

DIREITO, PRIVACIDADE E TECNOLOGIA EM SAÚDE

Governança de Dados, Consentimento Auditável e Integridade Probatória na **Publicidade Médica.**

Como a nova publicidade médica pode se beneficiar do consentimento auditável, cadeia de custódia digital e arquitetura de confiança para proteger pacientes, médicos e instituições de saúde.

Dr. Júlio Cesar Garcia

Advogado · Professor · Pesquisador



EDIÇÃO 01 · 2026

Governança de Dados, Consentimento Auditável e Integridade Probatória na Publicidade Médica.



DR. JÚLIO CESAR GARCIA



● EDIÇÃO 01 · 2026

AUTOR

Dr. Júlio Cesar Garcia
Advogado, OAB/PR 35.946 · Pós-doutor, Levin College of Law, University of Florida ·
Doutor pela UFPR · Mestre pela UEM · Professor do PPGD UNIVEL · Coordenador do
ITDS · Editor da REDIR.

EDIÇÃO

Versão-base 1.0, maio de 2026
Versão revisada para apreciação editorial, maio de 2026

DIREITOS

Este material destina-se a apreciação editorial e referência institucional. A
reprodução parcial é permitida desde que citada a fonte. Toda referência
normativa apresentada deve ser verificada pelo usuário em sua versão oficial
vigente.

Contato: julio.garcia@univel.br

Sumário

Resumo executivo	5
Teses centrais	7
I PARTE I O problema da publicidade médica contemporânea	8
II PARTE II Fundamentação jurídica e ética	21
III PARTE III Da autorização informal ao consentimento auditável	29
IV PARTE IV Arquitetura de prova e integridade	34
V PARTE V Ciclo de vida, operação e riscos	46
VI PARTE VI Governança, métricas e síntese	56
A–D Anexos Matriz normativa, requisitos, glossário e checklist	63
Referências	72
Sobre o autor	74



EXECUTIVE

Resumo executivo

A publicidade médica brasileira atravessa uma mudança relevante. Depois de anos em que a exposição pública da atividade médica foi interpretada sob regime mais restritivo, a Resolução CFM nº 2.336/2023 passou a disciplinar, sob condições, novas formas de comunicação institucional, educativa e reputacional. Imagens, relatos, repostagens, demonstrações de resultados e conteúdos de bastidores profissionais passaram a integrar um campo regulado no qual a pergunta decisiva não é apenas se algo pode ser publicado, mas como a publicação pode ser contextualizada, controlada e defendida depois.

Essa mudança criou oportunidade, mas também revelou fragilidade. A rotina de clínicas e consultórios ainda costuma tratar consentimento de modo informal: mensagem de aplicativo, print de tela, resposta breve, autorização verbal, termo digitalizado ou planilha mantida pela equipe de marketing. Essas soluções podem parecer suficientes no cotidiano, mas se tornam frágeis quando o conteúdo envolve dados de saúde, imagem, intimidade, assimetria informacional, expectativa de resultado, vulnerabilidade e exposição pública.

O ponto central deste obra é que a autorização do paciente para uso de imagem, relato ou depoimento não deve ser tratada como episódio isolado. Ela deve ser compreendida como evento jurídico e técnico inserido em um ciclo de vida. Esse ciclo começa na informação clara, passa pelo consentimento livre, específico, destacado e granular, depende de autenticação razoável, exige preservação de contexto e integridade, continua durante o uso do conteúdo, permanece auditável enquanto houver finalidade legítima e deve admitir revogação efetiva.

Há, porém, uma premissa anterior: consentimento não converte em ética uma publicação que a deontologia médica veda. O Código de Ética Médica e a Resolução CFM nº 2.336/2023 impõem limites próprios de sigilo, sobriedade, anonimato, veracidade e não promessa de resultado. Em especial, casos clínicos identificáveis, pacientes reconhecíveis, imagens de procedimentos que

identifiquem o paciente, manipulações visuais e promessas explícitas ou implícitas de resultado exigem cautela reforçada. O consentimento auditável é requisito de governança quando o uso for juridicamente e eticamente admissível; não é licença para exposição indevida.

A tecnologia pode contribuir de modo relevante, desde que compreendida sem exageros. Magic Link fortalece a vinculação entre canal, ato de aceite e registro temporal, mas não prova identidade jurídica plena. Hash criptográfico demonstra integridade desde o momento do cálculo, mas não valida consentimento mal informado. Timestamp reforça anterioridade, mas depende de fonte temporal confiável. Blockchain pode preservar prova criptográfica pública, mas não deve armazenar dados sensíveis nem transformar publicação antiética em lícita. Inteligência artificial pode apoiar triagem, revisão e auditoria, mas não deve publicar automaticamente, fabricar prova social ou alterar evidência clínica sem registro, transparência e supervisão humana qualificada.

A publicidade médica verificável exige a combinação de seis dimensões: proteção de dados pessoais sensíveis, ética profissional, consentimento granular, prova digital, segurança da informação e governança operacional. A confiança não nasce apenas daquilo que é comunicado ao público. Ela nasce também da capacidade institucional de demonstrar que a comunicação respeitou o paciente, preservou a integridade do conteúdo, observou limites éticos e manteve controle sobre o uso autorizado.

Teses centrais desta obra.

Novas proposições que estruturam o argumento e o desdobramento técnico dos capítulos seguintes.

- 01 Publicidade médica com imagem, relato ou depoimento de paciente, quando envolver identificação direta ou indireta, tende a configurar tratamento de dado pessoal sensível.

- 02 A finalidade assistencial não autoriza, por si só, finalidade publicitária, institucional ou reputacional.

- 03 A análise ética vem antes da análise probatória: nem todo conteúdo consentido é publicável.

- 04 Quando o uso for admissível, o consentimento em saúde deve ser específico, destacado, granular, informado, livre e revogável.

- 05 Print é indício útil, mas não substitui cadeia probatória estruturada.

- 06 Hash, timestamp e blockchain reforçam integridade e anterioridade, mas não validam consentimento juridicamente defeituoso nem conteúdo eticamente inadequado.

- 07 Inteligência artificial pode apoiar revisão, triagem e auditoria, mas exige transparência ativa, preservação do original e supervisão humana qualificada.

- 08 Governança contratual e operacional é condição para reduzir responsabilidade em cadeias com médicos, clínicas, fornecedores, plataformas e agências.

- 09 A confiança institucional depende da capacidade de demonstrar, e não apenas afirmar, que a comunicação respeitou autonomia, sigilo, ética médica e proteção de dados.

PARTE



O problema da publicidade médica contemporânea.



CAPÍTULO

1

O novo problema da publicidade médica.

Durante muito tempo, o debate sobre publicidade médica concentrou-se em limites de exposição: o que o médico pode divulgar, que tipo de imagem pode aparecer, como evitar promessa de resultado, quando a comunicação se transforma em sensacionalismo e quais informações profissionais podem ser apresentadas ao público. Esse debate continua indispensável, mas já não é suficiente.

A publicidade médica contemporânea ocorre em ambiente de circulação acelerada. Um elogio publicado por paciente em rede social pode ser repostado em segundos. Uma fotografia clínica pode circular entre equipe médica, agência, editor, gestor de tráfego e profissional de comunicação. Um vídeo educativo pode ser usado em site, rede social, mensagem, aula, congresso e material institucional. Um relato inicialmente escrito como agradecimento pode se transformar em prova social, peça reputacional ou argumento de autoridade. Cada deslocamento de contexto produz uma nova pergunta: o paciente autorizou aquele uso específico e esse uso é eticamente admissível?

A resposta informal costuma ser “sim, há um print”. O problema é que o print mostra apenas a superfície de uma comunicação. Ele não demonstra, por si, a identidade de quem operava o dispositivo, a integridade da conversa, a versão do termo apresentado, o escopo autorizado, a finalidade, o canal, o prazo, a possibilidade de revogação ou a correspondência entre conteúdo autorizado e conteúdo publicado. Ele registra aparência visual, mas raramente preserva história completa.



A Resolução CFM nº 2.336/2023 modernizou a publicidade médica, mas não instituiu autorização geral para exploração reputacional da experiência do paciente. A abertura ética é condicionada por sobriedade, veracidade, finalidade educativa quando aplicável, preservação de privacidade, vedação a promessa de resultado, respeito ao anonimato quando exigível e manutenção da responsabilidade profissional. Aquilo que é condicionado precisa ser demonstrável.

A publicidade médica, nesse cenário, deixa de ser apenas comunicação. Ela passa a ser operação de tratamento de dados sensíveis em ambiente público ou potencialmente público. O paciente não é matéria-prima de marketing. É titular de dados, sujeito de direitos, pessoa em relação de confiança com o médico e, muitas vezes, indivíduo em situação de vulnerabilidade. A imagem de um procedimento, uma cicatriz, um relato de dor superada, a menção a uma cirurgia ou a avaliação de atendimento podem revelar condição clínica, especialidade procurada, expectativa terapêutica e elementos íntimos da vida pessoal.

O problema central da nova publicidade médica não é apenas editorial. É metodológico e ético. Antes de perguntar “como provar que o paciente autorizou?”, a instituição deve perguntar “este conteúdo pode ser publicado?”. Quando a resposta for positiva, deve haver método para provar que a circulação foi autorizada, limitada, íntegra, contextualizada, revogável e auditável.

CAPÍTULO

2

Publicidade médica como tratamento de dados sensíveis.

A Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, classifica dados referentes à saúde como dados pessoais sensíveis. Essa classificação não depende de o dado estar dentro de um prontuário. O contexto pode tornar a informação sensível. Uma imagem de antes e depois, uma cicatriz, uma legenda associada a procedimento, um depoimento sobre tratamento, uma avaliação de atendimento em determinada especialidade ou uma publicação que permita inferir condição de saúde podem estar no campo dos dados sensíveis.

