MANUAL DE GOVERNANÇA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Considerando que a **ATEAL- Associação Terapêutica de Estimulação Auditiva e Linguagem** se encontra profundamente comprometida com a Privacidade e Proteção de Dados Pessoais e, em implantação da LGPD.

Considerando que no curso de suas atividades diárias e operações a Entidade processa Dados Pessoais relacionados a seus funcionários, pacientes, parceiros, prestadores de serviços, contribuintes e fornecedores.

Considerando seus valores éticos relacionados à Privacidade e Proteção de Dados Pessoais, e plenamente consciente da importância do tema e dos riscos envolvidos em eventual violação de dados, a **ATEAL** assume o compromisso de proteger tais dados, motivo pelo qual implanta o presente Manual de Governança de Privacidade e Proteção de Dados Pessoais e o Anexo I – Política de Segurança da Informação e Anexo II – Política de Retenção e Descarte de Dados ("Manual").

1. MISSÃO, VISÃO E VALORES

A ATEAL define como pilares para a condução dos temas em relação à Privacidade e Proteção de Dados Pessoais as seguintes premissas:

Missão: Implementar de forma efetiva o presente Manual com a finalidade de garantir a Privacidade e a Proteção de Dados Pessoais de forma permanente.

Visão: Ser uma Entidade memorável aos funcionários, pacientes e parceiros tornando-se referência quanto às questões de implantação de boas práticas de Privacidade e Proteção de Dados Pessoais e Segurança da Informação no seu ramo de atuação.

Valores: Comportamento Ético, Segurança, Transparência, Respeito às pessoas, Excelência na prestação de serviços com foco em resultados positivos.

2. OBJETIVOS

Este Manual designa as orientações gerais para Privacidade e Proteção de Dados Pessoais dentro da **ATEAL** considerando que, para a execução de suas atividades coleta, manuseia e armazena informações que estão relacionadas a pessoas físicas ("Dados Pessoais"), com vistas a: I) estar em conformidade com as leis e regulamentações aplicáveis de proteção de Dados Pessoais e Privacidade e seguir as melhores práticas; II) proteger os direitos dos funcionários, pacientes, fornecedores, contribuintes e parceiros contra os riscos de violações de Privacidade e Dados Pessoais; III) ser transparente com relação aos procedimentos da entidade no Tratamento de Dados Pessoais; e IV) promover a conscientização em toda a entidade em relação à proteção de Dados Pessoais e questões de privacidade.

3. ABRANGÊNCIA

Este Manual é aplicável à **ATEAL** e a todos os funcionários e terceiros que tenham acesso a quaisquer Dados Pessoais mantidos e captados pela **ATEAL** ou em seu nome.

4. COMITÊ DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Este Manual estabelece a criação permanente do Comitê de Privacidade e Proteção de Dados Pessoais ("Comitê") para gerenciar atividades relacionadas à Privacidade e Proteção de Dados e tem como objetivo promover o conhecimento sobre os mecanismos de Privacidade e Proteção de Dados existentes e a proposição de ações voltadas ao seu aperfeiçoamento, com vistas ao cumprimento das disposições legais. O Comitê será composto de colaboradores ativos de diversas áreas e se reunirá sempre que necessário elaborando relatório de suas atividades (incluindo uma revisão da implementação deste Manual, se o caso).

5. ENCARREGADO DE DADOS PESSOAIS

A Entidade nomeará uma pessoa de seu quadro para exercer a função de Encarregado de Dados Pessoais ("DPO"), poderá ainda, se for o caso, optar por contratação externa de empresa especializada.

O Encarregado terá como missão orientar a implementação efetiva deste Manual, sem se limitar a ela, sempre definindo e disseminando boas práticas com relação ao uso de Dados Pessoais, com função primordial de ser o interlocutor entre o usuário de Dados

Pessoal e a ATEAL e a ANPD, expedindo notificações sobre violações de dados e mantendo-se em agenda contínua de treinamentos/conscientização acerca do tema.

6. PRINCÍPIOS

A ATEAL adotará os princípios da Adequação, Necessidade, Transparência, Livre Acesso, Qualidade dos Dados, Segurança, Prevenção e da Responsabilização e Prestação de Contas, observando-os na coleta, manuseio, armazenamento, compartilhamento e tratamento de "Dados Pessoais" sempre atendendo os padrões de privacidade e proteção de dados e em conformidade com a legislação e regulamentação aplicável.

