CONSELHO REGIONAL DE MEDICINA DO PARANÁ

POLÍTICA INSTITUCIONAL DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Como o CRM-PR trata dados pessoais em suas atividades públicas, administrativas e digitais

Documento	Política Institucional de Privacidade e Proteção de Dados Pessoais do CRM-PR
Versão	0.2 - primeira minuta completa
Data	29 de julho de 2026
Situação	Submetida à validação jurídica, técnica e setorial

A versão pública deverá ser disponibilizada em privacidade.crmpr.org.br e em meio impresso na sede e nas representações, após aprovação institucional.

Como ler esta política

Esta política explica, em linguagem pública, quais dados pessoais podem ser tratados pelo CRM-PR, de onde eles vêm, para que são usados, com quem podem ser compartilhados, por quanto tempo são conservados e como os titulares podem exercer seus direitos. Ela se aplica aos atendimentos presenciais e remotos, aos processos físicos e eletrônicos, aos sistemas institucionais, ao site e às demais atividades do Conselho.

> **Ponto central**
> Nas atividades obrigatórias do CRM-PR, o tratamento de dados decorre da lei e das competências públicas do Conselho. Por isso, em regra, não depende de consentimento. O consentimento será usado apenas quando houver escolha real e uma finalidade facultativa e específica.

Avisos específicos poderão complementar esta política, especialmente nos formulários de atendimento, no recebimento de denúncias, no uso de cookies, no monitoramento por câmeras e em eventos. Em caso de divergência, prevalecem a legislação e as normas processuais aplicáveis ao caso concreto.

Sumário

1. Apresentação, objetivo e alcance	9. Compartilhamento, operadores e transferências internacionais
2. Quem controla os dados e como falar com o encarregado	10. Transparência pública e proteção de dados
3. Princípios e compromissos	11. Segurança da informação e incidentes
4. Conceitos essenciais	12. Retenção, eliminação e preservação documental
5. Titulares, categorias e origem dos dados	13. Direitos dos titulares e atendimento
6. Atividades de tratamento do CRM-PR	14. Atualizações, vigência e controle de versões
7. Bases legais utilizadas	15. Referências normativas essenciais
8. Dados sensíveis, crianças e adolescentes	

1. Apresentação, objetivo e alcance

O Conselho Regional de Medicina do Paraná (CRM-PR) é uma autarquia federal integrante do sistema formado pelo Conselho Federal de Medicina (CFM) e pelos Conselhos Regionais de Medicina. Entre suas atribuições estão o registro de médicos e pessoas jurídicas, a fiscalização do exercício profissional, a apuração de infrações ético-profissionais, a orientação institucional e a execução de atividades administrativas necessárias ao funcionamento do Conselho.

Para cumprir essas atribuições, o CRM-PR trata dados pessoais de médicos, pacientes, denunciantes, testemunhas, representantes de empresas, empregados, candidatos, fornecedores, visitantes e outras pessoas relacionadas às suas atividades. Alguns desses dados são sensíveis, como informações de saúde, biometria e documentos clínicos.

Esta política tem três objetivos:

- dar transparência às operações de tratamento realizadas pelo CRM-PR;
- orientar titulares, empregados, conselheiros, colaboradores e prestadores de serviço;
- estabelecer compromissos públicos de privacidade, segurança, necessidade e responsabilização.

A política abrange dados tratados em meio físico ou digital, na sede e nas representações, em sistemas próprios ou compartilhados, no site, em canais de atendimento e em serviços executados por prestadores contratados. Ela não substitui o Código de Processo Ético-Profissional, as regras de acesso a autos, a Lei de Acesso à Informação, os instrumentos contratuais nem os procedimentos internos de segurança e governança.

2. Quem controla os dados e como falar com o encarregado

2.1 Controlador

O CRM-PR é o controlador dos dados pessoais quando define as finalidades e os elementos essenciais do tratamento realizado no exercício de suas competências e atividades institucionais.

Identificação institucional: Conselho Regional de Medicina do Paraná - CRM-PR. Endereço da sede: Rua Victório Viezzer, 84, Vista Alegre, Curitiba/PR, CEP 80810-340.

2.2 Encarregado pelo tratamento de dados pessoais

O encarregado atua como canal de comunicação entre o CRM-PR, os titulares e a Agência Nacional de Proteção de Dados (ANPD), recebe solicitações, presta esclarecimentos, orienta a instituição e acompanha medidas de conformidade.

Canal de contato: dpo@crmpr.org.br

Página institucional: privacidade.crmpr.org.br

A identidade e o ato de designação do encarregado serão mantidos atualizados na página institucional, sem necessidade de alterar esta política a cada substituição.

