POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Visando a adequação dos procedimentos internos de tratamento de dados pessoais à Lei 13.979/2018, com a aplicação das melhores práticas de proteção e sigilo de dados, faz-se necessário a implantação de certas medidas de segurança da informação, a fim de garantir o armazenamento seguro dos dados pessoais dos beneficiários, pacientes, prestadores e funcionários do CÍRCULO OPERÁRIO CAXIENSE, visando proteger os dados pessoais contra a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizado, bem como contra qualquer forma de tratamento ilícito ou em desconformidade com a Lei Geral de Proteção de Dados Pessoais ou à Política de Proteção de Dados da Associação.

Esta Política de Privacidade aplica-se a todos os colaboradores e prestadores de serviço do Círculo Saúde e os termos aqui dispostos são aplicados no tratamento interno de dados da Associação e devem ser condizentes, no mesmo nível ou em nível superior, no que concerne à segurança de informação praticada nas empresas prestadoras de serviço, com as quais ocorre o compartilhamento de dados de controle do Círculo Saúde.

1. Definições iniciais

1.1 Esta Política tem por objetivo a orientação e divulgação para terceiros dos procedimentos de Segurança da Informação estabelecidos no tratamento interno de dados pessoais pelo Círculo Saúde, prevendo requisitos mínimos que devem ser também atendidos por empresas prestadores de serviço que receberem dados pessoais coletados pela instituição.

1.2 Para fins desta Política de Privacidade e Proteção de Dados, conceitua-se os seguintes termos:

"*LGPD*" significa a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados) que normatiza o tratamento de dados pessoais no Brasil;

"*Dados Pessoais*" significa qualquer informação pessoal relacionada ou relacionável a um Titular de Dados;

"*Titular*" ou "*Titular de dados*" significa o usuário, associado ou beneficiário, vinculado à plano de saúde do Círculo Saúde, seja ele dependente ou titular, que autoriza a concessão dos dados para operação nos limites estritos e especificados nesta política;

"*Dados Pessoais Sensíveis*" significam quaisquer 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;

"*Dados Compartilhados*" ou "*Informações Compartilhadas*" significa os Dados Pessoais que os controladores transferem entre si em decorrência da relação de credenciamento para execução de serviços relacionados ao plano de saúde que o titular de dados possui;

"*Controlador de Dados*" significa a pessoa a quem cabem as decisões relativas ao tratamento de dados pessoais dos titulares que venha a coletar e tratar;

"*Operador de Dados*" significa a pessoa que realiza a coleta e o tratamento de dados pessoais de seus usuários/clientes;

"*Tratamento de dados*" significa toda e qualquer operação realizada com dados pessoais, tais como a coleta, armazenamento, transmissão e eliminação de dados, dentre outros;

"*Violação de Dados*" significa qualquer violação de segurança ou sigilo que resulte na destruição acidental ou ilegal, dano, perda, alteração, divulgação não autorizada ou acesso aos Dados Pessoais do Titular transmitidos, armazenados ou de outra maneira Processados.

"*DPO*" ou "*Encarregado de Dados*" significa a pessoa que atua como canal de comunicação entre o Controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados, no que diz respeito ao tratamento de dados pessoais;

1.3 Os dados pessoais tornados anônimos - ou seja, os quais, por meio de técnicas confiáveis, perdem a associação com um indivíduo específico - não serão considerados dados pessoais;

1.4 Os termos desta Política visam assegurar a proteção efetiva em termos de segurança informática e cibernética dos dados pessoais referentes aos beneficiários, pacientes, funcionários e prestadores, armazenados em servidor interno do Círculo Saúde, portanto seus termos são de observação e implementação obrigatória, obrigando-se as empresas prestadoras de serviço a praticar nível de segurança compatível com o previsto nesta Política.

2. Proteção e Sigilo dos Dados Pessoais.

2.1 O Círculo Saúde e as empresas prestadoras de serviço asseguram estar adequadas ou em processo de adequação à Lei Geral de Proteção de Dados, no que concerne o tratamento interno de informações pessoais dos beneficiários, pacientes, funcionários e prestadores, incluindo, mas não se limitando, à designação de um encarregado de dados, implantação de termos de confidencialidade com os colaboradores, pactuação e aditivação de cláusulas de proteção e sigilo de dados compartilhados com terceiros, e adoção de planos resposta em caso de vazamento e acesso não autorizado ao banco de dados, conforme Política de Proteção de Dados da Instituição.

2.2 Além disso, o Círculo Saúde assegura que realizou a capacitação de sua equipe e do Encarregado de Dados, garantindo a preparação contínua de seus colaboradores para realizar tratamento de dados pessoais, atendendo os direitos dos titulares e os deveres para com a Autoridade Nacional de Proteção de Dados (ANPD), nos ditames da LGPD.