Boa-fé

Todas as operações de tratamento serão pautadas no princípio da boa-fé, nas boas intenções, na moral e nos bons costumes.

Finalidade

O tratamento de Dados Pessoais realizar-se-á de maneira compatível com a finalidade original para a qual foram coletados, não podendo ser coletados com um propósito e utilizado para outro. Quaisquer outras finalidades deverão ser compatíveis com a razão original para qual os Dados Pessoais foram coletados.

Legalidade, Transparência e Não Discriminação

A Entidade tratará os Dados Pessoais de forma justa, transparente e em conformidade com legislação. Atuará somente quando houver um propósito/finalidade de tratamento que se enquadra em uma das hipóteses legais permitidas abaixo elencadas, sendo certo, que os Titulares de Dados deverão ser informados sobre a razão e a forma pela qual seus Dados Pessoais serão tratados.

i) para o cumprimento de obrigação legal ou regulatória pelo controlador;

ii) quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

iii) para o exercício regular de direitos em processo judicial, administrativo ou arbitral;

iv) quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;

v) para fins de cumprimentos legais com parcerias públicas.

Quando o Tratamento de Dados Pessoais não se enquadrar nas hipóteses acima, a Entidade deverá obter o consentimento dos Titulares dos Dados para o tratamento de seus dados pessoais, e assegurar que este consentimento seja obtido de forma livre, informada e inequívoca. A Entidade deverá coletar, armazenar e gerenciar todas as respostas de consentimento de maneira organizada e acessível, para que a comprovação de consentimento possa ser fornecida quando necessário. Da mesma forma, o Titular de Dados deverá ter a possibilidade de retirar o seu consentimento a qualquer momento com a mesma facilidade que foi fornecido.

Em algumas circunstâncias a Entidade também poderá tratar Dados Pessoais Sensíveis, envolvendo, mas não limitado a: dados de à saúde, de menores, biométricos, orientação sexual, condenações ou ofensas criminais, origem racial ou étnica, opiniões políticas, crenças religiosas, filiação a sindicato ou a organização de caráter religioso, filosófico ou político.

O tratamento de Dados Pessoais Sensíveis ocorrerá somente nos casos específicos descritos abaixo, nos quais deverão ser observados padrões de segurança mais robustos do que os empregados aos demais Dados Pessoais:

i) quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; e

ii) sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;

c) proteção da vida ou da incolumidade física do titular ou de terceiro; e

d) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

Necessidade e Minimização

Os Dados Pessoais coletados devem ser apropriados, relevantes e não excessivos com relação à finalidade para a qual são coletados e seu subsequente processamento. A Entidade tratará os Dados Pessoais na medida em que seja necessário para atingir um propósito específico. Em havendo amparo legal, o compartilhamento com outra empresa/poder público deverá observar este princípio.

Adequação

A Entidade deverá adotar medidas razoáveis para assegurar que quaisquer Dados Pessoais em sua posse sejam mantidos de forma adequada, atualizados em relação às finalidades para as quais foram coletados, sendo certo que deverá possibilitar ao Titular do Dado Pessoal a possibilidade de requerer a exclusão ou correção de dados imprecisos ou desatualizados, quando previstos em lei.

Retenção e Limitação do Armazenamento de Dados

A Entidade deverá ter conhecimento de suas atividades de tratamento, períodos de retenção estabelecidos e processos de revisão periódica, não podendo manter os Dados Pessoais por prazo superior ao necessário para atender as finalidades pretendidas, devendo para tanto organizar a exclusão automática ou manual dos dados.

Prevenção e Confidencialidade

A Entidade deverá assegurar que medidas técnicas e administrativas apropriadas serão aplicadas aos Dados Pessoais para protegê-los contra o Tratamento não autorizado ou ilegal, bem como contra a perda acidental, destruição ou danos. O Tratamento de Dados Pessoais também deverá garantir a devida confidencialidade, salvo se requisitado por ordem judicial e cumprimento de obrigação legal. Dentre as medidas técnicas mais comuns, podem ser descritas:

- Anonimização, significa que os Dados Pessoais são tornados anônimos de tal forma que os dados não mais se referem a uma pessoa direta ou indiretamente identificável. O anonimato tem que ser irreversível.