> **O que o encarregado não substitui**
> Pedidos de acesso a processos, recursos, reclamações de atendimento, requerimentos administrativos e solicitações pela Lei de Acesso à Informação devem seguir seus canais próprios. O encarregado tratará a questão de proteção de dados e poderá orientar o encaminhamento correto.

3. Princípios e compromissos

O CRM-PR busca tratar dados pessoais de acordo com os seguintes compromissos:

- **Finalidade e adequação:** usar dados para propósitos legítimos, específicos e compatíveis com as atribuições do Conselho;
- **Necessidade:** solicitar e acessar apenas os dados pertinentes ao serviço, processo ou atividade;

- **Livre acesso e transparência:** informar de forma clara como o tratamento ocorre, ressalvados os sigilos legais e a proteção de terceiros;
- **Qualidade dos dados:** adotar medidas para manter dados relevantes corretos e atualizados;
- **Segurança e prevenção:** reduzir riscos de acesso não autorizado, perda, alteração, divulgação ou uso indevido;
- **Não discriminação:** não usar dados para fins discriminatórios ilícitos ou abusivos;
- **Responsabilização:** documentar decisões, atribuir responsabilidades e revisar práticas de privacidade;
- **Proteção desde a concepção:** considerar privacidade e segurança no desenvolvimento ou contratação de processos e sistemas.

4. Conceitos essenciais

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

Dado pessoal sensível: dado sobre origem racial ou étnica, convicção religiosa, opinião política, filiação sindical ou a organização religiosa, filosófica ou política, saúde, vida sexual, genética ou biometria, quando vinculado a uma pessoa.

Tratamento: qualquer operação com dados pessoais, como coleta, acesso, uso, registro, organização, compartilhamento, arquivamento, armazenamento, alteração, anonimização ou eliminação.

Controlador: pessoa ou instituição que decide as finalidades e os elementos essenciais do tratamento.

Operador: pessoa ou instituição juridicamente distinta que trata dados em nome do controlador e segundo suas instruções.

Titular: pessoa natural a quem os dados se referem.

Anonimização: processo que retira, com meios técnicos razoáveis, a possibilidade de associar o dado a uma pessoa.

Incidente de segurança: evento confirmado que comprometa a confidencialidade, a integridade, a disponibilidade ou a autenticidade de dados pessoais.

Uso compartilhado: comunicação ou tratamento conjunto de dados entre órgãos, entidades ou agentes, dentro das hipóteses admitidas pela legislação.

Empregados, conselheiros e colaboradores que tratam dados no exercício de suas funções atuam sob a autoridade do CRM-PR e devem observar as regras internas de acesso, confidencialidade e segurança. Eles não se tornam, apenas por isso, operadores autônomos na acepção da LGPD.

5. Titulares, categorias e origem dos dados

5.1 Quem pode ser titular

O CRM-PR pode tratar dados de:

- médicos inscritos, requerentes de inscrição e profissionais vinculados a procedimentos;
- sócios, diretores técnicos, representantes e empregados de pessoas jurídicas;
- pacientes, familiares, acompanhantes, denunciantes, noticiantes, testemunhas, peritos e procuradores;
- conselheiros, empregados, estagiários, aprendizes, candidatos e dependentes;
- fornecedores, licitantes, representantes, equipes contratadas e parceiros institucionais;
- participantes, palestrantes e convidados de eventos, cursos, pesquisas e campanhas;
- visitantes, usuários dos canais de atendimento e usuários dos ambientes digitais.

5.2 Categorias de dados

Conforme a atividade, podem ser tratados:

- dados de identificação e contato, como nome, CPF, documento de identidade, endereço, telefone, e-mail, assinatura e fotografia;

- dados profissionais, acadêmicos e cadastrais, como número de inscrição, especialidade, formação, vínculos, responsabilidade técnica e situação profissional;
- dados financeiros e patrimoniais, como pagamentos, débitos, boletos, dados bancários e informações necessárias à cobrança;
- dados processuais e probatórios, como declarações, manifestações, documentos, imagens, áudios, vídeos, registros de atendimento e informações sobre fatos apurados;
- dados sensíveis, especialmente informações de saúde, prontuários, exames, laudos, receitas, biometria e dados ocupacionais;
- dados técnicos e de segurança, como endereço IP, registros de acesso, autenticação, dispositivo, navegador, cookies e eventos de sistema;
- imagem e voz captadas em eventos, reuniões, atendimentos remotos, fiscalização ou monitoramento de segurança, quando pertinente.

