tratados em apenas dois ambientes: GOOGLE DRIVE (arquivos) e VIMAN (sistema de gestão OPME).

Em ambos os casos a Medic® detém contrato de adesão que abrange todos os quesitos de segurança da informação, garantia de operabilidade, backups, monitoramentos de vulnerabilidade e outros aspectos tecnológicos.

A Medic® não possui informações pessoais ou sensíveis armazenadas localmente.

POLÍTICA DE CRIPTOGRAFIA

A Medic® não armazena informações pessoais ou sensíveis localmente.

Todos os arquivos digitais são armazenados e tratados no Google Drive e VIMAN.

No Google Drive a criptografia é por responsabilidade do próprio Google, e no VIMAN o banco de dados é criptografado e nativo do sistema, sendo possível o acesso somente através do próprio sistema.

POLÍTICA DE SEGURANÇA DE REDE

A Medic® não armazena informações pessoais ou sensíveis localmente.

Todos os arquivos são armazenados e tratados no Google Drive e VIMAN, os quais são responsáveis por toda a segurança da rede.

A rede sem fio corporativa é liberada somente para pessoas predeterminadas pelo RH e com aprovação da gerência.

Uma rede sem fio isolada é utilizada para visitantes, não oferecendo riscos à rede interna.

Em ambos os casos, os acessos não oferecem riscos às informações sensíveis ou pessoais visto que são todos armazenados em ambientes externos à Medic® (Google Drive e VIMAN).

POLÍTICA DE SENHAS

Todas as senhas utilizadas na Medic® ou em ambiente externo contendo informações pessoais ou sensíveis devem obedecer ao critério de senha forte: conter ao menos um caractere maiúsculo, minúsculo e especial, possuindo letras e números, bem como ter um tamanho mínimo de 8 dígitos.

Todas as senhas devem ser atualizadas a cada 3 meses ou antes, se necessário.

POLÍTICA DE VULNERABILIDADES

A Medic® não armazena informações pessoais ou sensíveis localmente.

Todos os arquivos são armazenados e tratados no Google Drive e VIMAN, onde os mesmos são responsáveis por toda a tratativa de vulnerabilidades.

Mesmo não havendo necessidade de firewall, pela inexistência de servidores ou redes internas que tratam ou armazenam dados sensíveis ou pessoais, ainda sim utilizamos o Firewall e Antivírus da própria Microsoft, que já está incluso no Windows.

Mensalmente executamos uma varredura completa nos computadores locais, utilizando as ferramentas do Windows Defender, mesmo sem a necessidade

premente, visto que todos os dados privados ou sensíveis se encontram em nuvens, totalmente isolados do ambiente local.

POLÍTICA DE ACESSO REMOTO

O acesso remoto, acesso à rede sem fio corporativa, bem como acesso físico a informações é predeterminado ou alterado pelo RH, com aprovação da gerência; sendo executada a liberação pela informática ou administrativo.

Para utilização de tecnologias, serão permitidos somente equipamentos corporativos.

O acesso remoto ao VIMAN passa por 3 níveis de senhas diferentes, até ser possível visualizar ou tratar alguma informação pessoal ou sensível. O acesso ao Google Drive utiliza a autenticação de MFA também.

POLÍTICA DE AVALIAÇÃO DE IMPACTO

Na contratação de sistemas, aquisição de hardwares ou alterações de processos o Comitê de LGPD participa da avaliação.

O Comitê de LGPD tem por finalidade garantir que os requisitos de privacidade estabelecidos na Política de Proteção de Dados Pessoais sejam considerados e relatados ao projetar ou atualizar sistemas, softwares, hardwares ou processos de negócios, nos casos em que a empresa atua como controlador.

POLÍTICA DE INFORMÁTICA

Todas as bases de dados da Medic® estão armazenadas em ambiente de terceiros, devidamente de acordo com a legislação de dados vigente.

A Medic® e seus terceiros utilizam-se de vários procedimentos internos para minimizar os riscos em relação às informações, como: regras de senhas fortes, Controle de acesso, Confidencialidade, Backup, uso de e-mail criptografado, Ferramentas antimalware, filtro antispam, antiphishing e o uso de Firewall.