Na rotina de comunicação, há tendência de tratar a publicidade médica como extensão natural do atendimento. A clínica possui a imagem, o paciente foi atendido, o resultado parece favorável, o relato foi positivo, a equipe gostou do conteúdo e surge a ideia de publicar. Mas a finalidade assistencial não autoriza automaticamente a finalidade publicitária. Imagem coletada para cuidado, registro clínico ou acompanhamento não pode ser convertida em material de comunicação apenas porque está disponível. O princípio da finalidade exige propósito legítimo, específico, explícito e informado, sem tratamento posterior incompatível com aquele que justificou a coleta original.

Quando o dado é sensível e o uso publicitário é admissível sob a ética médica, a base prudencial mais defensável tende a ser o consentimento específico e destacado do titular, nos termos do art. 11 da LGPD. Essa conclusão não deve ser lida como exclusão absoluta de controvérsias doutrinárias. Há discussões sobre hipóteses específicas de exercício regular de direitos, tutela da saúde, pesquisa ou obrigação regulatória. Entretanto, para uso reputacional, institucional ou publicitário de conteúdo identificável de paciente, a recomendação institucionalmente mais segura é tratar o consentimento como requisito central, com informação clara, separação de finalidade e possibilidade real de revogação.



A LGPD atribui relevância especial ao ônus de demonstrar a conformidade do consentimento. Em eventual questionamento, não basta afirmar que o paciente autorizou. A clínica ou profissional deve demonstrar qual informação foi prestada, qual termo foi apresentado, em qual versão, para qual finalidade, por qual canal, em que momento, com que escopos, vinculado a qual conteúdo, por quanto tempo e com qual mecanismo de revogação.

A demonstração exige mais do que documento estático. Exige conjunto de evidências. O termo é apenas uma parte. Também importam logs, canal, vínculo ao titular ou representante, versão do conteúdo, status de revogação, histórico de uso, controles de acesso e preservação de integridade. Quando esses elementos estão dispersos, a defesa institucional passa a depender de reconstruções posteriores, justamente quando a prova já deveria estar preservada.



CASO ILUSTRATIVO

Uma clínica capta imagem de paciente em pós-operatório com finalidade assistencial. Meses depois, a equipe de marketing seleciona a mesma imagem para campanha em rede social. A imagem está disponível, mas a disponibilidade não substitui consentimento específico para publicização nem análise ética sobre anonimato, finalidade, contexto e promessa de resultado.

CAPÍTULO

3

Prova social médica e assimetria informacional.

A prova social tem enorme força na formação de confiança. Pessoas procuram sinais de experiência alheia antes de escolher um serviço, especialmente quando a decisão envolve risco, intimidade ou expectativa de melhora. Na medicina, essa dinâmica é ainda mais intensa. O paciente avalia competência, segurança, reputação, empatia, clareza e possibilidade de resultado, sem dispor do mesmo repertório técnico do profissional.

Prova social médica não é equivalente à prova social de outros mercados. Um comentário sobre restaurante ou hospedagem não carrega o mesmo peso ético de um depoimento sobre cirurgia, fertilidade, estética, dor, saúde mental, diagnóstico ou recuperação funcional. A medicina envolve assimetria informacional e relação fiduciária. O paciente confia no médico porque não domina o mesmo conhecimento técnico. Essa confiança é necessária ao cuidado, mas pode gerar vulnerabilidade no momento de autorizar exposição pública.

A assimetria aparece de várias formas. O paciente pode acreditar que negar autorização prejudicará sua relação com a equipe. Pode sentir gratidão e concordar com algo que não compreendeu. Pode aceitar uso de imagem em pós-operatório, dor, sedação leve ou fragilidade emocional. Pode não distinguir uso em prontuário, aula, congresso, site institucional, rede social orgânica e anúncio patrocinado. Pode autorizar uma fotografia para contexto educativo e, depois, vê-la em peça reputacional. A liberdade formal do consentimento pode ocultar vulnerabilidade real.



Por isso, consentimento em publicidade médica deve ser desenhado para reduzir pressão, não para capturar aceite a qualquer custo. A linguagem deve ser neutra. O fluxo deve separar atendimento de autorização publicitária. A recusa deve ser simples e sem consequência assistencial. A revogação deve ser acessível. O termo deve informar finalidade, canal, prazo, escopo, possibilidade de edição e limites de retirada. A oferta de desconto, vantagem, compensação ou tratamento privilegiado em troca de autorização de imagem tende a comprometer a liberdade do consentimento e deve ser evitada.

Conteúdo espontaneamente publicado pelo paciente também exige cuidado. O fato de um elogio estar público não significa que a clínica possa reaproveitá-lo livremente. A repostagem institucional altera contexto, finalidade, alcance e responsabilidade. Para fins éticos, passa a ser comunicação do médico ou do estabelecimento; para fins de proteção de dados, pode configurar novo tratamento; para fins consumeristas, pode influenciar decisão de outros pacientes.



CASO ILUSTRATIVO

Um paciente publica elogio detalhado ao tratamento recebido, com menção a procedimento e resultado. A clínica deseja repostar para ampliar alcance. Embora o conteúdo tenha sido publicado pelo paciente, a repostagem em canal institucional exige curadoria ética e, quando houver dado sensível identificável, autorização específica para aquele novo contexto.



CAPÍTULO

4

Sujeitos vulneráveis, terceiros e limites éticos.

A publicidade médica envolvendo pacientes exige atenção especial quando há sujeitos vulneráveis ou terceiros incidentais. Vulnerabilidade pode decorrer da idade, condição de saúde, estado emocional, capacidade de compreensão, dependência assistencial, deficiência, contexto de exposição ou relação de confiança com a equipe.

Crianças e adolescentes exigem proteção reforçada, mas não uniforme. Para crianças, a LGPD exige consentimento específico e em destaque por pelo menos um dos pais ou responsável legal, ressalvadas hipóteses legais específicas. Para adolescentes, a análise deve considerar autonomia progressiva, proteção integral, melhor interesse, capacidade de compreensão, contexto da exposição e participação informada do próprio titular sempre que compatível com sua maturidade. O Enunciado CD/ANPD nº 1/2023 reconhece a possibilidade de tratamento de dados de crianças e adolescentes com base nas hipóteses legais dos arts. 7º e 11 da LGPD, desde que observado e prevalecente o melhor interesse.

Quando a exposição ocorre em ambiente digital, o Estatuto Digital da Criança e do Adolescente, Lei nº 15.211/2025, e sua regulamentação reforçam a lógica de responsabilidade compartilhada e proteção em produtos e serviços digitais acessados por crianças e adolescentes. Em publicidade médica, isso não substitui a LGPD nem o ECA, mas acrescenta uma camada de cautela sobre circulação, alcance, aferição de idade, publicidade comercial, plataformas e riscos persistentes de exposição.



A autorização parental não deve ser tratada como cheque em branco. Uma publicação de criança em contexto clínico pode produzir efeitos futuros de constrangimento, estigmatização, identificação indesejada ou exposição permanente. A pergunta ética não é apenas “o responsável autorizou?”, mas “a exposição preserva o melhor interesse da criança ou adolescente e respeita sua condição peculiar de desenvolvimento?”.

Pessoas com deficiência, transtornos cognitivos, limitações temporárias de discernimento ou flutuação de capacidade exigem cuidado equivalente. O Estatuto da Pessoa com Deficiência reforça autonomia, acessibilidade e tomada de decisão apoiada. Isso significa que o consentimento deve ser compreensível, acessível e compatível com a situação concreta, sem presumir incapacidade nem ignorar necessidades de apoio.

Há ainda vulnerabilidade aguda. Pacientes em pós-operatório imediato, dor intensa, luto, diagnóstico recente, sedação, ansiedade elevada ou forte dependência emocional podem não estar em condição adequada para consentir com uso publicitário. Nesses casos, a boa prática é evitar a coleta naquele momento ou exigir reconfirmação posterior em ambiente neutro.

Terceiros incidentais também importam. Acompanhantes, familiares, cuidadores, profissionais, outros pacientes, vozes ao fundo, reflexos, tatuagens, prontuários visíveis, telas e objetos pessoais podem identificar pessoas que não participaram do consentimento. A governança de publicidade médica deve prever revisão editorial, supressão de elementos identificadores, anonimização robusta ou autorização específica quando terceiros forem reconhecíveis.



CASO ILUSTRATIVO

Um responsável legal autoriza uso de imagem de criança em campanha educativa. Anos depois, a criança, já adolescente, manifesta oposição à continuidade da exposição. Ainda que a autorização originária tenha sido formalmente colhida, o melhor interesse da pessoa em desenvolvimento exige reavaliação da continuidade do uso, retirada dos canais sob controle institucional e registro da nova manifestação.



CAPÍTULO

5

Telessaúde, comunicação assistencial e captura remota.

A expansão da telessaúde ampliou a fronteira entre cuidado, comunicação e exposição. Consultas por vídeo, mensagens entre paciente e equipe, áudios, fotografias clínicas enviadas por aplicativo, prints de conversas e gravações de atendimento integram um ecossistema que mistura prontuário, comunicação assistencial e potencial material de divulgação.

O risco específico é a confusão de finalidades. Uma imagem enviada pelo paciente para avaliação clínica integra contexto assistencial, está protegida por sigilo médico e pelo regime de dados sensíveis da LGPD. Sua eventual utilização em material educativo, institucional ou reputacional exige nova finalidade, nova transparência, nova análise ética e consentimento específico quando o uso for admissível. O prontuário não é repositório de marketing.

Gravações de teleconsulta apresentam camada adicional. A gravação pode ser legítima quando atende a finalidade assistencial, de segurança ou obrigação regulatória, com transparência ao paciente. Mas a transformação dessa gravação em conteúdo de divulgação, ainda que parcial, editada ou com voz dissimulada, demanda autorização específica e ponderação rigorosa sobre sigilo, dignidade, contexto e risco de identificação. Trechos de atendimento real, mesmo sob alegação educativa, devem ser tratados com cautela extrema.