5.3 De onde os dados vêm

Os dados podem ser:

- fornecidos pelo titular, por representante, procurador, empregador, instituição de saúde ou pessoa relacionada ao fato;
- gerados durante atendimentos, análises, diligências, fiscalizações, processos, pagamentos, contratos ou uso de sistemas;
- recebidos do CFM, de outros CRMs, de órgãos públicos, autoridades, instituições financeiras ou prestadores, quando houver fundamento jurídico;
- obtidos em bases oficiais, registros públicos, portais institucionais ou outras fontes de acesso legítimo e pertinente à finalidade;
- inferidos a partir de informações existentes, desde que a inferência seja necessária, adequada e passível de revisão.

> **Dado público também exige cuidado**
> O fato de uma informação estar disponível em fonte pública não autoriza uso irrestrito. O CRM-PR deve observar a finalidade da fonte, a necessidade, a boa-fé, o interesse público e os direitos do titular.

6. Atividades de tratamento do CRM-PR

A seguir estão as principais atividades em que o CRM-PR trata dados pessoais. As categorias e os destinatários variam conforme o caso. Nem todos os dados indicados são coletados em todas as situações.

6.1 Registro e cadastro de médicos e pessoas jurídicas

Dados que podem ser tratados: dados de identificação e contato, documentos civis, fotografia, assinatura, biometria quando utilizada, formação, diploma, especialidade, vínculos, situação cadastral, dados de sócios e responsáveis técnicos e documentos da pessoa jurídica.

Para que são usados: receber inscrições, emitir identidade e certidões, manter o cadastro profissional, verificar habilitação e regularidade, registrar especialidades, responsabilidades técnicas, alterações e cancelamentos e atender obrigações do sistema CFM/CRMs.

Fundamentos principais: cumprimento de obrigação legal ou regulatória, finalidade pública e execução das competências legais do CRM-PR; exercício regular de direitos; prevenção à fraude e segurança em autenticação, quando aplicável.

Acesso e compartilhamento: setores de registro e atendimento, CFM, outros CRMs, instituições de ensino, órgãos públicos e prestadores necessários à emissão, autenticação e manutenção dos serviços.

6.2 Atendimento, protocolos, ouvidoria, SIC e participação social

Dados que podem ser tratados: identificação, contato, representação, conteúdo da solicitação, anexos, gravações ou registros de atendimento e dados necessários à resposta.

Para que são usados: autenticar o requerente, registrar e encaminhar pedidos, prestar serviços, responder manifestações, receber reclamações, pedidos de informação, consultas e contribuições em audiências ou processos participativos.

Fundamentos principais: cumprimento de dever legal, execução de competências públicas, atendimento ao usuário do serviço público, exercício regular de direitos e consentimento apenas para finalidades facultativas específicas.

Acesso e compartilhamento: unidades competentes para responder, órgãos públicos relacionados, CFM/CRMs, prestadores de protocolo, atendimento, correspondência e tecnologia, além do solicitante ou representante legitimado.

6.3 Fiscalização do exercício profissional e de estabelecimentos

Dados que podem ser tratados: identificação e dados profissionais de médicos e responsáveis, informações sobre estabelecimentos e equipes, documentos assistenciais, escalas, contratos, imagens, dados de pacientes e outros elementos necessários à diligência.

Para que são usados: planejar e realizar fiscalizações, verificar condições do exercício profissional, apurar irregularidades, produzir relatórios, adotar medidas administrativas e subsidiar outros procedimentos.

Fundamentos principais: cumprimento de obrigações legais e regulatórias, finalidade pública e poder de fiscalização, exercício regular de direitos e proteção da vida ou da incolumidade física, quando a situação concreta o justificar.

Acesso e compartilhamento: fiscais, conselheiros e setores competentes; CFM e outros CRMs; gestores e instituições fiscalizadas; autoridades e órgãos públicos quando houver obrigação, competência ou necessidade formalmente demonstrada.

6.4 Denúncias, sindicâncias e processos ético-profissionais

Dados que podem ser tratados: identificação e contato de denunciantes, médicos, pacientes, testemunhas e representantes; alegações, manifestações, prontuários, exames, laudos, receitas, imagens, áudios, vídeos e demais provas.

Para que são usados: receber e verificar denúncias, instaurar apuração de ofício quando cabível, instruir sindicâncias e processos, realizar comunicações, julgar, processar recursos, preservar provas e garantir direitos processuais.

Fundamentos principais: cumprimento de obrigação legal ou regulatória, exercício regular de direitos em processo administrativo ou judicial e execução das competências públicas do CRM-PR, inclusive para dados sensíveis.