Estas ações permitem a proteção da confidencialidade, segurança e integridade de seus Dados Pessoais e Sensíveis, prevenindo a ocorrência de eventuais danos em virtude do tratamento desses dados.

Nesse sentido, mapeamos constantemente possíveis riscos à segurança da informação e, com base nesse mapeamento, implantamos as melhores ferramentas de controle visando mitigar riscos de quaisquer violações, todavia, em se tratando de ambiente digital, não estamos imunes a eventuais contratempos.

Por medidas de segurança, a entrada na empresa com mídias removíveis é expressamente proibida, salvo em situações pontuais liberadas pela gerência e acompanhadas pela T.I.

Todo descarte de mídia será feito de forma segura, executando uma limpeza profunda ou destruindo de forma que informações não sejam acessíveis ou recuperáveis.

Para utilização de tecnologias, serão permitidos somente equipamentos corporativos.

POLÍTICA DE GESTÃO DE PATCHES

Todos os equipamentos internos são mantidos atualizados por nossa T.I. de acordo com as últimas versões estáveis disponibilizadas pelos fornecedores de softwares e hardwares. Os equipamentos externos são mantidos atualizados por terceiros.

Todos os softwares com possibilidade de se manter atualizações e instalações automáticas, de acordo com a disponibilidade do fornecedor, são mantidos dessa forma.

Os demais são atualizados manualmente, com buscas quinzenais por novas atualizações.

POLÍTICA DE GESTÃO DE INCIDENTES

A qualquer incidente, um chamado é aberto para o departamento de T.I. realizar toda a análise, ação corretiva e ação preventiva para não ocorrência novamente.

POLÍTICA DE GESTÃO DE PRIVACIDADE

Todos os questionamentos, reclamações, pedidos e demandas relacionados a dados armazenados pela Medic® terão um processo interno documentado.

As respostas e tratativas de solicitações de direitos individuais serão efetuadas por escrito pelo responsável da área.

O princípio básico da política de privacidade da Medic® é a de tratar dados com o mínimo necessário à finalidade.

SEGURANÇA DE INFORMAÇÕES PESSOAIS

Todos os Dados Pessoais ou Sensíveis serão guardados em bases de dados da Medic®, as quais estão devidamente de acordo com a legislação de dados vigente.

A Medic® e seus fornecedores utilizam vários procedimentos de segurança, para mitigar riscos com base nas seguintes ações internas: Política de senhas, Controle de acesso, Confidencialidade, Backup, Uso de e-mail, Ferramentas antimalware, filtro antispam, antiphishing e o uso de Firewall.
Estas ações permitem a proteção da confidencialidade, segurança e integridade dos Dados Pessoais e Sensíveis, prevenindo a ocorrência de eventuais danos em virtude do tratamento desses dados.

Nesse sentido, mapeamos periodicamente possíveis riscos à segurança da informação bem como seus fluxos e, com base nesse mapeamento, implantamos e comunicamos aos colaboradores, prestadores de serviços e consultores as melhores ferramentas de controle visando mitigar riscos de quaisquer violações, todavia, em se tratando de ambiente digital, não estamos imunes a eventuais contratempos.

GOVERNANÇA DE DADOS

A gerência é responsável por editar e atualizar esta Política, indicar o Data Protection Officer (“D.P.O”), o controlador e o operador de todo o Tratamento de Dados, os quais, em conjunto, estão preparados para dar solução a quaisquer desvios relacionados ao tema.

A Medic® está sujeita à legislação pertinente ao tema de Proteção de Dados, bem como, possui o consentimento (colhido de forma expressa e inequívoca no Termo

de Consentimento) para o Tratamento e consequente proteção dos Dados, nos casos em que a Medic® atuar na condição de Controlador.

O Titular dos Dados poderá, mediante solicitação, obter informações sobre todos os seus Dados Pessoais ou Sensíveis armazenados, poderá recebê-los, examiná-los e, se necessário, alterá-los ou apagá-los, sempre nos casos em que a Medic® atuar na condição de Controlador.

Para tanto, basta enviar um e-mail para o endereço lgpd@medic.com.br e estes pedidos serão considerados de acordo com as leis aplicáveis.

Na hipótese de solicitação para apagar as informações, essa somente será proferida nos exatos limites da lei, ou seja, apenas quando os dados forem desnecessários, excessivos ou tratados em desconformidade com a lei.