- Pseudonimização, que é um processo pelo qual os Dados Pessoais não mais se relacionam diretamente com uma pessoa identificável (por exemplo, mencionando seu nome), mas não é anônimo, porque ainda é possível, com informações adicionais, que são mantidas separadamente, identificar uma pessoa;
- Criptografia: é o processo de codificar mensagens ou informação de tal forma que somente partes autorizadas possam lê-la.

Responsabilização e Prestação de Contas

A Entidade é responsável e deverá demonstrar o cumprimento desta Política, assegurando a implementação de diversas medidas que incluem, mas não se limitam a: garantir que os Titulares dos Dados Pessoais possam exercer os seus direitos previsto no ordenamento jurídico, recomendar que fornecedores/parceiros contratados pela empresa que tenham acesso aos Dados Pessoais também estejam agindo de acordo a legislação e garantir que a empresa cumpra todas as exigências e solicitações da ANPD (Autoridade Nacional de Proteção de Dados).

7. PADRÕES DE SEGURANÇA

A Entidade compromete-se a implementar em todos os processos, novos ou já existentes, as melhores práticas do mercado em padrões de Segurança da Informação com vistas a garantir a Privacidade e Proteção de Dados Pessoais dos colaboradores, clientes e fornecedores/parceiros.

8. TRANSFERÊNCIA INTERNACIONAL DE DADOS

Quando os Dados Pessoais forem armazenados/tratados em países diferentes de onde foram coletados, a legislação e regulamentação aplicáveis à transferência internacional de dados de cada país deverá ser observada e deverá a empresa garantir um nível mínimo de proteção descrito neste manual

9. DIREITOS DOS TITULARES DE DADOS PESSOAIS

A Entidade estará comprometida com os direitos dos Titulares de Dados Pessoais previsto na legislação, os quais incluem:

· informar a finalidade da coleta e o período de armazenamento;

· a correção dos dados se estiverem imprecisos, incorretos ou incompletos;

· a exclusão, bloqueio e/ou anonimização quando aplicável;

· a retirada do Consentimento a qualquer momento, de forma simples e gratuita;

· implementar canais de atendimento às solicitações das demandas de titulares de dados;

· a revisão das decisões tomadas unicamente com base em Tratamento Automatizado de Dados Pessoais e a disponibilização de canal de acesso ao Encarregado de Dados Pessoais.

10. PRESTADORES DE SERVIÇOS

Os prestadores de serviços que tratem Dados Pessoais sob as instruções da Entidade estarão sujeitos às obrigações impostas pela legislação. A Entidade deverá assegurar que o contrato firmado entre as partes contemple cláusulas de privacidade e proteção de dados pessoais que garantam, no mínimo, medidas de segurança, controles técnicos e administrativos apropriados para garantir a confidencialidade das informações.

11. INCIDENTES

É dever de qualquer pessoa que saiba de um uso inapropriado de Dado Pessoal comunicar o Encarregado de Dados Pessoais. Em havendo algum tipo de incidentes e/ou potenciais violações de dados, imediatamente, as áreas deverão reportar ao Encarregado de Dados Pessoais, a qual deverá encaminhar e escalonar os possíveis problemas ao Comitê de Privacidade e Proteção de Dados Pessoais para tomada de decisão e apontamento/avaliação dos riscos e impactos para a empresa. Se compromete ainda, em criar planos de respostas aos incidentes e remediações.

Entende-se por violações de dados, mas não se limitam a qualquer vazamento, perda, exclusão, roubo ou acesso não autorizado de Dados Pessoais controlados ou tratados pela Entidade.

12. REVISÕES PERIÓDICAS E MONITORAMENTO

A Entidade se compromete a realizar revisões periódicas a fim de confirmar se as iniciativas de Privacidade e Proteção de Dados Pessoais, estão sendo aplicadas em seus sistemas, processos e outras atividades a luz da legislação vigente e através das melhores práticas de mercado aplicáveis a segurança da informação.

Se compromete ainda, a realizar monitoramento contínuo das melhorias, a fim de garantir a efetiva Privacidade e Proteção de Dados Pessoais.

13. CONSCIENTIZAÇÃO E TREINAMENTO

Todos os funcionários deverão ser conscientizados acerca dos temas envolvendo Privacidade e Proteção de Dados Pessoais, campanhas de conscientização e treinamentos serão conduzidos pelo Comitê.

Anexo I
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. A presente política é definida pelo conjunto de regras gerais que direcionam a segurança da informação e são suportadas por normas e procedimentos que deverão ser seguidos por toda a organização.