Acesso e compartilhamento: acesso restrito a pessoas autorizadas; disponibilização aos sujeitos processuais e representantes na medida necessária ao procedimento; compartilhamento com o CFM, outros CRMs, instituições envolvidas na prova e autoridades competentes, quando juridicamente cabível.

> **Sigilo não equivale a anonimato**
> A denúncia anônima não é aceita como denúncia formal pelo Código de Processo Ético-Profissional. O sigilo do procedimento não garante que a identidade do denunciante ou o conteúdo da denúncia permaneçam ocultos do médico envolvido quando o acesso for necessário à apuração, ao contraditório ou à ampla defesa.

6.5 Anuidades, taxas, multas, cobrança e execução

Dados que podem ser tratados: identificação, inscrição profissional, débitos, pagamentos, parcelamentos, dados bancários, documentos de cobrança e informações processuais.

Para que são usados: calcular, lançar e receber receitas, emitir boletos, conciliar pagamentos, negociar ou parcelar débitos, inscrever créditos, realizar cobrança administrativa ou judicial e cumprir obrigações contábeis, fiscais e de controle.

Fundamentos principais: cumprimento de obrigação legal e regulatória, exercício regular de direitos e execução de contratos ou instrumentos de parcelamento.

Acesso e compartilhamento: setores financeiro, contábil e jurídico; instituições financeiras, meios de pagamento, serviços de cobrança e correspondência; órgãos de controle, Judiciário e autoridades fiscais, nos limites legais.

6.6 Licitações, compras, contratos, convênios e fornecedores

Dados que podem ser tratados: dados de representantes, procuradores, sócios, responsáveis técnicos, empregados e equipes; documentos de habilitação, contatos, dados bancários, registros contratuais e informações de fiscalização.

Para que são usados: planejar contratações, selecionar fornecedores, formalizar e fiscalizar contratos, realizar pagamentos, aplicar medidas administrativas, prestar contas e cumprir deveres de transparência e controle.

Fundamentos principais: cumprimento de obrigações legais, procedimentos pré-contratuais, execução de contrato, exercício regular de direitos e legítimo interesse institucional em atividades de apoio, quando cabível e avaliado.

Acesso e compartilhamento: comissão de contratação, fiscais e gestores, áreas requisitantes, assessorias, bancos, órgãos de controle, portais oficiais, demais órgãos públicos e prestadores envolvidos na execução contratual.

6.7 Gestão de pessoas, seleção, estágio e saúde ocupacional

Dados que podem ser tratados: identificação, contato, currículo, formação, histórico profissional, documentos funcionais, folha de pagamento, benefícios, frequência, avaliação, dados bancários, dependentes, biometria e dados de saúde ocupacional.

Para que são usados: recrutar e selecionar, formalizar e gerir vínculos, cumprir obrigações trabalhistas, previdenciárias, fiscais e de saúde e segurança do trabalho, administrar benefícios, capacitação, acesso físico e lógico e processos disciplinares.

Fundamentos principais: cumprimento de obrigação legal ou regulatória, procedimentos pré-contratuais e execução contratual, exercício regular de direitos, tutela da saúde em contexto autorizado e prevenção à fraude e segurança.

Acesso e compartilhamento: gestão de pessoas, chefias e áreas competentes; bancos, operadoras de benefícios, serviços de saúde ocupacional, seguradoras, órgãos públicos e prestadores contratados, conforme necessidade e contrato.

6.8 Processos judiciais, consultoria e defesa institucional

Dados que podem ser tratados: dados das partes, representantes, testemunhas, profissionais, documentos administrativos, provas, informações financeiras e dados sensíveis relacionados à controvérsia.

Para que são usados: prestar consultoria, formular manifestações, ajuizar ou responder ações, cumprir decisões, produzir provas, negociar soluções, exercer defesa institucional e acompanhar processos.

Fundamentos principais: exercício regular de direitos em processos judiciais, administrativos ou extrajudiciais e cumprimento de obrigação legal.

Acesso e compartilhamento: assessoria jurídica, procuradores e advogados, Judiciário, Ministério Público, advocacias públicas, peritos, auxiliares da justiça e demais participantes legitimados no processo.

6.9 Transparência, controle, auditoria e prestação de contas

Dados que podem ser tratados: dados funcionais, contratuais, financeiros, patrimoniais, decisórios e informações constantes de documentos públicos.

Para que são usados: cumprir deveres de transparência, prestar contas, atender auditorias, controle interno e externo, publicar atos e responder a pedidos de informação.

Fundamentos principais: cumprimento de obrigação legal ou regulatória, finalidade pública e exercício regular de direitos.

Acesso e compartilhamento: Portal da Transparência, órgãos de controle, auditorias, interessados em pedidos de informação e sociedade, após avaliação de necessidade, publicidade, sigilo e proteção de dados.

