

**MOREIRA DINIZ ANÁLISES CLÍNICAS, VACINAÇÃO E MEDICINA
DIAGNÓSTICA LTDA**

Laboratório Andreia Braz
CNPJ nº 59.930.364/0001-13

CÓDIGO DE BOAS PRÁTICAS DE PROTEÇÃO DE DADOS PESSOAIS

Documento do MOREIRA DINIZ ANÁLISES CLÍNICAS, VACINAÇÃO E MEDICINA DIAGNÓSTICA LTDA (Laboratório Andreia Braz), CNPJ nº 59.930.364/0001-13, estabelecido nos termos do art. 50 da Lei nº 13.709/2018, para orientar o tratamento de dados pessoais na prestação de serviços de análises clínicas e de vacinação, nas unidades de Mateus Leme, Azurita, Juatuba e Serra Azul.

1. Considerações iniciais

O Laboratório Andreia Braz é um estabelecimento de saúde voltado a análises clínicas e vacinação. Dada a natureza de sua atividade, trata de forma intensiva dados pessoais e dados pessoais sensíveis relativos à saúde, o que exige atenção especial ao fluxo dessas informações.

Este Código de Boas Práticas consolida os princípios, as bases legais e os procedimentos adotados pelo laboratório para o tratamento de dados pessoais, com o objetivo de assegurar a conformidade com a Lei nº 13.709/2018 e com as normas setoriais aplicáveis, reforçando a confiança de pacientes, colaboradores e parceiros. Ele complementa a Política de Privacidade, a Política de Cookies, o Plano de Resposta a Incidentes e os demais documentos do programa de governança em privacidade do laboratório.

2. Marco normativo aplicável

O tratamento de dados pessoais pelo laboratório observa, entre outras, as seguintes normas:

- Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais);
- Constituição Federal, art. 5º, incisos X e XII, e inciso LXXIX (direito fundamental à proteção de dados);
- Lei nº 8.078/1990 (Código de Defesa do Consumidor) e Código Civil;
- Lei nº 12.965/2014 (Marco Civil da Internet);
- Lei nº 13.787/2018 (digitalização e guarda de prontuário de paciente);
- RDC ANVISA nº 786/2023 e demais normas sanitárias aplicáveis a laboratórios de análises clínicas;
- Resoluções do Conselho Federal de Medicina, do Conselho Federal de Farmácia e do Conselho Federal de Biomedicina quanto ao sigilo profissional;
- Resoluções da ANPD, em especial a Resolução CD/ANPD nº 2/2022 (agentes de tratamento de pequeno porte) e a Resolução CD/ANPD nº 15/2024 (comunicação de incidentes).

3. Princípios do tratamento de dados

O laboratório observa os princípios do art. 6º da Lei nº 13.709/2018:

- **Finalidade:** tratamento para propósitos legítimos, específicos e informados ao titular.
- **Adequação:** compatibilidade do tratamento com as finalidades informadas.
- **Necessidade e minimização:** coleta e uso limitados ao mínimo necessário à finalidade.
- **Livre acesso:** garantia ao titular de consulta facilitada e gratuita sobre o tratamento.
- **Qualidade dos dados:** exatidão, clareza e atualização dos dados.
- **Transparência:** informações claras e acessíveis sobre o tratamento.
- **Segurança e prevenção:** medidas técnicas e administrativas de proteção e prevenção de danos.
- **Não discriminação:** vedação ao tratamento para fins discriminatórios ilícitos ou abusivos.
- **Responsabilização e prestação de contas:** demonstração da adoção de medidas eficazes de conformidade.

4. Bases legais do tratamento

O tratamento de dados pessoais deve estar fundamentado em uma das bases legais dos arts. 7º e 11 da Lei nº 13.709/2018. No laboratório, as bases predominantes são:

- **Dados comuns:** execução de contrato (art. 7º, inciso V) e cumprimento de obrigação legal e regulatória (art. 7º, inciso II).
- **Dados sensíveis de saúde:** tutela da saúde, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (art. 11, inciso II, alínea "f"), e obrigação legal ou regulatória (art. 11, inciso II, alínea "a").
- **Atendimentos ao SUS:** execução de políticas públicas (art. 7º, inciso III; art. 11, inciso II, alínea "b").
- **Exercício regular de direitos:** em processos judiciais, administrativos ou arbitrais (art. 7º, inciso VI; art. 11, inciso II, alínea "d").
- **Consentimento:** apenas quando nenhuma outra base for cabível, como no marketing e no uso de imagem, e, no caso de crianças e adolescentes, mediante consentimento de um dos pais ou responsável (art. 14).