A captura remota também levanta questões de identidade e autoria. Quem enviou a fotografia é, de fato, o titular? O dispositivo está sob seu controle? O canal pertence ao paciente ou a familiar? O ambiente comporta consentimento livre? Um fluxo remoto deve combinar verificação razoável de identidade, contexto explícito de finalidade, registro técnico do canal e possibilidade de confirmação posterior, especialmente quando o conteúdo for sensível ou de alta exposição.



PONTO DE ATENÇÃO

Conteúdo gerado em ambiente assistencial remoto está protegido por sigilo e finalidade clínica. Sua conversão em conteúdo publicitário exige base legal autônoma, nova manifestação informada e segregação operacional entre cuidado e comunicação.



CAPÍTULO

6

Marketing de influência, publicidade patrocinada e plataformas digitais.

A publicidade médica contemporânea não circula apenas em perfis orgânicos. Ela aparece em campanhas patrocinadas, públicos semelhantes, remarketing, parcerias, anúncios segmentados, marketing de influência e métricas comerciais aplicadas a conteúdo de saúde.

Essa modalidade introduz risco específico. Plataformas digitais aplicam políticas próprias a conteúdo de saúde, frequentemente mais restritivas do que a comunicação orgânica. A depender do desenho do tratamento, da autonomia decisória, das instruções contratuais e da combinação de dados, pode haver responsabilidade compartilhada, controladoria conjunta ou atuação como operador/suboperador. O ponto prudencial é não presumir que a plataforma seja sempre neutra nem afirmar responsabilidade automática em todo cenário. O enquadramento depende do caso concreto.

A publicidade patrocinada altera percepção e alcance. Um anúncio que parece informação clínica neutra, mas é veiculado em formato comercial, pode caracterizar publicidade dissimulada. A identificação clara do caráter publicitário dialoga com o CDC, com a ética médica e com a confiança do paciente. Quando o conteúdo envolve depoimento ou imagem de paciente real, a exposição se intensifica pelo alcance algorítmico, pela segmentação, pela coleta indireta de dados de quem interage e pela ampliação temporal e geográfica da peça.

A segmentação merece atenção própria. Pixels de rastreamento, públicos personalizados, públicos semelhantes, remarketing e métricas comportamentais podem criar inferências sobre interesse em condição de saúde, procedimento, dor, especialidade médica ou vulnerabilidade. Mesmo quando a instituição não insere



diretamente categoria sensível na plataforma, a combinação entre conteúdo médico, comportamento de navegação e segmentação algorítmica pode gerar dados sensíveis por inferência.

O marketing de influência adiciona outra camada. Médicos influenciadores acumulam papéis: comunicador, prestador, formador de opinião, parceiro comercial e, em alguns contextos, agente vinculado a serviço público. A divulgação de produtos, técnicas, dispositivos, medicamentos, suplementos ou serviços exige clareza sobre vínculos, conflitos de interesse, base científica, sobriedade e ausência de promessa de resultado. A flexibilização regulatória não transforma o médico em garoto-propaganda.



CASO ILUSTRATIVO

Um depoimento textual colhido para uso em site institucional é inserido em campanha patrocinada segmentada por interesse em determinada condição clínica. A finalidade original era informativa, em canal próprio. A nova finalidade é comercial, com alcance ampliado e tratamento algorítmico. Trata-se de uso adicional, que exige consentimento específico para campanha patrocinada, revisão ética, prazo limitado e transparência publicitária.

PARTE



Fundamentação jurídica e
ética.

CAPÍTULO

7

A Resolução CFM nº 2.336/2023 e a diferença entre permissão, consentimento e prova.

A Resolução CFM nº 2.336/2023 representa marco na publicidade médica brasileira. Ela reconhece transformações sociais, tecnológicas e comunicacionais já em curso. Médicos e clínicas comunicam-se em redes sociais, produzem conteúdo educativo, apresentam estrutura de atendimento, explicam procedimentos, respondem dúvidas e constroem reputação em ambiente digital. A norma não ignora esse cenário; ela o regula.

A leitura correta da Resolução exige distinguir permissão ética, consentimento do titular e suficiência probatória. O fato de determinada prática ser permitida sob condições não significa que qualquer forma de execução seja adequada. A possibilidade de uso educativo de imagem não dispensa finalidade educativa, contexto, anonimato quando exigível, sobriedade e ausência de promessa de resultado. A possibilidade de repostar elogios não transforma todo depoimento em peça publicitária livre. A divulgação de resultados não autoriza edição enganosa, comparação abusiva ou indução de expectativa irreal.

O Código de Ética Médica reforça esse limite. Além do dever de sigilo, o art. 75 veda fazer referência a casos clínicos identificáveis ou exibir pacientes ou imagens que os tornem reconhecíveis em anúncios profissionais ou divulgação de assuntos médicos, mesmo com autorização do paciente. A Resolução CFM nº 2.336/2023, em seu art. 14, permite uso de imagem de pacientes ou bancos de imagens com finalidade educativa, mas veda imagem de procedimento que identifique o



paciente, veda edição, manipulação ou melhoramento das imagens e exige, quando as imagens forem de banco próprio do médico ou serviço, autorização, respeito ao pudor e privacidade e garantia de anonimato mesmo quando houver autorização.

Essa é a chave de leitura: consentimento é necessário, mas não suficiente. Um paciente pode consentir com publicação que, ainda assim, viole a ética médica. Pode autorizar imagem manipulada, mas a manipulação continuar inadequada. Pode aceitar depoimento entusiasmado, mas o conteúdo induzir promessa de resultado. Pode permitir exposição, mas a publicação comprometer anonimato, contexto, sobriedade ou dignidade.

A governança adequada precisa combinar consentimento e curadoria. O consentimento responde à autonomia do titular e ao regime de proteção de dados. A curadoria ética responde à responsabilidade do médico e da instituição. A decisão de publicar deve passar por avaliação humana sobre finalidade educativa, linguagem, imagem, edição, canal, legenda, recorrência, identificação do profissional, risco de interpretação equivocada, anonimato e aderência às normas do CFM.

Imagens comparativas exigem cuidado redobrado. Ângulo, iluminação, distância, postura, expressão, lente, fundo, maquiagem, edema, tempo de recuperação e edição podem alterar substancialmente a percepção do resultado. A publicação deve preservar contexto clínico, evitar promessa explícita ou implícita, registrar imagens originais, documentar edições permitidas e impedir tratamento visual que suavize cicatrizes, altere textura, simule melhora ou crie expectativa incompatível com a realidade médica.



PONTO DE ATENÇÃO

Permissão normativa não equivale a prova de licitude. Consentimento auditável não é autorização para violar anonimato, sigilo, sobriedade ou veracidade. A boa governança deve demonstrar também as razões pelas quais determinado conteúdo não foi publicado.



CAPÍTULO

8

LGPD, ANPD, CDC, direitos da personalidade e responsabilidade civil.

A publicidade médica envolvendo pacientes ocupa uma zona de interseção normativa. Não basta olhar para uma única regra. A prática envolve proteção de dados, ética médica, responsabilidade civil, direito do consumidor, direitos da personalidade, segurança da informação, contratos, prova digital e governança.

A LGPD fornece o eixo de proteção de dados. O art. 5º define dado pessoal, dado sensível, titular, controlador, operador e consentimento. O art. 6º estabelece princípios que funcionam como critérios de legitimidade. O art. 8º disciplina consentimento e ônus de prova. O art. 11 trata de dados sensíveis. O art. 14 protege crianças e adolescentes. O art. 16 disciplina hipóteses de conservação após término do tratamento. O art. 18 assegura direitos do titular. Os arts. 33 a 36 tratam de transferência internacional. O art. 42 disciplina responsabilidade e reparação de danos. O art. 46 exige medidas de segurança. O art. 48 trata de comunicação de incidentes. O art. 50 incentiva boas práticas e governança.

A ANPD, em 2026 estruturada como Agência Nacional de Proteção de Dados, desempenha papel central de orientação, regulamentação, fiscalização e sanção. A Resolução CD/ANPD nº 4/2023 disciplina dosimetria de sanções. A Resolução CD/ANPD nº 15/2024 disciplina comunicação de incidentes de segurança. A Resolução CD/ANPD nº 19/2024 disciplina transferência internacional de dados e mecanismos contratuais. O Enunciado CD/ANPD nº 1/2023 é referência relevante para tratamento de dados de crianças e adolescentes sob o critério do melhor interesse.



A dimensão da responsabilidade civil merece destaque. O art. 42 da LGPD impõe ao controlador e ao operador o dever de reparar dano patrimonial, moral, individual ou coletivo decorrente de tratamento em violação à lei. A solidariedade entre agentes depende da configuração legal: controladores diretamente envolvidos no tratamento danoso; operador que descumpra instruções lícitas do controlador ou atua além delas; ou participação juridicamente relevante no tratamento irregular. Não basta presença nominal na cadeia. É preciso examinar decisões, instruções, autonomia, contratos, segurança e nexos com o dano.

O Código de Defesa do Consumidor acrescenta camada própria. A publicidade médica dirigida ao público deve respeitar informação adequada, boa-fé, transparência e vedação a publicidade enganosa ou abusiva. Promessas implícitas de resultado, omissões relevantes, depoimentos descontextualizados e imagens que induzam expectativa irreal podem gerar risco consumerista, além de ético e regulatório.

Os direitos da personalidade, previstos no Código Civil, arts. 11 a 21, têm autonomia. Nome, imagem, honra, intimidade, privacidade e projeções post mortem não se esgotam na LGPD. A autorização para uso de imagem deve ser interpretada restritivamente e vinculada à finalidade informada. Um tratamento pode ter registro formal de consentimento e ainda assim violar dignidade ou imagem se executado de modo abusivo.

O sigilo profissional fecha o quadro normativo. O art. 154 do Código Penal tipifica revelação de segredo profissional sem justa causa. O Código de Ética Médica reforça a vedação. Em publicidade médica, o sigilo não cessa simplesmente porque o paciente autorizou determinado uso. O profissional permanece guardião de informações sensíveis e deve avaliar o que pode, o que deve e o que não deve ser exposto.