6.10 Eventos, ensino, pesquisas, campanhas e comunicação institucional

Dados que podem ser tratados: identificação, contato, inscrição profissional, presença, certificação, preferências, imagem, voz, currículo e informações fornecidas em pesquisas.

Para que são usados: organizar eventos e atividades educativas, emitir certificados, divulgar ações institucionais, realizar pesquisas e estatísticas, registrar a memória institucional e encaminhar comunicações relacionadas.

Fundamentos principais: execução de atividade institucional e de serviço solicitado, consentimento quando houver escolha real ou uso facultativo de imagem e comunicação, legítimo interesse após avaliação e realização de estudos com salvaguardas.

Acesso e compartilhamento: equipe de eventos e comunicação, palestrantes, plataformas de transmissão, fornecedores de inscrição e certificação, instituições parceiras e público, quando houver divulgação legitimamente prevista.

Quando um evento for gravado ou fotografado, o CRM-PR deverá informar previamente as finalidades e as formas de divulgação. Registros gerais do ambiente e da atividade podem receber tratamento distinto de depoimentos, retratos destacados ou campanhas, que podem exigir autorização específica.

6.11 Ambientes digitais, autenticação, registros de acesso e cookies

Dados que podem ser tratados: endereço IP, data e hora, navegador, dispositivo, páginas acessadas, registros de autenticação, eventos de segurança, identificadores e cookies.

Para que são usados: permitir o funcionamento do site e dos serviços, autenticar usuários, manter sessões, prevenir fraude, investigar falhas, proteger sistemas, produzir estatísticas e melhorar a experiência digital.

Fundamentos principais: cumprimento de obrigações legais relacionadas a registros, execução de serviços solicitados, prevenção à fraude e segurança, legítimo interesse após avaliação e consentimento para tecnologias não essenciais quando exigido.

Acesso e compartilhamento: equipe de tecnologia, fornecedores de hospedagem, suporte, autenticação, análise e segurança. A relação atualizada de cookies e terceiros deverá constar em aviso específico.

6.12 Segurança física, controle de acesso e CFTV

Dados que podem ser tratados: imagem, data, hora, local de circulação, registros de entrada e saída e identificação de visitantes, quando utilizada.

Para que são usados: proteger pessoas, instalações, documentos e patrimônio, controlar acessos, prevenir e apurar incidentes e exercer direitos em procedimentos administrativos ou judiciais.

Fundamentos principais: exercício regular de direitos, segurança de pessoas e instalações e legítimo interesse institucional, quando cabível e precedido de avaliação.

Acesso e compartilhamento: acesso restrito às áreas responsáveis pela segurança e apuração; prestadores de vigilância e manutenção; autoridades competentes, quando houver obrigação ou necessidade formalizada.

As áreas monitoradas devem possuir sinalização visível e aviso específico. Câmeras não devem ser instaladas em locais de expectativa elevada de privacidade. O prazo de retenção das imagens será definido conforme necessidade, capacidade técnica, riscos e procedimentos de preservação de prova.

7. Bases legais utilizadas

A base legal depende da finalidade e da categoria de dado. O CRM-PR poderá utilizar, conforme o caso:

Cumprimento de obrigação legal ou regulatória: para registros profissionais, fiscalização, processos éticos, transparência, gestão documental, pessoal, finanças, contratos e outras atribuições obrigatórias.

Finalidade pública e execução de competências legais: como regra geral para o tratamento pelo CRM-PR, observados os arts. 23 e 26 da LGPD e a legislação do sistema CFM/CRMs.

Tratamento e uso compartilhado para execução de políticas públicas: quando houver previsão em lei ou regulamento e necessidade demonstrada.

Exercício regular de direitos: em contratos, processos administrativos, judiciais, arbitrais ou extrajudiciais, inclusive com dados sensíveis.

Execução de contrato ou de procedimentos preliminares: em relações de trabalho, fornecimento, prestação de serviços, inscrições facultativas e outros vínculos contratuais.

Prevenção à fraude e segurança: especialmente em identificação e autenticação eletrônica, inclusive com biometria quando indispensável e proporcional.

Proteção da vida ou da incolumidade física: em situações concretas de risco.

Tutela da saúde: apenas quando o tratamento ocorrer nos limites legais por profissional de saúde, serviço de saúde ou autoridade sanitária.

Legítimo interesse: em atividades de apoio nas quais essa base seja juridicamente adequada, após avaliação da necessidade, das expectativas do titular, dos riscos e das salvaguardas. Essa base não substitui competências ou obrigações legais.