A base legal da tutela da saúde não se aplica indistintamente a toda atividade do laboratório; ela se destina aos tratamentos ligados ao diagnóstico e ao cuidado, realizados por ou sob a responsabilidade de profissionais sujeitos ao dever de sigilo. Mesmo quando dispensado o consentimento, o tratamento deve respeitar os princípios da necessidade, da finalidade e da adequação. O legítimo interesse não pode fundamentar o tratamento de dados sensíveis de saúde.

5. Agentes de tratamento

O laboratório atua, em regra, como **controlador** dos dados dos pacientes que atende por conta própria, definindo as finalidades e os meios do tratamento. Atua como **operador** quando executa exames por conta e ordem de terceiros, como o SUS, a Unidade de Pronto Atendimento e o hospital conveniado, que são controladores dos dados de seus pacientes. Os laboratórios de apoio, os prestadores de tecnologia e a contabilidade atuam como

operadores do laboratório. A definição concreta de cada papel depende de quem toma as decisões sobre o tratamento em cada operação.

O laboratório pode enquadrar-se como agente de tratamento de pequeno porte, nos termos da Resolução CD/ANPD nº 2/2022, o que lhe assegura tratamento diferenciado quanto a determinadas obrigações, sem afastar o dever de conformidade com a Lei nº 13.709/2018.

6. Obrigações do laboratório

Como agente de tratamento, o laboratório obriga-se, entre outros deveres, a: indicar o Encarregado pelo Tratamento de Dados (art. 41); manter a segurança da informação em todos os tratamentos (arts. 46 a 49); manter registro das operações de tratamento (art. 37); firmar contratos com operadores (art. 39); atender aos direitos dos titulares (art. 18); e comunicar incidentes de segurança relevantes (art. 48).

7. Direitos dos titulares

O laboratório assegura aos titulares os direitos do art. 18 da Lei nº 13.709/2018:

- confirmação da existência de tratamento e acesso aos dados;
- correção de dados incompletos, inexatos ou desatualizados;
- anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei;
- portabilidade a outro fornecedor, observados os segredos comercial e industrial;
- eliminação dos dados tratados com base no consentimento, salvo as hipóteses de guarda obrigatória;
- informação sobre o compartilhamento e sobre a possibilidade de não fornecer consentimento;
- revogação do consentimento e oposição a tratamento em desconformidade com a lei.

O laboratório mantém canal de atendimento ao titular, registra as solicitações, confirma a identidade do requerente e responde nos prazos legais, ressalvadas as limitações decorrentes da guarda obrigatória dos registros de saúde.

8. Protocolo de atendimento e dados cadastrais

8.1. O primeiro tratamento de dados ocorre no cadastro do paciente, quando são coletados dados como nome, CPF, data de nascimento, endereço, telefone, e-mail, nome da mãe e número do convênio ou do cartão do SUS. O laboratório coleta apenas os dados necessários à finalidade, dispensando, por exemplo, o RG quando o paciente possuir CPF.

8.2. As bases legais aplicáveis são a execução de contrato (art. 7º, inciso V) e a obrigação legal e regulatória (art. 7º, inciso II) para os dados comuns, e a tutela da saúde (art. 11, inciso II, alínea "f") para os dados sensíveis vinculados ao atendimento.

8.3. Os dados cadastrais não vinculados a prontuário devem ser eliminados quando cessar a finalidade. Os dados vinculados aos registros de saúde observam o prazo de guarda indicado no item 12.

9. Protocolo de coleta e exames laboratoriais

9.1. Os laboratórios de análises clínicas geram e gerenciam dados sensíveis de saúde em todas as etapas, da coleta da amostra ao armazenamento do resultado. Cada etapa deve

observar a identificação correta do paciente, a rastreabilidade das amostras e o sigilo das informações.

9.2. A base legal aplicável à coleta, ao processamento, à emissão de laudo, à liberação e ao armazenamento dos resultados, quando realizados por profissionais sujeitos ao dever de sigilo, é a tutela da saúde (art. 11, inciso II, alínea "f"), sem prejuízo das obrigações regulatórias (alínea "a").

9.3. Os profissionais de análises clínicas, como biomédicos e farmacêuticos bioquímicos, estão sujeitos ao dever de sigilo previsto nas normas de seus conselhos profissionais. O acesso aos dados e aos resultados deve observar o princípio da necessidade, restringindo-se aos colaboradores que deles necessitam para o exercício de suas funções.

10. Protocolo de compartilhamento de dados

10.1. O compartilhamento de dados pelo laboratório ocorre apenas quando necessário e de acordo com o princípio da minimização, notadamente com laboratórios de apoio, convênios, o SUS, a Unidade de Pronto Atendimento, o hospital conveniado e as autoridades sanitárias.