2.3 O Círculo Saúde, bem como as empresas prestadoras de serviço, deverá designar profissional responsável, em conjunto de esforços com o Encarregado de Dados (DPO), para tratar sobre a Segurança da Informação e implementar as ferramentas necessárias.

2.4 O Encarregado de Dados do Círculo Saúde é a MARTINS, ROBLEDO e BERNARDON - SOCIEDADE DE ADVOGADOS, ou MRB Advocacia Empresarial, que responde nos seguintes meios de contato: e-mail: <lgpd@mrbadv.com.br>; telefone (51) 3022-3431 ou (51) 3093-3690.

3. Restrição de acesso aos usuários

3.1 O Círculo Saúde assegura a restrição de acesso somente aos usuários que possuem permissão para acessar os dados coletados, realizando separação específica quanto a dados sensíveis, mediante a segregação das concessões de acesso por setores e a utilização de senhas para cada usuário.

3.2 As senhas adotadas, seja no computador pessoal ou no acesso de sistemas, são de uso pessoal e intransferível, devendo ser mantidas em sigilo, apenas de ciência do usuário, adotando política de senhas fortes, incluindo a sua troca obrigatória e periódica.

3.3 O e-mail e senha utilizados não podem ser utilizados em cadastros em sites de terceiros ou rede sociais se não vinculadas à atividade da Associação. Os acessos a estes sites e redes sociais, bem como a outros links de conteúdo impróprio, são restringidos no âmbito interno do Círculo Saúde.

3.4 Preferencialmente, será utilizada a autenticação multifator para o acesso de usuários administradores, que possuem acesso amplo e irrestrito de qualquer informação, especialmente aos dados sensíveis e financeiros.

4. Segurança nos computadores e softwares

4.1 É vedado o uso de softwares, sistemas operacionais ou ferramentas sem o devido licenciamento atualizado ou que viole direitos autorais.

4.2 A Controladora deverá possuir proteção contra softwares maliciosos *(anti-malware/anti-virus*), devidamente licenciado e atualizado, em todos os computadores que acessam dados pessoais, utilizando alertas sobre páginas da Web e softwares inseguros.

4.3 Também deve ser implementado *Firewall*, para barrar usuários e softwares maliciosos de servidores internos.

4.3.1 Conforme interesse e viabilidade, haverá a implantação de *Firewall de Borda*, para prevenir o acesso não autorizado e restringir/controlar o fluxo de tráfego entre redes com diferentes níveis de segurança, tais como a Internet e a rede interna.

4.4 Deve haver mecanismo de bloqueio de uso de dispositivos de armazenamento removíveis (tais como pendrive, cartões de memória, HD’s externos, dentre outros) nos computadores corporativos.

4.5 Também, deve haver aplicação de protocolo de comunicação seguro (criptografia) nos processos de comunicação, armazenamento e *backup* de bancos de dados, de modo a impedir o acesso não autorizado, vedado o uso de computadores particulares para acessar dados pessoais de controle do Círculo Saúde.

4.6 Além disso, deve haver processo de gestão de vulnerabilidades, incluindo a identificação e correção periódica de vulnerabilidades identificadas na proteção dos computadores, bem como de *patchs* em softwares que armazenam ou manipulam dados pessoais.

4.7 Deverá ser adotado padrões de desenvolvimento seguro de softwares, buscando a prevenção de falhas e proteção contra vulnerabilidades, ou extensão desta prática a terceiros quando aplicável.

4.8 Para acesso remoto em computadores fora do ambiente de trabalho, deve-se utilizar-se *VPN (Virtual Private Network*), incluindo mecanismos de acesso condicional bem como segurança na autenticação do usuário.

4.9 Os computadores devem ser mantidos em bloqueio quando não estiverem em uso, devendo ser aplicado o bloqueio automático de tela em caso de ausência do computador maior que 15 minutos, com o destravamento da tela mediante a inserção do usuário e senha. Ainda, sempre que o usuário sair do computador, deve ser efetuado o *log-out*.

4.10 Por fim, deve haver um Plano de Continuidade de Negócios, de modo a garantir a continuidade das operações em caso de indisponibilidade prolongada dos recursos que possibilitam o acesso aos dados pessoais.

5. Proteção do banco de dados

5.1 Não é permitido o armazenamento de dados pessoais coletados no Círculo Saúde em máquinas não autorizadas e de uso pessoal, incluindo a comunicação de dados por redes sociais

pessoais (*Whatsapp, Facebook, Telegram*, dentre outros), tampouco é permitido o transporte não autorizado da informação em mídia removível.

5.2 Todos os colaboradores devem estar cientes que são responsáveis pela proteção e segurança dos próprios computadores e aparelhos, devendo acessar sites impróprios e redes sociais somente caso estritamente necessário.