Consentimento: para finalidades facultativas, específicas e destacadas, quando o titular puder recusar sem perder serviço ou direito obrigatório. O consentimento pode ser revogado, sem afetar os tratamentos anteriores realizados de forma legítima.

> **Sem autorizações genéricas**
> A assinatura em formulários de atendimento ou denúncia pode registrar a ciência do aviso de privacidade, mas não funciona como consentimento genérico nem permite tratamentos incompatíveis com a finalidade informada.

8. Dados sensíveis, crianças e adolescentes

8.1 Dados pessoais sensíveis

O CRM-PR pode receber dados sensíveis em registros, fiscalizações, denúncias, processos, gestão de pessoas e outras atividades. Esses dados exigem necessidade demonstrada, acesso limitado, compartilhamento restrito e medidas de segurança compatíveis com o risco.

Prontuários e documentos clínicos devem ser solicitados, acessados e mantidos apenas na extensão necessária à atividade. Sempre que possível e sem prejudicar a prova ou o dever legal, dados de terceiros sem relação com o caso devem ser ocultados, separados ou ter acesso restringido.

8.2 Crianças e adolescentes

Dados de crianças e adolescentes podem aparecer, por exemplo, em prontuários, denúncias, fiscalizações, eventos, benefícios de dependentes ou processos judiciais. O tratamento deve observar e fazer prevalecer o melhor interesse da criança ou do adolescente, com informação adequada à sua compreensão e salvaguardas proporcionais à vulnerabilidade.

As bases legais dos arts. 7º e 11 da LGPD podem ser utilizadas quando adequadas ao caso, sem reduzir a proteção especial do art. 14. O consentimento do responsável será solicitado quando essa for a base juridicamente aplicável, mas não será usado para impedir o cumprimento de obrigação legal, a proteção do titular ou a apuração institucional legítima.

9. Compartilhamento, operadores e transferências internacionais

9.1 Quando os dados podem ser compartilhados

O CRM-PR pode compartilhar dados quando isso for necessário à finalidade informada e houver fundamento jurídico. Entre os possíveis destinatários estão:

- CFM e outros Conselhos Regionais de Medicina;
- órgãos e entidades públicas, autoridades administrativas, órgãos de controle, Ministério Público, Judiciário e autoridades policiais;

- instituições de saúde, ensino ou outras entidades relacionadas à instrução de procedimentos;
- instituições financeiras, meios de pagamento, serviços postais e de cobrança;
- fornecedores de sistemas, nuvem, hospedagem, suporte, segurança, atendimento, eventos, benefícios, saúde ocupacional e outros serviços;
- partes, procuradores, advogados, peritos, testemunhas e sujeitos processuais, nos limites do procedimento;
- sociedade, quando houver dever de publicação ou atendimento legítimo à transparência pública.

O CRM-PR não vende dados pessoais nem os fornece para publicidade comercial de terceiros.

9.2 Papéis dos agentes

O CFM, outros CRMs e órgãos públicos não serão tratados automaticamente como cocontroladores. Cada entidade poderá atuar como controlador independente, destinatário, operador ou controlador conjunto, conforme quem decide a finalidade e os elementos essenciais do tratamento em cada fluxo. As responsabilidades devem ser definidas em normas, convênios, contratos ou outros instrumentos adequados.

Prestadores que tratem dados em nome do CRM-PR devem receber instruções, limitar o uso às finalidades contratadas, manter confidencialidade, adotar medidas de segurança, auxiliar no atendimento de direitos e comunicar incidentes sem demora indevida.

9.3 Transferência internacional

Alguns serviços de tecnologia podem envolver armazenamento, suporte remoto ou acesso a dados fora do Brasil. A transferência internacional somente ocorrerá quando houver necessidade e um mecanismo admitido pela LGPD e pela regulamentação da ANPD, como decisão de adequação, cláusulas-padrão, garantias contratuais ou outra hipótese legal aplicável.

Antes da contratação ou renovação de serviço que possa envolver transferência internacional, o CRM-PR deverá avaliar os países envolvidos, os prestadores, as categorias de dados, os riscos, as medidas de segurança e as garantias jurídicas.

10. Transparência pública e proteção de dados

O CRM-PR está sujeito a deveres de publicidade, transparência e acesso à informação. A LGPD não elimina esses deveres, e a Lei de Acesso à Informação não autoriza divulgação irrestrita de dados pessoais. As duas normas devem ser aplicadas de forma coordenada.