2. Estabelece procedimentos para utilização correta dos ativos de tecnologia da informação, a fim de evitar incidentes que possam: inutilizar, extinguir ou alterar dados. Promover ainda, a conscientização para com a segurança da informação e meios que contribuam para a manutenção dos princípios da segurança da Informação e seus aspectos: Confidencialidade, Integridade e Disponibilidade, Autenticidade e Não repúdio.

3. Política de Uso da Internet:

a) O colaborador não deverá compartilhar sua credencial de acesso ao computador a terceiros, caso contrário se responsabilizará pelo acesso indevido;

b) É vedado o acesso a sites que estejam fora do interesse da Entidade, como: bate papo, redes sociais, conteúdo ofensivo, racista ou pornográfico, a Entidade poderá definir exceções;

c) É vedado o acesso a sites de estrutura duvidosa que ofereçam risco à segurança da informação ou que possuam ferramentas que visem burlar os mecanismos de segurança da Entidade ou ocultar as credenciais de acesso à internet, como navegadores anônimos e proxy anônimo;

d) A critério da Entidade, sites com conteúdo não pertinente ao trabalho, terão o acesso bloqueado;

e) O colaborador que fizer mau uso da internet, terá o acesso bloqueado.

4. Uso da rede Sem Fio: a Entidade disponibiliza a rede sem fio (Wi-Fi) Corporativa e outra para acesso de Visitantes. O colaborador deverá utilizar com os mesmos princípios do item supra.

5. Uso da Rede Cabeada: a utilização da rede cabeada deverá ser realizada por dispositivos autorizados, terão seu acesso à Internet permitido de acordo com o grupo de liberação, para que funcionem de acordo com a política de segurança da Informação.

6. Política de Acesso aos Arquivos da Rede: todos os arquivos deverão ser salvos na rede, nas pastas dos respectivos departamentos, onde serão realizados *backups* periódicos. **Fica vedado** salvar arquivos no disco do computador pessoal de trabalho, pen drive, HD externos ou outro meio.

7. Política de Uso do E-mail:

a) O e-mail deverá ser utilizado apenas para os interesses da Entidade, não devendo ser utilizado para fins particulares, envio de spams, propaganda, conteúdo impróprio, difamatório, calunioso ou que prejudique a imagem da Entidade e seus colaboradores;

b) O funcionário deverá utilizar senha com a complexidade descrita nesta política de segurança e não fornecer sua senha para terceiros sob nenhuma hipótese;

c) O acesso do e-mail deverá ser realizado através da plataforma que a Entidade indicar;

d) O colaborador não deverá abrir e-mails de origem duvidosa, ou que julgar não pertinentes ao trabalho, incluindo anexos. Diante de qualquer dúvida deverá entrar em contato com a área de TI e mover a mensagem suspeita para a caixa de spam;

e) A camada de segurança AntiSpam poderá classificar o e-mail como provável spam ou bloquear a mensagem, caso seja classificado como spam.

8. Política de Uso dos Computadores:

a) O acesso aos computadores, sistemas e arquivos da rede da Entidade será fornecido através de credenciais de acesso de uso pessoal, a credencial de acesso será composta por login e senha;

b) Todo computador deverá possuir sistema antivírus instalado, ativo e atualizado que será fornecido, instalado e monitorado pela equipe de TI;

c) Não deverão ser instalados softwares não homologados pelo área de TI, softwares piratas, softwares para fins que não são do interesse da empresa ou não

relacionados com a função do colaborador;

d) Somente a equipe de TI estará autorizada à instalar softwares de qualquer tipo;

e) Não deverão ser baixados e/ou executados arquivos desconhecidos ou fora do interesse da Entidade, que possuam as extensões: .exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf, ou qualquer outra extensão que represente um risco à segurança;

f) Os computadores poderão ser monitorados e auditados pela equipe de TI a qualquer tempo, para fim de verificação de conformidade com a política de segurança da informação;

g) Os computadores terão padronizados: o papel de parede, impressoras, ícones e unidades de rede mapeadas;

h) O colaborador deverá bloquear seu computador quando ausentar-se do departamento, mesmo que por breve período de tempo, se o tiver que se ausentar por tempo indeterminado deverá desligar o computador;

i) Não será fornecida credencial de acesso do tipo Administrador.