FINALIDADE	FUNDAMENTO OU BASE PRUDENCIAL	LÍMITE ESSENCIAL
Cuidado assistencial	Hipóteses do art. 11, II, da LGPD, conforme o caso, como tutela da saúde, obrigação legal/regulatória, proteção da vida ou exercício regular de direitos	Não autoriza, por si, uso publicitário
Uso publicitário ou reputacional de conteúdo de paciente	Consentimento específico, destacado, informado, granular e revogável, quando o uso for eticamente admissível	Não supera vedações éticas, anonimato e ausência de promessa de resultado
Retenção de registros de consentimento, uso e revogação	Art. 11, II, conforme o caso; art. 16; exercício regular de direitos; cumprimento de obrigação legal/regulatória; princípios de necessidade, segurança e responsabilização	Deve ser proporcional, segura, restrita e vinculada à finalidade probatória
Comunicação institucional sem dado de paciente	Pode admitir legítimo interesse ou execução de contrato, conforme contexto	Não deve servir para contornar consentimento em dado sensível
Transferência internacional	Arts. 33 a 36 da LGPD e Resolução CD/ANPD nº 19/2024	Exige mapeamento de fluxos, garantias e mecanismo válido



CAPÍTULO

9

Consentimento dinâmico em saúde e novas fontes de dados.

A literatura internacional sobre privacidade em saúde já apontava, antes da expansão contemporânea da publicidade médica em redes sociais, que dados de saúde deixaram de estar confinados a sistemas hospitalares tradicionais. Aplicativos, wearables, plataformas digitais, mensagens, avaliações, imagens enviadas por pacientes e interações online passaram a compor novas fontes de dados em saúde.

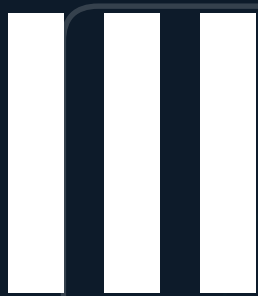
No contexto da publicidade médica, relatos, avaliações, mensagens, imagens e depoimentos funcionam como fontes emergentes de informação reputacional em saúde. Não são prontuário em sentido estrito, mas podem revelar condição clínica, procedimento, experiência assistencial, expectativa de resultado, relação com profissional e elementos de vulnerabilidade.

O consentimento tradicional, estático e amplo, responde mal a esse cenário. A autorização precisa ser dinâmica, não no sentido de instável, mas de acompanhável. O titular deve poder compreender, consultar e revogar. A instituição deve demonstrar histórico, escopos, uso, retirada e retenção probatória. O uso deve respeitar finalidade. A revogação deve produzir efeitos nos ambientes sob controle institucional. A preservação probatória deve ser distinguida da continuidade de exposição pública.

A literatura sobre consentimento dinâmico também revela um desafio de usabilidade. Sistemas excessivamente complexos afastam o titular e estimulam consentimentos formais, mas pouco conscientes. Sistemas simples demais sacrificam controle. O equilíbrio está em apresentar escolhas granulares, linguagem clara e interfaces que permitam decisão real sem transformar o paciente em especialista jurídico ou técnico.

A lição para a publicidade médica é direta: consentimento bom não é o mais longo. É o mais compreensível, específico, rastreável, revogável e operacionalmente executável.

PARTE



Da autorização informal ao
consentimento auditável.

CAPÍTULO

10

A fragilidade do print como prova digital.

O print ocupa lugar curioso na cultura jurídica e administrativa brasileira. É simples, rápido, intuitivo e frequentemente aceito como indício. Em muitas situações, ajuda a reconstruir fatos. Mas, quando se trata de consentimento para uso de dado sensível em publicidade médica, o print isolado é frágil demais para o risco envolvido.

Imagine situação comum. A equipe envia ao paciente a mensagem: “podemos postar sua foto?”. O paciente responde: “pode”. A equipe salva a tela. O conteúdo é publicado. Meses depois, o paciente afirma que autorizou apenas envio interno, ou apenas uso em aula, ou apenas aquela imagem específica, ou que não compreendeu que seria anúncio patrocinado. Em outro cenário, o paciente revoga a autorização e a clínica não consegue demonstrar quando recebeu a revogação, quem foi comunicado, quais providências tomou e por que ainda havia conteúdo replicado em canais externos.

O print mostra algo, mas deixa de mostrar muito. Não preserva necessariamente metadados originais. Não comprova autoria com robustez. Não demonstra integridade da conversa. Não vincula aceite a termo específico. Não estabelece finalidade clara. Não diferencia escopos. Não registra prazo. Não prova que o conteúdo publicado corresponde ao conteúdo autorizado. Não documenta revogação. Não organiza cadeia de custódia.

Isso não significa que o print seja sempre inválido. No processo civil brasileiro, a prova é ampla, e o juiz pode valorar diferentes elementos conforme o caso. O CPC admite meios típicos e atípicos de prova, desde que moralmente legítimos. O problema é outro: o print tende a exigir complementação por contexto,



metadados, testemunhos, registros de sistema, ata notarial, perícia ou outros elementos.

A ata notarial é instrumento útil para fortalecer prova de conteúdo digital. Ela permite que o tabelião constate, com fé pública, a existência e o conteúdo de páginas, mensagens, perfis, campanhas e materiais acessíveis em determinado momento. Não substitui consentimento, integridade, autoria, finalidade ou cadeia de custódia. Sua função é complementar, sobretudo quando é necessário demonstrar existência externa de conteúdo publicado, republicado ou capturado por terceiros.

A teoria da prova digital valoriza método. A ABNT NBR ISO/IEC 27037:2013, ao tratar de identificação, coleta, aquisição e preservação de evidência digital, reforça atributos como auditabilidade, repetibilidade, reprodutibilidade e justificabilidade. Ainda que a norma não tenha sido criada especificamente para publicidade médica, oferece referência útil: prova digital robusta depende de preservação de integridade, documentação da coleta e rastreabilidade.

CRITÉRIO	AUTORIZAÇÃO INFORMAL	CONSENTIMENTO AUDITÁVEL
Autoria	Dependente de presunção ou contexto externo	Fortalecida por canal validado, autenticação proporcional e logs
Finalidade	Genérica ou implícita	Específica, destacada e granular
Integridade	Difícil de verificar	Verificável por pacote de evidência, hash e trilha temporal
Contexto	Parcial, reconstruído depois	Registrado no momento do aceite
Revogação	Manual e dispersa	Rastreável e vinculada ao consentimento original
Defesa institucional	Possível, mas frágil quando isolada	Mais consistente, sem eliminar risco

A questão, portanto, não é demonizar o print. É superar sua dependência como núcleo de prova em ambiente que exige maior maturidade.

CAPÍTULO

11

Captura ativa de consentimento.

A diferença entre captura passiva e captura ativa é uma das chaves para compreender a governança moderna de consentimento.

Na captura passiva, a instituição registra aparência de autorização depois que ela acontece em canal não desenhado para isso. A conversa em aplicativo, a autorização verbal, a fotografia de termo assinado, o arquivo solto em pasta compartilhada e a resposta genérica do paciente são exemplos. O consentimento é coletado ao redor da rotina, sem fluxo próprio, campos estruturados ou prova técnica integrada.

Na captura ativa, o consentimento ocorre dentro de fluxo desenhado para consentir. O titular recebe informação, visualiza finalidade, escolhe escopos, confirma decisão, tem registro temporal, vincula o aceite a conteúdo ou categoria de conteúdo, recebe canal de acesso e pode revogar. A instituição registra metadados, versão do termo, logs, status, hash, histórico de uso e eventual revogação.

Essa mudança parece técnica, mas é profundamente jurídica. Consentimento não é apenas declaração de vontade. É declaração de vontade informada, livre e vinculada a finalidade. Quando o fluxo força a organização de finalidade, escopo, canal, prazo e conteúdo, reduz ambiguidade. Quando preserva evidência no momento do aceite, evita reconstruções oportunistas. Quando registra revogação, demonstra respeito ao ciclo de vida.

A captura ativa pode ocorrer presencialmente ou remotamente. Em ambiente presencial, um QR Code pode direcionar o paciente a página de consentimento vinculada ao profissional, procedimento ou contexto. Um desafio simples, como código verbal informado no consultório, pode reduzir acesso fortuito por terceiros.

Em ambiente remoto, link autenticado pode conduzir o titular a termo específico. Em ambos os casos, a finalidade não é apenas obter clique. É transformar autorização em evento auditável.

É importante não exagerar a função de cada componente. QR Code não identifica sozinho o paciente. Código verbal não é autenticação forte isolada. Link não prova compreensão. Mas, combinados com identificação mínima, logs, termo específico, aceite ativo, hash e trilha temporal, esses elementos formam cadeia de evidência mais robusta do que autorização dispersa.

PARTE

IV

Arquitetura de prova e
integridade.

CAPÍTULO

12

Consentimento granular por finalidade.

Consentimento publicitário em saúde deve ser granular porque as finalidades são diferentes. Autorizar uso em prontuário não equivale a autorizar uso em rede social. Autorizar uso em aula médica não equivale a autorizar uso em site institucional. Autorizar relato textual não equivale a autorizar imagem reconhecível. Autorizar material educativo não equivale a autorizar anúncio patrocinado. Autorizar por tempo determinado não equivale a autorizar uso contínuo.

A granularidade protege o paciente e a instituição. Protege o paciente porque permite escolhas reais. Protege a instituição porque reduz disputa interpretativa. Quando cada finalidade é escopo próprio, a clínica sabe o que pode fazer, a equipe de marketing sabe o que está autorizado, o médico sabe os limites éticos da publicação e o paciente sabe o que decidiu.