Antes de publicar ou fornecer documento com dados pessoais, o CRM-PR deve avaliar:

- a existência de dever legal de publicidade ou de interesse público na divulgação;
- a pertinência dos dados para a finalidade de transparência;
- a possibilidade de ocultar CPF, endereço, contato, assinatura, dados bancários, informações de saúde e dados de terceiros;
- a existência de sigilo processual, profissional, comercial, fiscal ou de outra natureza;
- os riscos de uso indevido, discriminação, fraude ou exposição desnecessária;
- a possibilidade de fornecer acesso parcial, certidão, extrato ou versão anonimizada.

Informações profissionais cuja publicidade seja necessária à segurança da sociedade e ao exercício regular da medicina poderão ser divulgadas nos limites das normas aplicáveis. Dados pessoais constantes de atos públicos não devem ser reutilizados para finalidades incompatíveis com o contexto da publicação.

11. Segurança da informação e incidentes

11.1 Medidas de segurança

O CRM-PR adota medidas técnicas e administrativas compatíveis com a natureza dos dados, o volume de tratamento, o estado da tecnologia e os riscos envolvidos. Essas medidas podem incluir:

- gestão de identidades, perfis e permissões de acesso;

- deveres de confidencialidade e responsabilização por uso indevido;
- registro e monitoramento de eventos de segurança, quando tecnicamente disponível e pertinente;
- cópias de segurança, continuidade, atualização e proteção de sistemas;
- controle de acesso físico e proteção de documentos;
- segurança no desenvolvimento, aquisição e contratação de soluções;
- avaliação de fornecedores e cláusulas contratuais de proteção de dados;
- capacitação periódica de conselheiros, empregados, colaboradores e prestadores;
- avaliação de riscos e relatórios de impacto quando o tratamento puder gerar alto risco.

Nenhum sistema é imune a falhas. A obrigação do CRM-PR é adotar medidas adequadas, proporcionais, verificáveis e atualizadas, sem prometer segurança absoluta.

11.2 Incidentes de segurança

Ao identificar suspeita ou confirmação de incidente envolvendo dados pessoais, o CRM-PR deverá acionar o fluxo interno de resposta para:

- conter o evento e preservar evidências;
- identificar sistemas, dados e titulares afetados;
- avaliar natureza, extensão, causas, riscos e danos possíveis;
- corrigir a vulnerabilidade e mitigar efeitos;
- registrar as decisões e as medidas adotadas;
- comunicar a ANPD e os titulares quando o incidente puder acarretar risco ou dano relevante, nos termos da regulamentação aplicável;
- acompanhar medidas posteriores e revisar controles.

> **Como comunicar um incidente**
> Empregados, conselheiros, colaboradores e prestadores devem informar imediatamente qualquer suspeita de perda, envio ao destinatário errado, acesso indevido, fraude, malware, exposição de documento ou falha de sistema pelo canal interno definido no Plano de Resposta a Incidentes. O canal público para titulares é dpo@crmpr.org.br.

12. Retenção, eliminação e preservação documental

Os dados serão conservados pelo tempo necessário à finalidade e pelos prazos decorrentes da legislação, das normas processuais, das obrigações de prestação de contas, da prescrição, da tabela de temporalidade e da política de gestão documental.

A definição do prazo considera:

- a finalidade que justificou a coleta;
- a duração do serviço, vínculo, processo ou contrato;
- os prazos administrativos, processuais, fiscais, trabalhistas e de controle;
- a necessidade de exercício regular de direitos e preservação de provas;
- a destinação arquivística e o valor histórico, probatório ou informativo do documento;
- os riscos e custos de conservação;
- a possibilidade de anonimização, restrição de acesso ou eliminação segura.

Documentos públicos, processos ético-profissionais, registros profissionais e outros acervos podem estar sujeitos a guarda prolongada ou permanente. Por isso, a eliminação solicitada pelo titular não é automática. Quando o dado puder ser eliminado, o descarte deve impedir reconstrução ou acesso indevido, observadas as limitações técnicas razoáveis e os ciclos de cópia de segurança.

A política pública não substitui a tabela de temporalidade. Os prazos específicos deverão ser mantidos em instrumento de gestão documental validado pelas áreas competentes.

13. Direitos dos titulares e atendimento

13.1 Direitos

Nos termos da LGPD, o titular pode requerer, conforme a situação:

- confirmação da existência de tratamento;
- acesso aos dados;
- correção de dados incompletos, inexatos ou desatualizados;
- anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade;
- informação sobre entidades com as quais houve uso compartilhado;
- informação sobre a possibilidade de negar consentimento e suas consequências;
- revogação do consentimento e eliminação dos dados tratados com base nele, quando cabível;
- oposição a tratamento realizado com dispensa de consentimento, em caso de descumprimento da LGPD;
- revisão e informações sobre decisões tomadas unicamente por tratamento automatizado que afetem seus interesses, se utilizadas;
- peticionamento perante a ANPD e defesa de direitos em juízo ou por outros meios legais.