9. Política de Senha e Acesso:

a) A senha de acesso de um novo colaborador de qualquer sistema deverá ser requisitada pelo superior imediato do setor, através de chamado, com preenchimento de formulário de solicitação de acessos;

b) A senha de acesso aos sistemas e computadores é de uso pessoal e não deve ser compartilhada;

c) Após 3 (três) tentativas seguidas de acesso com senha inválida, a senha será bloqueada e o colaborador deverá entrar em contato com a equipe de TI para desbloqueio da senha;

10. Política de dispositivos Pessoais

a) Não será permitido a guarda de arquivos pessoais na rede da Entidade, que incluem: músicas, imagens, vídeos e outros arquivos em geral.

b) Será permitido o uso de dispositivos pessoais, como notebook, desde que estejam de acordo com as políticas de segurança da informação da Entidade e seja informado e solicitada autorização ao departamento de TI.

11. Política de Uso de Impressoras: a quantidade de impressões, será registrada em Log, e poderá ser auditada quanto ao colaborador que imprimiu, quantidade de páginas, nome do arquivo impresso. O uso das impressoras deverá ser feito para os interesses da empresa e utilizadas com consciência ecológica.

12. Política de *Backup* e Contingência:

a) Procedimento de Backup dos Arquivos e Bancos de Dados é realizado semanal e mensalmente, por seus respectivos responsáveis, internos e terceirizados, sendo este completo e automatizados.

13. Política de Controle de Acesso à Infraestrutura:

a) Bloqueio de Acesso a funcionários Desligados, o departamento de Recursos Humanos deverá informar ao setor de TI, quando houver o desligamento de funcionários, para que as credenciais de acesso aos sistemas, computadores, e-mail e ambiente de rede, sejam bloqueadas;

b) Registro de Chamados diante de qualquer incidente ou pedido de suporte, deverá ser registrado o pedido ou a demanda através de CI ou através de email direcionado sempre à liderança da área.

14. Responsabilidades:

a) Área de TI, manter e atualizar essa política de segurança da Informação periodicamente;

b) Funcionários, cumprir as políticas de segurança da informação e contribuir para sua melhoria e eficiência.

c) Gestores e Diretoria, apoiar a implementação da presente política.

15. Cumprimento: diante do descumprimento desta política em geral, o funcionário poderá, a qualquer tempo, ser auditado, através da equipe de TI e poderá receber em consequência, a aplicação de ações disciplinares cabíveis que se fizerem necessárias.

Anexo II
POLÍTICA DE RETENÇÃO E DESCARTE DE DADOS

1. A Entidade deverá realizar procedimentos de *backups*, armazenagem e rastreabilidade para as informações que contenham dados pessoais, de forma que estes possam atender aos requisitos relacionados ao tempo de retenção.

2. Assegurar que todas as medidas de segurança sistêmicas foram devidamente adotadas quando situações de armazenamento de dados pessoais ocorrer dentro da Entidade, e principalmente, fora do ambiente da organização.

3. A retenção de dados pessoais deverá respeitar o ciclo de vida dos dados dentro da Entidade e deverá ser pautada no embasamento legal que sustenta o tratamento dos dados pessoais.

4. A eliminação de dados que estejam armazenados em mídias como cd, dvd, disquete, disco rígido, fita de dados, arquivos, *pen drive* ou outro meio digital, bem como os registrados em papel e/ou formulários deverão ocorrer tão logo a finalidade atrelada ao tratamento se encerre, respeitando o prazo prescricional para medidas jurídicas.

4.1 Os descartes deverão ser realizados dentro dos limites técnicos, a Entidade deverá empregar as melhores técnicas a fim de garantir que sejam descartados corretamente, preservando a confidencialidade das informações.

4.2 Deverá a Entidade registrar o descarte de toda e qualquer informação que detenha dados pessoais.

5. Os prazos para retenção dos dados pessoais dependerão de cada finalidade e obedecerão aos prazos e prescrições legais estipulados. A Entidade poderá estipular prazos quando a lei for omissa.

5.1 Os prazos de retenção serão estabelecidos conforme legislação aplicável, para os casos que a lei for omissa ou for de legítimo interesse do controlador estabelecer-se-á até 05 (cinco) anos, podendo ser revisto a qualquer tempo.

5.1.1 Entende-se como Dados Cadastrais todos os dados coletados através de:

i) plataformas online (site, rede social e outros);

ii) *stand* de vendas ou qualquer outro evento da Entidade;

iii)abordagem comercial por telefone, e-mail e aplicativos de comunicação.