Há, contudo, um filtro anterior: granularidade não torna admissível o que a ética médica veda. Um sistema pode tecnicamente permitir a escolha “publicar imagem reconhecível de procedimento”, mas o fluxo jurídico-ético deve bloquear escopos incompatíveis com CEM, Resolução CFM, sigilo, anonimato ou dignidade. Boa governança não apenas registra autorizações; impede que autorizações inadequadas sejam solicitadas ou utilizadas.

Um modelo maduro deve separar finalidades assistenciais, educativas, institucionais, acadêmicas, científicas e reputacionais. Deve distinguir imagem identificável, imagem desidentificada, imagem anonimizada e relato textual. Deve diferenciar canais próprios, redes sociais, site, material impresso, aula, congresso,



publicação científica e campanha patrocinada. Deve permitir limitação temporal quando aplicável. Deve registrar revogação por finalidade, não apenas revogação global.

O termo guarda-chuva é vício comum. Autorizações como “autorizo o uso da minha imagem para quaisquer fins” são frágeis porque eliminam especificidade. Em dados sensíveis, quanto mais ampla a autorização, maior tende a ser a vulnerabilidade. O consentimento deve iluminar a finalidade, não escondê-la.

FINALIDADE	EXEMPLO	GRAU DE EXPOSIÇÃO	CAUTELA MÍNIMA
Assistencial	Imagem em prontuário, teleconsulta ou acompanhamento clínico	Restrito	Sigilo, finalidade clínica e segregação de uso publicitário
Educativa fechada	Aula interna, discussão técnica ou treinamento profissional	Controlado	Minimização, confidencialidade e autorização específica quando houver identificação
Acadêmica ou científica	Congresso, artigo, pesquisa ou apresentação científica	Variável	Avaliação ética, anonimização robusta e análise de risco de reidentificação
Institucional orgânica	Site, perfil próprio ou material da clínica	Público	Consentimento granular, revisão ética, anonimato quando exigível e prazo de uso
Reputacional ou prova social	Depoimento, relato, repostagem ou avaliação destacada	Público ampliado	Consentimento específico, sobriedade, contexto e vedação a promessa de resultado



FINALIDADE	EXEMPLO	GRAU DE EXPOSIÇÃO	CAUTELA MÍNIMA
Publicidade patrocinada	Anúncio, impulsionamento, remarketing ou campanha segmentada	Amplificado e algorítmico	Consentimento próprio, transparência publicitária, limitação temporal e avaliação de segmentação

A anonimização exige precisão. Em saúde, ocultar o rosto não significa necessariamente anonimizar. Tatuagens, voz, cicatrizes, datas, localização, raridade do procedimento, legenda, contexto familiar, uniforme, prontuário visível ou combinação de metadados podem permitir reidentificação. Pseudonimização apenas substitui identificadores diretos por códigos, mantendo possibilidade de reversão. Desidentificação visual reduz sinais aparentes, mas pode não eliminar risco. Cada publicação deve avaliar não apenas o que aparece, mas o que pode ser inferido.

CAPÍTULO

13

Autenticação, Magic Link e fatores complementares.

Autoria é ponto sensível da prova digital. Em litígios ou questionamentos administrativos, não basta demonstrar que alguém clicou. É necessário demonstrar, com razoabilidade técnica, que o ato foi praticado pelo titular ou por pessoa legitimada.

Em sistemas voltados a pacientes, exigir criação de senha pode gerar fricção desnecessária. Senhas são esquecidas, reutilizadas, compartilhadas e vazadas. Em muitos casos, o paciente acessa o ambiente poucas vezes, apenas para autorizar, consultar ou revogar consentimento. O Magic Link, link temporário enviado a canal previamente associado ao paciente, pode oferecer boa relação entre usabilidade e segurança.

O Magic Link fortalece a cadeia de autoria porque vincula evento a canal, destinatário, prazo, finalidade e documento apresentado. Quando combinado com logs de emissão, abertura, aceite, user-agent, IP minimizado ou hashado, versão do termo e status do evento, oferece narrativa probatória mais consistente do que mensagem solta. Ainda assim, não prova identidade jurídica plena. Um e-mail pode estar aberto em dispositivo compartilhado. Um link pode ser encaminhado. Um celular pode estar com terceiro. Sua função é compor conjunto de sinais.

Tokens assinados, como JSON Web Signature, RFC 7515, podem reforçar integridade técnica de mensagens ou tokens. Um token temporário deve carregar apenas informações necessárias, ter finalidade delimitada, expirar em curto prazo e ser inutilizado após uso ou vencimento. JWS, contudo, não deve ser confundido com assinatura eletrônica qualificada nem com certificado ICP-Brasil. Quando a estratégia exigir assinatura eletrônica com efeitos jurídicos próprios, a análise deve considerar a Lei nº 14.063/2020 e a Medida Provisória nº 2.200-2/2001.



Em situações de maior risco, podem ser proporcionais fatores complementares: confirmação por segundo canal, validação documental, assinatura eletrônica avançada ou qualificada, videoconferência registrada, biometria ou reconfirmação posterior. A escolha deve respeitar adequação, necessidade, proporcionalidade e minimização. Autenticação não deve virar coleta excessiva de dados.



CASO ILUSTRATIVO

Um Magic Link é enviado ao e-mail informado por familiar do paciente, que cuidava da logística do atendimento. O familiar abre o link e marca escopos. Tecnicamente, houve aceite. Juridicamente, o ato não foi praticado pelo titular. A instituição, ao identificar falha na vinculação do canal, não deve invocar o evento como consentimento válido.

CAPÍTULO

14

Pacote de evidência e cadeia de custódia digital.

O consentimento auditável exige objeto técnico que preserve o evento. Esse objeto pode ser chamado de pacote de evidência. Seu papel é reunir, de forma estruturada, os elementos que permitem demonstrar o que aconteceu.

Um pacote de evidência adequado deve conter identificadores opacos, dados mínimos do titular, controlador e profissional vinculado, termo apresentado, versão do termo, hash do termo, finalidades autorizadas, canal de coleta, contexto, timestamp, metadados técnicos minimizados, status do consentimento, vínculo ao conteúdo autorizado e referência a eventual revogação posterior.

A lógica é semelhante à do prontuário em um ponto essencial: o valor não está apenas em registrar informação, mas em preservar sequência confiável de eventos. No prontuário, a evolução clínica importa porque documenta história assistencial. Na governança de consentimento, o pacote de evidência importa porque documenta história da autorização, uso, controle e revogação.

Logs append-only, registros que aceitam novas inserções, mas não alteração retroativa pela aplicação, são relevantes. Quando o consentimento é concedido, registra-se um evento. Quando revogado, registra-se outro evento vinculado. Quando há uso do conteúdo, registra-se uso. Quando há exportação probatória, registra-se exportação. Essa lógica evita falsa limpeza do histórico. Governança não consiste em apagar o passado, mas em registrar corretamente o ciclo.

A cadeia de custódia digital, tomada como referência metodológica, reforça identificação, coleta, preservação, armazenamento, documentação, rastreabilidade e auditoria. No campo penal, o CPP disciplina cadeia de custódia com finalidades próprias. Em publicidade médica e proteção de dados, a referência



é analógica. Ainda assim, a ideia central é útil: a prova vale mais quando sua trajetória pode ser explicada.

O pacote também deve ser exportável e compreensível. Prova que só o sistema entende é operacionalmente frágil. A exportação deve permitir leitura humana e análise técnica por advogado, auditor, CRM, ANPD, perito ou julgador, sem exigir acesso irrestrito ao ambiente interno. Deve conter termo, versão, escopos, canal, data e hora, trilha de eventos, status de revogação, vínculo ao conteúdo, hash, timestamp, logs minimizados, histórico de uso e declaração técnica explicativa. Exportações devem ser justificadas, registradas e protegidas.

ELEMENTO EXPORTÁVEL	FUNÇÃO PROBATÓRIA
Termo e versão	Demonstrar exatamente o conteúdo informado ao titular
Escopos e canais	Vincular autorização à finalidade e ao meio de uso
Trilha de eventos	Reconstituir aceite, uso, revogação e exportação
Hash e timestamp	Verificar integridade e anterioridade do pacote
Logs minimizados	Fortalecer autoria provável sem exposição excessiva
Declaração técnica	Explicar método, limites e forma de verificação



CAPÍTULO

15

Hash, timestamp e integridade criptográfica.

Hash criptográfico é impressão digital matemática de um conteúdo. Ao aplicar função como SHA-256 a arquivo ou conjunto de dados, obtém-se sequência de caracteres. Qualquer alteração mínima no conteúdo original altera o resultado. Essa propriedade permite verificar integridade sem revelar o conteúdo.

No contexto de consentimento médico-publicitário, o hash pode ser calculado sobre o pacote de evidência. Se o pacote contém termo, versão, finalidade, escopo, data, identificadores e metadados, o hash passa a representar aquela configuração exata. Se alguém modificar finalidade, data, versão ou campo relevante, o hash resultante deixa de coincidir.

Quando o pacote é estruturado em JSON, a canonicalização é relevante. O mesmo conteúdo pode ser serializado com chaves em ordem diferente. Para evitar divergências artificiais, utiliza-se formato canônico, como o JSON Canonicalization Scheme, RFC 8785. Assim, o hash reflete o conteúdo, não a ordem acidental de apresentação das chaves.

O timestamp, ou carimbo de tempo, acrescenta dimensão temporal. Ele indica quando aquele pacote existia naquela forma. A combinação entre hash e timestamp produz prova de integridade e anterioridade mais forte do que arquivo isolado.

Mas o hash tem limites. Demonstra integridade desde o momento do cálculo. Não demonstra que o paciente leu, compreendeu, decidiu livremente ou estava em condição adequada de consentir. Não demonstra que a finalidade era ética. Não demonstra autoria absoluta. Também não equivale a anonimização. Um hash ou

identificador pode ser dado pessoal se for vinculável a um titular por meios razoáveis, especialmente quando associado a registros internos, datas, eventos, transações ou metadados persistentes.

Hash é componente probatório, não prova completa. Sua força está na combinação com consentimento informado, autenticação proporcional, logs, termo claro, curadoria ética e governança de uso.