13.2 Como fazer o pedido

O pedido pode ser enviado ao encarregado pelo e-mail dpo@crmpr.org.br. Para proteger o próprio titular e evitar fraude, o CRM-PR poderá solicitar comprovação de identidade, representação e informações suficientes para localizar o tratamento, sem exigir dados desproporcionais.

O requerimento é gratuito. A confirmação simplificada ou o acesso poderá ser fornecido imediatamente quando possível; a declaração clara e completa será fornecida no prazo legal aplicável, ressalvadas hipóteses de complexidade, necessidade de complementação, sigilo ou regulamentação específica. Se não puder adotar a providência, o CRM-PR apresentará as razões de fato ou de direito.

13.3 Limites e coordenação com outros regimes

Os direitos do titular não são absolutos. Um pedido poderá ser limitado ou indeferido, de forma fundamentada, quando necessário para:

- cumprir obrigação legal, regulatória, processual ou arquivística;
- preservar sindicância, processo ético-profissional, fiscalização, auditoria ou investigação;
- proteger direitos, dados e sigilos de outras pessoas;
- manter a integridade, a autenticidade e o contexto de documentos e provas;
- exercer direitos em processo judicial, administrativo ou extrajudicial;
- cumprir dever de transparência ou preservar informação de interesse público;
- respeitar limitações técnicas comprovadas ou evitar esforço desproporcional, sem afastar medidas alternativas razoáveis.

O pedido de acesso pela LGPD não substitui vista ou cópia de autos, pedido pela Lei de Acesso à Informação, retificação cadastral, recurso administrativo ou direito processual específico. O CRM-PR indicará o canal adequado quando a pretensão tiver natureza diferente.

14. Atualizações, vigência e controle de versões

Esta política entra em vigor após aprovação e publicação institucional. Poderá ser atualizada para refletir mudanças legais, regulatórias, tecnológicas ou operacionais. Alterações relevantes serão identificadas pelo número da versão e pela data, com síntese no histórico de alterações.

A versão vigente deverá permanecer disponível em privacidade.crmpr.org.br. Cópias impressas poderão ser consultadas na sede e nas representações. Em caso de divergência entre uma cópia impressa desatualizada e a versão eletrônica vigente, prevalecerá a versão eletrônica, sem prejuízo da análise do caso concreto.

Versão	Data	Alteração	Situação
0.1	29/07/2026	Primeira minuta completa para validação interna	Não publicada
0.2	29/07/2026	Primeira minuta complete, aprovada para publicação no Portal da Transparência	Publicada

15. Referências normativas essenciais

- Constituição Federal, especialmente direitos à intimidade, à privacidade, à proteção de dados pessoais, ao acesso à informação e os princípios da Administração Pública.
- Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais, com as alterações posteriores, inclusive a Lei nº 15.352/2026.
- Lei nº 12.527/2011 - Lei de Acesso à Informação.
- Lei nº 9.784/1999 - Processo Administrativo Federal.
- Lei nº 13.460/2017 - Participação, proteção e defesa dos direitos do usuário dos serviços públicos.
- Lei nº 14.129/2021 - Governo Digital.
- Lei nº 12.965/2014 e Decreto nº 8.771/2016 - Marco Civil da Internet e regulamentação.
- Lei nº 8.159/1991 e normas arquivísticas aplicáveis à gestão e preservação de documentos públicos.
- Lei nº 3.268/1957 e Decreto nº 44.045/1958, com alterações - Conselhos de Medicina.
- Resolução CFM nº 2.306/2022 - Código de Processo Ético-Profissional, enquanto vigente.
- Instruções normativas e atos do CFM e do CRM-PR sobre privacidade, segurança da informação e proteção de dados, naquilo que forem compatíveis com a legislação posterior.
- Resolução CD/ANPD nº 15/2024 - Comunicação de Incidente de Segurança.
- Resolução CD/ANPD nº 18/2024 - Atuação do encarregado pelo tratamento de dados pessoais.
- Resolução CD/ANPD nº 19/2024, com alterações - Transferência Internacional de Dados.
- Enunciado CD/ANPD nº 1/2023 - Tratamento de dados de crianças e adolescentes.
- Guias e orientações vigentes da ANPD, especialmente sobre tratamento de dados pelo Poder Público, agentes de tratamento e legítimo interesse.

Outras normas setoriais, processuais, trabalhistas, fiscais, contratuais, de transparência, controle e segurança podem ser aplicáveis conforme a atividade.