5.3 É proibida a gravação de áudio, vídeo, ou fotografia de documentos e telas de computador sem autorização expressa da respectiva liderança, gerência e/ou diretoria.

5.4 As informações contidas na base de dados do Círculo Saúde devem ser utilizadas somente para as finalidades contratadas, devidamente consentidas ou de cunho regulatório, proibida a sua utilização, divulgação ou cópia para fins diversos.

5.5 Deverá ocorrer o *backup* periódico de segurança do banco de dados da Instituição, a fim de evitar a destruição completa dos dados pessoais armazenados, o qual será de acesso único da gerência e/ou diretoria do Círculo Saúde.

6. Medidas de cautela

6.1 Deve ser utilizado o computador para anotações e lembretes, evitando-se o uso de papeis de anotação, os quais podem ser extraviados. No caso de anotação em papel, deve ser realizado o seu descarte assim que possível.

6.2 Deve haver implementação de filtro de mensagens maliciosas, todavia os colaboradores devem possuir cautela com e-mails suspeitos de *phishing*, solicitando informações ou contendo links para site externos. Por isso, na dúvida, não deve ser aberto e-mails, links ou anexos se houver dúvida sobre a fonte.

6.3 Em caso de suspeita de incidentes de segurança de informação, o operador de dados deve imediatamente comunicar aos responsáveis pela Segurança da Informação ou ao

Encarregado de Dados do Círculo Saúde, para ser adotado o protocolo de violação de dados. São exemplos de incidentes de violação de dados:

- Acessos ou tentativas de acesso não autorizados;
- Compartilhamento ou comprometimento de senha;
- Infecção de computador por código malicioso (*malware*);
- Vazamento de dados e informações pessoais;

7. Remoção segura dos dados

7.1 Após o término da finalidade para o armazenamento do dado, bem como do prazo legal para manutenção dos documentos para fins regulatórios, ressalvadas as hipóteses legais, deve haver a remoção segura dos dados pessoais armazenados em seus ambientes e equipamentos.

7.2 Tal remoção também deve ocorrer em caso de solicitação do titular de dados ou quando da solicitação do Círculo Saúde à uma de suas empresas prestadoras de serviço, adotando o respectivo protocolo de atendimento da demanda solicitada.

7.3 É possibilitada a manutenção dos dados para além do prazo legal somente mediante anonimização, para fins pessoais e de legítimo interesse do controlador.

7.4 A remoção segura mencionada neste tópico se refere ao descarte, de modo definitivo e irreversível, dos dados pessoais e de seus respectivos suportes documentais ou digitais, inclusive cópias ou *backups*, quando esgotada a finalidade de armazenamento, ou quando assim solicitado pelo titular. Em havendo dúvidas, poderá ser consultado o Encarregado de Dados, cláusula 2.4, a respeito da providência.

7.5 A Instituição deverá possuir protocolo de tempo de guarda dos documentos físicos que administra, de acordo com o respectivo prazo legal e obrigatório de armazenamento.

8. Protocolos de Segurança Física

8.1 Conforme necessidade e viabilidade, serão instaladas câmeras de monitoramento onde constam documentos físicos importantes e eventual datacenter, servidor interno, e/ou *backup* de arquivos.

8.2 Igualmente, deverão ser instalados dispositivos de detecção de incêndios, bem como termostato, para prevenir a ocorrência de incêndios e curtos-circuitos que ameacem os dados e documentos armazenados.

8.3 Nos arquivos físicos, os dados pessoais e documentos serão segregados por pastas e arquivos conforme o respectivo titular, de modo lógico e organizado.

8.4 Nos locais onde contenham dados pessoais de relevante sigilo, especialmente dados sensíveis, será controlado o seu acesso mediante concessão de chaves, com registro controlado de compartilhamento, cujo acesso somente será de pessoas autorizadas.

9. Disposições finais

8.1 O Círculo Saúde, para assegurar a proteção e sigilo dos dados, resguarda-se do direito de monitorar e registrar o acesso à rede, internet, sistemas e demais ambientes físicos e de computadores da Instituição ou por usuários que possam ser devidamente identificados.

8.2 A violação ou não observância das regras contidas nesta Política pode acarretar incidente de violação de dados, podendo ensejar sanções cabíveis ao respectivo infrator.

8.3 Este documento deve ser disponibilizado a todos operadores de dados do Círculo Saúde e às empresas terceiras prestadoras de serviço que tratem de dados pessoais da Instituição, para que se adequem aos termos aqui dispostos.

8.4 Quaisquer dúvidas ao conteúdo deste documento devem ser direcionadas para a área responsável pela segurança de informação ou o encarregado de dados do Círculo Saúde.