CAPÍTULO

16

Blockchain, ancoragem e verificação pública.

Blockchain tornou-se palavra cercada por exageros. Em governança de consentimento, seu uso deve ser preciso. A função adequada não é armazenar dados sensíveis de pacientes em rede pública. Isso seria incompatível com minimização, privacidade, controle de acesso e possibilidade de gestão de ciclo de vida. A função tecnicamente defensável é registrar prova criptográfica, como hash, sem expor conteúdo.

O modelo híbrido é o mais adequado. Dados sensíveis permanecem off-chain, cifrados, controlados e sujeitos a políticas de retenção, acesso e descarte. Na rede pública, quando aplicável, registra-se apenas o mínimo criptográfico necessário, sem nome, CPF, e-mail, imagem, relato, prontuário, metadado semântico ou identificador que permita correlacionamento indevido.

A ancoragem em blockchain pública pode demonstrar que determinado hash existia em certo momento. Se, no futuro, a instituição apresentar o pacote de evidência, qualquer parte pode recalcular o hash e compará-lo com o registro ancorado. Coincidência indica que o pacote não foi alterado desde a ancoragem. Divergência indica modificação ou inconsistência.

A verificação pública deve ser desenhada com minimização. Uma página ou mecanismo de consulta pode exibir identificador opaco, data, status técnico, hash e referência de transação. Não deve revelar nome do paciente, conteúdo clínico, imagem, relato ou informação que permita identificação. Mesmo hashes devem ser avaliados quanto a risco de vínculo com bases internas ou externas.



Blockchain agrega prova de anterioridade, dificuldade de adulteração retroativa e verificação independente. Mas não valida consentimento mal redigido, não torna lícito uso abusivo, não substitui transparência, não elimina dever de segurança, não garante remoção total de conteúdo disseminado e não dispensa revisão humana.

Formulação prudencial: blockchain não transforma autorização ruim em autorização válida. Ela preserva evidência criptográfica de que determinado pacote existia, em determinada forma, em determinado tempo.

PARTE

V

Ciclo de vida, operação e
riscos.



CAPÍTULO

17

Portal do titular, revogação e ciclo de vida.

Consentimento não termina no aceite. Essa é uma das maiores diferenças entre cultura documental antiga e cultura de governança. O titular não deixa de ser titular depois que clica. Direitos de informação, acesso, esclarecimento, oposição quando aplicável, eliminação e revogação continuam existindo.

Um portal do titular, ou mecanismo equivalente, é a expressão prática dessa continuidade. Deve permitir que o paciente visualize autorizações concedidas, compreenda finalidades, veja canais autorizados, consulte histórico, revogue por finalidade, solicite esclarecimentos e acompanhe providências. Transparência deixa de ser promessa abstrata e torna-se funcionalidade verificável.

A revogação deve ser tratada como novo evento, não como apagamento silencioso. Quando o paciente revoga, o sistema deve registrar data, hora, escopo revogado, vínculo ao consentimento original, providências tomadas e eventual limitação técnica. Conteúdo controlado pela instituição deve ser retirado, bloqueado ou descontinuado conforme o escopo. O histórico de consentimento e revogação pode ser preservado para exercício regular de direitos, cumprimento de obrigação legal ou regulatória e prestação de contas, desde que com base adequada, acesso restrito, segurança e proporcionalidade.

Há tensão legítima entre eliminação e preservação probatória. O paciente pode revogar uso público futuro, mas a instituição pode precisar preservar registro de que havia autorização antes da revogação, especialmente se houver questionamento posterior. A solução não está em negar direitos do titular nem em apagar toda evidência. Está em separar conteúdo publicitário, que pode precisar ser retirado, do registro probatório mínimo, que pode precisar ser preservado.



Também é necessário reconhecer limites práticos. A instituição responde pelo que controla. Pode retirar conteúdo de seu site, redes próprias, campanhas vigentes e materiais sob sua gestão. Não pode garantir, em termos absolutos, remoção de prints feitos por terceiros, indexações, republicações não autorizadas ou cópias fora de seu controle. A obrigação adequada é de meios diligentes, documentados e proporcionais.

Fluxo conceitual do ciclo de vida: 1. informação clara ao titular; 2. consentimento granular por finalidade; 3. registro estruturado e pacote de evidência; 4. uso controlado dentro do escopo; 5. auditoria e verificação de integridade; 6. revogação ou expiração; 7. retirada operacional, descarte ou preservação probatória proporcional.

CAPÍTULO

18

Segurança da informação e separação de dados.

Prova robusta depende de ambiente seguro. Um pacote de evidência perde força se o sistema que o guarda é vulnerável, se acessos são indiscriminados, se logs são alteráveis, se dados de clínicas diferentes se misturam ou se fornecedores externos operam sem contrato e controle.

A segurança deve começar pela minimização. Coletar menos dados reduz risco. Dados pessoais sensíveis devem ser protegidos em trânsito e em repouso. Chaves criptográficas devem ser geridas com segregação, rotação e controle de acesso. Logs devem registrar acessos relevantes sem coletar excesso. Backups, continuidade e recuperação devem ser planejados. Incidentes devem ter plano de resposta. Fornecedores devem ser avaliados.

Em plataformas multi-tenant, nas quais várias clínicas compartilham infraestrutura, a separação de dados é crítica. Cada tenant, ou instância lógica que isola dados de uma organização em relação às demais, deve receber tratamento estanque. Row-Level Security, ou mecanismo equivalente, reforça isolamento no nível do banco de dados. A aplicação não deve ser a única barreira. O próprio banco deve restringir linhas conforme tenant, papel e necessidade.

Controle de acesso baseado em papéis é essencial. Recepção, marketing, médico, gestor, encarregado, operador técnico e auditor não precisam ver as mesmas informações. O princípio do menor privilégio deve orientar permissões. Quanto mais sensível o conteúdo, mais restrito deve ser o acesso.

A governança de fornecedores completa o quadro. Hospedagem, e-mail transacional, autenticação, armazenamento em nuvem, agência de marketing, editores, ferramentas de IA, serviços de mídia programática e ancoragem em blockchain podem participar da cadeia. Cada fornecedor deve ter papel definido,



cláusulas de confidencialidade, instruções de tratamento, medidas de segurança, regras de subcontratação, obrigações de incidente, retorno ou eliminação de dados e avaliação de transferência internacional quando aplicável.

Tratamentos sensíveis, com exposição pública, uso de imagem, dados de crianças ou adolescentes, publicidade patrocinada, IA, fornecedores externos ou transferência internacional podem justificar Relatório de Impacto à Proteção de Dados Pessoais, RIPD. Em publicidade médica, a pergunta central do RIPD não é apenas “o sistema é seguro?”, mas “a exposição é necessária, proporcional, compreensível, revogável, auditável e compatível com a vulnerabilidade do titular?”.

CAPÍTULO

19

Resposta a incidentes e transferência internacional.

Incidentes de segurança, vazamentos, acessos indevidos, exposições não autorizadas e usos além de escopo não são hipóteses teóricas. São eventos prováveis ao longo do tempo. Em publicidade médica, a sensibilidade do dado eleva o impacto. Exposição não autorizada de imagem clínica, relato ou identificação de paciente pode gerar dano material, moral, reputacional e ético.

A LGPD, art. 48, impõe ao controlador o dever de comunicar à ANPD e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante. A Resolução CD/ANPD nº 15/2024 disciplina o procedimento. Quando o incidente estiver confirmado, envolver dados pessoais e puder acarretar risco ou dano relevante, a comunicação à ANPD e aos titulares deve ocorrer, em regra, em até três dias úteis, ressalvada legislação específica. Informações complementares podem ser apresentadas de modo fundamentado quando não estiverem disponíveis de imediato.

Na avaliação de risco, dados sensíveis, dados de crianças, adolescentes ou idosos, dados protegidos por sigilo profissional, dados de autenticação e tratamento em larga escala são fatores relevantes. Em publicidade médica, muitos incidentes envolverão ao menos uma dessas categorias. Por isso, o plano de resposta deve ser conhecido, ensaiado, atualizado e ativável rapidamente.

A instituição deve manter plano de resposta que contemple identificação, contenção, análise, comunicação, remediação e lições aprendidas. O encarregado tem papel central como ponto de contato com titulares e ANPD. Equipes médica, técnica, jurídica, de comunicação e de fornecedores devem ter papéis definidos previamente. A improvisação, em matéria de incidente, costuma ampliar dano.



O operador deve informar o controlador sem demora injustificada e fornecer informações necessárias à comunicação. Contratos devem prever fluxo de alerta, prazos internos, evidências, preservação de logs, cooperação técnica e responsabilidades. A ausência de cláusulas claras costuma converter incidente técnico em crise institucional.

A transferência internacional de dados exige atenção própria. Plataformas de e-mail transacional, armazenamento em nuvem, IA, serviços de ancoragem, CDN, ferramentas de analytics, mídia programática e agências internacionais podem implicar dados processados fora do Brasil. Os arts. 33 a 36 da LGPD e a Resolução CD/ANPD nº 19/2024 disciplinam mecanismos de transferência internacional, incluindo cláusulas-padrão contratuais, cláusulas específicas, normas corporativas globais e decisões de adequação.

A instituição deve mapear fluxos, identificar países, operadores e suboperadores, verificar se há dados sensíveis, avaliar garantias contratuais e técnicas, documentar o mecanismo de transferência e informar o titular quando necessário. Em publicidade médica, a pergunta não é apenas onde o dado está armazenado; é por quais serviços, APIs, ferramentas de IA, redes de anúncios e fornecedores ele trafega.



PONTO DE ATENÇÃO

Plano de incidentes não é documento de prateleira. Deve ser conhecido, testado, atualizado e compatível com a sensibilidade dos dados de saúde.

CAPÍTULO

20

Inteligência artificial, mídia sintética e supervisão humana.