10.2. Diferentemente do que se costuma supor, a base legal principal para o compartilhamento de dados de saúde entre serviços e profissionais de saúde não é o consentimento, mas a tutela da saúde (art. 11, inciso II, alínea "f") e o cumprimento de obrigação legal ou regulatória (art. 11, inciso II, alínea "a"). O consentimento é reservado às hipóteses em que os dados sejam compartilhados com terceiros que não sejam serviços ou profissionais de saúde e não haja outra base legal cabível.

10.3. O compartilhamento de dados de saúde com finalidade econômica observa as restrições do art. 11, § 4º, da Lei nº 13.709/2018, sendo admitido apenas em benefício do titular e para a prestação de serviços de saúde.

10.4. O compartilhamento com operadores, como laboratórios de apoio, prestadores de tecnologia e contabilidade, deve ser precedido de contrato de tratamento de dados, que defina finalidades, responsabilidades, medidas de segurança e destinação dos dados ao término do serviço (art. 39 da Lei nº 13.709/2018). O compartilhamento com o SUS observa a condição de operador do laboratório perante a Secretaria Municipal de Saúde.

11. Protocolo de segurança da informação

11.1. Nos termos do art. 46 da Lei nº 13.709/2018, o laboratório adota medidas técnicas e administrativas de segurança, dentre as quais:

Medida	Descrição
Política e conscientização	Elaborar, revisar e comunicar diretrizes de proteção de dados e capacitar periodicamente os colaboradores.
Gestão de acesso	Conceder acesso apenas às pessoas autorizadas, por perfil de função, com login individual, revogação no desligamento e, quando possível, duplo fator de autenticação.
Gestão de backups	Manter cópias de segurança criptografadas e protegidas contra acessos não autorizados, com testes de restauração.
Gestão de ativos e dispositivos	Inventariar os ativos que tratam dados pessoais e disciplinar o uso de equipamentos e mídias removíveis.

Proteção contra programas maliciosos	Manter solução de antimalware instalada e atualizada nos equipamentos que tratam dados.
Registro de acessos (logs)	Registrar, sempre que possível, data, horário, identidade do responsável e ação executada nos sistemas críticos.
Gestão de fornecedores	Avaliar e contratar operadores que atendam a requisitos mínimos de segurança.
Segurança no descarte	Eliminar documentos físicos por fragmentação e dados eletrônicos de forma segura.

11.2. Recomenda-se, ainda, a adoção progressiva de criptografia, pseudonimização e anonimização, quando aplicáveis, observado o estágio de adequação do laboratório e a proporcionalidade das medidas ao seu porte.

12. Retenção e eliminação de dados

12.1. Os dados são mantidos apenas enquanto necessários às finalidades e aos prazos legais. Os prontuários e registros dos pacientes são preservados pelo prazo mínimo de 20 (vinte) anos, nos termos da Lei nº 13.787/2018, observadas as normas da ANVISA. Os documentos fiscais e financeiros seguem os prazos das legislações fiscal e tributária.

12.2. Encerrados os prazos e as finalidades, os dados são eliminados de forma segura ou anonimizados, resguardados o sigilo e a intimidade do titular. Os dados tratados com base no consentimento são eliminados quando este for revogado, salvo obrigação legal de guarda.

13. Encarregado, governança e sanções

13.1. O laboratório indica o Encarregado pelo Tratamento de Dados (DPO), responsável pela interlocução com os titulares e a ANPD (art. 41), e mantém programa de governança em privacidade, com políticas, treinamentos, contratos e revisão periódica.

13.2. O descumprimento da Lei nº 13.709/2018 sujeita os agentes de tratamento às sanções do art. 52, que incluem advertência, multa simples de até 2% do faturamento, limitada a R\$ 50.000.000,00 por infração, multa diária, publicização da infração, bloqueio e eliminação dos dados, e suspensão ou proibição parcial ou total das atividades de tratamento, aplicadas pela ANPD como autoridade competente.

14. Disposições finais

Este Código de Boas Práticas é revisado periodicamente e sempre que houver alteração normativa ou operacional relevante. Sua observância é obrigatória para todos os colaboradores, prestadores de serviços e operadores do laboratório.

Mateus Leme/MG, 23 de Julho de 2026.

MOREIRA DINIZ ANÁLISES CLÍNICAS, VACINAÇÃO E MEDICINA DIAGNÓSTICA LTDA

(Laboratório Andreia Braz)

CNPJ nº 59.930.364/0001-13