POLÍTICA DE TREINAMENTOS

A Medic® irá implementar programas de treinamento sobre proteção de Dados Pessoais e Sensíveis aos seus colaboradores, seguindo os princípios contidos nesta Política de Proteção de Dados Pessoais, determinando inclusive:
i) treinamentos sobre Política da Proteção de Dados Pessoais serão realizados trimestralmente na Medic®, de forma presencial e remota; com início em Junho/2021.
ii) o treinamento aos colaboradores ou prestadores recém contratados serão realizados como parte do processo de integração;
iii) treinamentos de conscientização trimestral especialmente dirigidos aos colaboradores.

AÇÕES PARA IMPLANTAÇÃO

Será criado um Comitê multidisciplinar de Privacidade com colaboradores da empresa que será responsável pela implementação das diretrizes e obrigações fixadas nesta Política e na LGPD.

O Comitê estará igualmente incumbido de desenvolver programas de conformidade e controles de forma a prevenir, detectar, monitorar e abordar violações em potencial, os quais serão submetidos à aprovação do DPO e, respeitando as diretrizes de Governança de Dados, deverão ser aprovados pela Diretoria.

DOCUMENTOS ASSOCIADOS

Documentos de normas e procedimento internos sobre:

- Anexo I - Termo de Consentimento para tratamento de Dados Documentos e Normas externas:
- NBR ISO/IEC 27002:2013 - Código de prática para controles de segurança da informação;
- Lei Geral de Proteção de Dados – Lei 13.709/18
- European General Data Protection Regulation – EU-GDPR
- Política de Segurança da Informação da Medic®.

Elaboração	Revisão	Aprovação
Compliance, Controles Internos, Jurídico, Tecnologia da Informação	V00	Comitê de Auditoria, Gestão do Risco, Compliance e de Recursos Humanos Conselho de Administração

TERMO DE CONSENTIMENTO PARA TRATAMENTO DE DADOS

Este documento visa registrar a manifestação livre, informada e inequívoca pela qual o Titular dos Dados concorda com as diretrizes da Política de Proteção de Dados Pessoais do Grupo Medic®, bem como, com o tratamento de seus Dados pessoais para finalidade específica de (*):

( ) cadastro de colaborador;

( ) cadastro de candidato a emprego;

( ) cadastro de pessoas com acesso às instalações da empresa;

( ) cadastro de fornecedor e relacionamento comercial;

( ) cadastro de cliente e relacionamento comercial;

_____

em conformidade com a Lei nº 13.709 – Lei Geral de Proteção de Dados Pessoais (LGPD).

Ao manifestar sua aceitação para com o presente termo, o Titular dos Dados consente e concorda que a Medic® tome decisões referentes ao tratamento de seus dados pessoais ou sensíveis, dados necessários ao usufruto de serviços e produtos ofertados pela Medic®, bem como realize o tratamento de tais dados, envolvendo operações como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Local/data:_____

Nome:

CPF:

_____

Assinatura

(*) Marque somente uma opção

TERMO DE COMPROMISSO

Eu,_____,
inscrito no CPF sob o nº_____, portador do RG nº_____ ,
declaro que obtive acesso a Política de Proteção de Dados Pessoais da Medic®, versão _____ disponibilizada no sítio www.medic.com.br, e estou ciente de todos os seus termos, com os quais tenho total concordância e me comprometo a cumpri-los durante a minha prestação de serviços.

Declaro estar ciente de que eventual violação de minha parte a qualquer regra estabelecida nesta política, sem prejuízo de eventuais sanções legais.

Por ser verdade, assino o presente termo.

Local/data:

_____

Assinatura

TERMO DE CONSCIENTIZAÇÃO - LGPD

Eu, _____, declaro ter recebido o Treinamento sobre a Lei Geral de Proteção de Dados Pessoais da empresa Medic® e fui orientado (a) sobre as diretrizes tomadas pela empresa no cumprimento das exigências discriminadas por esta lei.

Declaro também estar ciente das consequências da não observância deste regulamento, que podem acarretar situações de prejuízo para a empresa tanto no aspecto jurídico perante Terceiros, quanto na própria rotina interna de funcionamento da mesma.

Ribeirão Preto/SP, _____ de _____ de _____.

_____

Colaborador (a):