A inteligência artificial já participa da comunicação em saúde, ainda que nem sempre de forma declarada. Pode classificar relatos, sugerir respostas, identificar risco, resumir mensagens, apoiar revisão editorial, detectar padrões de reclamação e auxiliar auditoria. Esses usos podem ser legítimos quando mantidos sob supervisão humana, com limites claros, segurança, minimização e registro.

O risco surge quando a IA deixa de apoiar e passa a substituir decisão profissional. Em publicidade médica, a IA não deve publicar automaticamente, fabricar depoimentos, criar prova social fictícia, simular pacientes reais, classificar pessoas como verdadeiras ou falsas, editar imagens clínicas sem registro, ocultar manipulações ou produzir respostas sensíveis sem revisão humana.

Mídia sintética torna o problema ainda mais delicado. Imagens, vídeos, áudios e textos podem ser gerados ou alterados de modo quase imperceptível. Em medicina, isso ameaça veracidade. Uma imagem de antes e depois editada, pele suavizada, cicatriz reduzida, iluminação artificialmente favorável ou simulação não declarada pode induzir expectativa incompatível com a ética médica.

O princípio orientador é transparência ativa. Quando a IA participa de processo que afeta o titular ou produz conteúdo para circulação pública, a instituição deve informar essa participação quando relevante, declarar finalidade, preservar conteúdo original, registrar intervenções e submeter a revisão humana qualificada antes da publicação. Edições de organização, enquadramento ou legibilidade podem ser legítimas quando não deturpam fatos clínicos e quando documentadas. Edições que alterem substância clínica devem ser tratadas como alto risco.



A governança deve exigir preservação do original, registro de edição, política interna de uso aceitável, declaração de uso de IA quando relevante, controle de fornecedores, avaliação de transferência internacional e revisão humana antes da publicação. Em conteúdos clínicos, a regra deve ser conservadora: IA pode melhorar organização e triagem, mas não deve alterar a substância da evidência.

USO DE IA	ENQUADRAMENTO RECOMENDADO
Triagem de relatos, organização documental e apoio à auditoria	Admissível com supervisão, segurança e registro
Sugestão de revisão textual	Admissível quando não altera fatos clínicos nem cria promessa de resultado
Edição estética de imagem clínica	Alto risco; exige preservação do original, registro e revisão médica
Criação de depoimento, paciente simulado ou prova social fictícia	Incompatível com veracidade, ética médica e confiança pública
Publicação automática sem revisão humana	Inadequada em conteúdo sensível e publicitário em saúde



PONTO DE ATENÇÃO

Supervisão humana qualificada não é obstáculo à inovação. É condição para que inovação seja confiável.

CAPÍTULO

21

Retenção, descarte e preservação probatória.

Todo dado deve ter ciclo de vida. A ausência de prazo e política de retenção transforma repositórios em passivos. Em publicidade médica, esse risco aumenta porque os dados são sensíveis, identificáveis e frequentemente ligados à imagem e reputação.

A instituição deve definir por quanto tempo mantém conteúdo publicado, consentimentos, revogações, logs, pacotes de evidência, registros de uso, exportações probatórias e registros de incidentes. Prazos devem ser proporcionais à finalidade. Um registro necessário para defesa pode ter prazo diferente de material publicitário ativo. Conteúdo revogado deve ter tratamento diferente de conteúdo vigente.

O descarte seguro pode envolver eliminação, anonimização, bloqueio, inutilização de chaves criptográficas ou limitação de acesso. Em qualquer hipótese, deve ser documentado. O descarte não deve ser ato invisível. Deve haver registro de que determinada finalidade se encerrou e de quais providências foram adotadas.

A preservação probatória exige equilíbrio. Se a instituição apaga todo registro de consentimento após revogação, pode ficar incapaz de demonstrar que publicação anterior era autorizada. Se preserva tudo indefinidamente, viola necessidade e minimização. A solução está em política clara, base jurídica adequada, acesso restrito, revisão periódica e separação entre uso público e registro defensivo.

O direito à eliminação não deve ser tratado como absoluto em toda hipótese, mas também não deve ser esvaziado. Deve ser analisado junto a finalidades remanescentes, bases legais, deveres regulatórios, direitos de defesa, art. 16 da LGPD e regime de dados sensíveis do art. 11.

PARTE

VI

Governança, métricas e
síntese.

CAPÍTULO

22

Governança operacional, contratos e responsabilidades.

A tecnologia organiza evidências, mas a governança define responsabilidades. Sem papéis claros, mesmo o melhor sistema pode ser mal utilizado.

O paciente é titular de dados e sujeito de direitos. Deve poder consentir, recusar, revogar e fiscalizar. O médico mantém responsabilidade ética pelo conteúdo associado ao exercício profissional. A clínica ou profissional controlador define finalidades, bases legais, políticas e limites de uso. Fornecedor tecnológico pode atuar como operador quando trata dados em nome do controlador. Agência de marketing pode atuar como operadora, controladora independente ou controladora conjunta, conforme decisões, autonomia e contrato. O encarregado atua como canal com titulares e ANPD. CRM e ANPD fiscalizam e orientam em suas esferas.

Contratos devem refletir esses papéis. Não basta contratar ferramenta ou agência. É necessário definir instruções de tratamento, confidencialidade, segurança, subcontratação, atendimento a titulares, resposta a incidentes, transferência internacional, devolução ou eliminação de dados, auditoria, uso de IA, proibição de reutilização e responsabilidades por publicação fora de escopo.

A política interna de publicidade médica deve funcionar como ponte entre direito, ética, marketing e tecnologia. Deve dizer quem pode selecionar conteúdo, quem revisa consentimento, quem aprova publicação, quem monitora revogação, quem responde a titulares, quem exporta evidências e quem decide em casos sensíveis.



Fluxo editorial recomendado: 1. seleção do conteúdo; 2. checagem do consentimento e do escopo; 3. análise ética de finalidade, anonimato, sobriedade e promessa de resultado; 4. revisão jurídica ou de compliance quando necessário; 5. validação médica; 6. publicação controlada; 7. monitoramento e registro de uso; 8. revogação, retirada, descarte ou preservação probatória.

ATOR	RESPONSABILIDADE PRINCIPAL	RISCO SE AUSENTE
Paciente	Consentir, recusar, revogar e fiscalizar	Autonomia meramente formal
Médico	Preservar ética, sigilo, sobriedade, anonimato e veracidade	Denúncia ética e dano reputacional
Controlador	Definir finalidade, base legal, política e governança	Sanção, litígio e falha de prestação de contas
Operador tecnológico	Executar tratamento conforme instruções e segurança	Vazamento, prova incompleta ou acesso indevido
Marketing	Produzir conteúdo dentro da política aprovada	Publicação fora de escopo ou linguagem antiética
Encarregado	Atender titulares e interagir com a ANPD	Resposta tardia, desorganizada ou inconsistente
Jurídico/compliance	Avaliar risco regulatório e contratos	Ambiguidade de papéis e exposição institucional

Governança não é burocracia. É a forma pela qual a instituição demonstra que a comunicação pública tem controles compatíveis com o risco que produz.

CAPÍTULO

23

Métricas, auditoria e maturidade.

Aquilo que não é medido tende a depender de memória, boa vontade e improviso. Em publicidade médica, isso é perigoso. A maturidade de governança deve ser observável.

Métricas úteis incluem percentual de publicações com consentimento ativo vinculado, número de consentimentos por finalidade, taxa de revogação, tempo médio de atendimento a titulares, número de pacotes de evidência completos, falhas de autenticação, latência de ancoragem quando aplicável, incidentes de segurança, publicações bloqueadas por ausência de escopo, publicações bloqueadas por risco ético, auditorias concluídas e fornecedores revisados.

A auditoria deve revisar termos, fluxos, publicações, logs, fornecedores, revogações, incidentes e treinamento de equipes. Deve verificar se conteúdos publicados correspondem ao escopo autorizado e aos limites éticos. Deve testar se a revogação funciona. Deve avaliar se o pacote de evidência é exportável e compreensível para defesa administrativa, judicial ou ética.

A maturidade pode ser compreendida em níveis:

NÍVEL	DESCRIÇÃO	CARACTERÍSTICA PRINCIPAL
1, informal	Autorizações dispersas	Prints, mensagens e controles pessoais
2, documentado	Termos padronizados	Registro existe, mas gestão é manual



NÍVEL	DESCRIÇÃO	CARACTERÍSTICA PRINCIPAL
3, rastreável	Consentimento ativo com logs	Autoria e contexto são fortalecidos
4, verificável	Hash, timestamp e pacote de evidência	Integridade pode ser demonstrada
5, auditável	Portal, revogação, métricas e auditoria contínua	Governança opera como sistema
6, ético-verificável	Bloqueios éticos, anonimato e supervisão humana qualificada	A instituição demonstra também por que não publica

O objetivo não é criar perfeição abstrata. É reduzir improviso, aumentar consistência e tornar prestação de contas possível.

CAPÍTULO

24

Publicidade médica verificável e confiança institucional.

A publicidade médica entrou em fase na qual reputação, ética, dados sensíveis e prova digital não podem mais ser separados. O profissional que comunica precisa considerar não apenas estética da publicação, mas legitimidade da exposição. A clínica que divulga resultados precisa considerar não apenas engajamento, mas consentimento, anonimato, contexto e integridade. A equipe de marketing precisa compreender que prova social em saúde não é ativo comum.

A confiança institucional nasce de múltiplos sinais: competência técnica, experiência assistencial, clareza de comunicação, segurança de dados, respeito à autonomia do paciente, sobriedade ética e capacidade de demonstrar conformidade. Em mercados saturados de exposição, a sobriedade verificável pode ser diferencial mais duradouro do que a publicação impactante.

Governança probatória não existe para ampliar publicidade de modo irrestrito. Existe para limitar, documentar e qualificar o uso de conteúdos sensíveis. Protege pacientes contra exposição indevida, médicos contra acusações baseadas em lacunas documentais, clínicas contra improviso operacional e a confiança social na medicina contra mercantilização da experiência do paciente.

A autorização informal pode parecer simples, mas simplicidade sem prova cobra preço quando há conflito. A governança auditável exige mais método no início, mas reduz incerteza ao longo do tempo. Em saúde, esse custo de organização é proporcional ao valor do bem protegido.

TESE DE FECHAMENTO

A tese final é esta: o futuro da publicidade médica não será definido apenas por quem comunica melhor, mas por quem consegue demonstrar melhor que sabe quando comunicar, quando não comunicar e, quando a comunicação for admissível, fazê-lo com ética, consentimento, integridade e respeito à autonomia do paciente.

Dr. Julio Garcia

ANEXO A

Matriz normativa essencial.

EIXO	NORMA DE REFERÊNCIA	NÚCLEO APLICÁVEL
Ética médica	Resolução CFM nº 2.217/2018, especialmente arts. 73 e 75; Resolução CFM nº 2.336/2023; Manual de Publicidade Médica do CFM	Sigilo, sobriedade, veracidade, anonimato, vedação de paciente reconhecível e limites de publicidade
Publicidade médica	Resolução CFM nº 2.336/2023, arts. 8º, 11, 12, 13 e 14	Redes sociais próprias, repostagens, proibições, finalidade educativa, imagem de paciente, não manipulação e não promessa de resultado
Proteção de dados	Lei nº 13.709/2018, arts. 5º, 6º, 7º, 8º, 9º, 11, 14, 16, 18, 33 a 36, 42, 46, 48, 50 e 52	Bases legais, consentimento, direitos do titular, segurança, responsabilização e governança
Crianças e adolescentes	ECA; LGPD art. 14; Enunciado CD/ANPD nº 1/2023; Lei nº 15.211/2025; Decreto nº 12.880/2026, quando aplicável ao ambiente digital	Proteção integral, melhor interesse, autonomia progressiva, aferição de idade e proteção em ambientes digitais
Incidentes de segurança	LGPD art. 48; Resolução CD/ANPD nº 15/2024	Comunicação à ANPD e titulares, critérios de risco, prazo, complementação e registro de incidentes
Transferência internacional	LGPD arts. 33 a 36; Resolução CD/ANPD nº 19/2024	Mecanismos de transferência internacional, cláusulas-padrão, garantias e decisões de adequação



EIXO	NORMA DE REFERÊNCIA	NÚCLEO APLICÁVEL
Dosimetria de sanções	Resolução CD/ANPD nº 4/2023	Critérios de aplicação de sanções e relevância de boa-fé, cooperação e medidas corretivas
Direitos da personalidade	Código Civil, arts. 11 a 21	Imagem, nome, honra, intimidade, privacidade e projeções post mortem
Sigilo profissional	Código Penal, art. 154; Código de Ética Médica, arts. 73 e 75	Vedação de revelação de segredo e de exposição de casos clínicos identificáveis
Consumidor	Lei nº 8.078/1990, arts. 6º, 36 e 37	Informação adequada, publicidade identificável, vedação a publicidade enganosa ou abusiva
Pessoa com deficiência	Lei nº 13.146/2015	Autonomia, acessibilidade, tomada de decisão apoiada e comunicação compreensível
Internet	Lei nº 12.965/2014, arts. 7º, 13 a 15	Direitos dos usuários, privacidade e guarda de registros
Prova civil	Lei nº 13.105/2015, arts. 369 e 384	Meios típicos e atípicos de prova e ata notarial
Cadeia de custódia	Decreto-Lei nº 3.689/1941, arts. 158-A a 158-F	Referência metodológica para preservação probatória, por analogia
Assinaturas eletrônicas	Lei nº 14.063/2020; MP nº 2.200-2/2001	Assinaturas simples, avançada e qualificada, ICP-Brasil
Prova digital	ABNT NBR ISO/IEC 27037:2013	Identificação, coleta, aquisição e preservação de evidência digital
Integridade técnica	RFC 7515, JWS; RFC 8785, JCS	Assinatura técnica de JSON, tokens e canonicalização para hash

ANEXO B

Requisitos materiais de um consentimento robusto.

O consentimento publicitário em saúde não se confunde com formulário. Constitui ato jurídico complexo, cuja validade depende de elementos materiais que podem estar organizados em diferentes instrumentos e camadas de informação. Os requisitos abaixo não representam minuta pronta, mas elementos mínimos a considerar na concepção de termos específicos:

- identificação adequada do titular e, quando aplicável, do representante legal;
- identificação do controlador, do profissional responsável e dos operadores relevantes;
- descrição inteligível do conteúdo a ser utilizado;
- confirmação prévia de que o uso é eticamente admissível;
- finalidade específica, separada por escopo, com escolha granular;
- canal autorizado, distinguindo site, rede social orgânica, campanha patrocinada, material impresso, aula, congresso e publicação científica;
- prazo de uso ou critério objetivo de revisão;
- regras de edição, recorte, anonimização, desidentificação ou tratamento de imagem;
- garantia de anonimato quando exigida pelas normas éticas;
- ausência de vantagem, desconto, compensação ou contrapartida financeira para induzir autorização;
- transparência sobre eventual uso de inteligência artificial;
- forma simples, gratuita e acessível de revogação;
- destino e prazo dos registros mantidos para fins probatórios após revogação;
- informações sobre direitos do titular previstos na LGPD;
- canais de contato com controlador e encarregado;
- informação sobre compartilhamento, fornecedores e transferência internacional quando aplicável;



- registro estruturado de aceite, com pacote de evidência adequado.

A presença desses elementos não garante automaticamente a validade do consentimento, mas sua ausência tende a fragilizar o ato e dificultar a prestação de contas. A redação final deve ser submetida à análise jurídica específica da instituição, considerando especialidade, perfil de pacientes, finalidades, canais e fluxos.



ANEXO C

Glossário técnico-jurídico.

Consentimento

manifestação livre, informada e inequívoca pela qual o titular concorda com tratamento de seus dados para finalidade determinada.

Consentimento auditável

consentimento estruturado de modo a permitir demonstração posterior de termo, versão, finalidade, escopo, canal, data, autoria provável, conteúdo autorizado e revogação.

Dado pessoal sensível

dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, dado referente à saúde ou vida sexual, dado genético ou biométrico, quando vinculado a pessoa natural.

Dado inferido

informação obtida por correlação, comportamento, contexto ou probabilidade, capaz de revelar característica do titular, inclusive condição de saúde.

Titular

pessoa natural a quem se referem os dados pessoais.

Controlador

pessoa natural ou jurídica que toma decisões referentes ao tratamento de dados pessoais.

Operador

pessoa natural ou jurídica que realiza tratamento de dados pessoais em nome do controlador.



Controladoria conjunta

situação em que dois ou mais agentes participam de decisões relevantes sobre finalidades e meios do tratamento, conforme o caso concreto.

Encarregado

pessoa indicada pelo controlador para atuar como canal de comunicação com titulares e ANPD.

Finalidade

propósito específico, informado e legítimo que justifica o tratamento.

Revogação

retirada do consentimento pelo titular, com efeitos sobre usos futuros, observadas bases legais de retenção quando aplicáveis.

Pacote de evidência

conjunto estruturado de dados, metadados, termo, versão, escopos, logs e registros técnicos que documentam evento de consentimento.

Hash

impressão digital criptográfica de conteúdo digital, usada para verificar integridade.

SHA-256

algoritmo criptográfico de hash amplamente utilizado para integridade digital.

Timestamp

carimbo de tempo que vincula evento ou registro a momento específico.

Magic Link

link temporário enviado a canal associado ao titular, usado para autenticação sem senha.



JWS

JSON Web Signature, padrão técnico de assinatura de mensagens em formato JSON, previsto no RFC 7515.

JCS

JSON Canonicalization Scheme, método de canonicalização JSON previsto no RFC 8785.

Assinatura eletrônica simples

modalidade de assinatura eletrônica com menor nível de garantia, conforme legislação aplicável.

Assinatura eletrônica avançada

assinatura que utiliza certificados ou meios capazes de associar o signatário de modo unívoco e detectar alterações posteriores, conforme legislação aplicável.

Assinatura eletrônica qualificada

assinatura baseada em certificado digital emitido no âmbito da ICP-Brasil.

Off-chain

armazenamento fora de rede blockchain, adequado para dados sensíveis protegidos.

On-chain

registro em rede blockchain, que deve limitar-se a dados não sensíveis ou provas criptográficas minimizadas.

Tenant

instância lógica que isola dados e configurações de uma organização em relação às demais em ambientes compartilhados.

Row-Level Security

mecanismo de banco de dados que restringe acesso a linhas conforme regras de usuário, papel ou tenant.



Logs append-only

registros que aceitam novas inserções, mas não alteração retroativa pela aplicação.

User-agent

identificação do software cliente, usualmente navegador, útil como metadado em logs.

Mídia sintética

conteúdo gerado ou alterado por inteligência artificial, incluindo imagem, áudio, vídeo ou texto.

Transparência ativa

dever de informar, de forma clara e antecipada, práticas de tratamento, uso de IA, edição de conteúdo e demais elementos relevantes para a decisão do titular.

ANEXO D

Checklist editorial pré-publicação.

Antes da publicação de imagem, relato ou depoimento de paciente, a instituição deve verificar:

- se o conteúdo é eticamente publicável;
- se há paciente reconhecível em contexto vedado pelo CEM ou pela Resolução CFM;
- se a finalidade declarada está coberta pelo consentimento;
- se o conteúdo publicado corresponde ao conteúdo autorizado;
- se há identificação direta ou indireta de paciente ou terceiro;
- se o canal de publicação está autorizado, especialmente em campanhas patrocinadas;
- se o prazo de uso está dentro do escopo;
- se há promessa de resultado, ainda que implícita;
- se há sensacionalismo, mercantilização, autopromoção excessiva ou comparação abusiva;
- se a imagem foi editada, recortada, manipulada ou melhorada;
- se houve uso de IA que exija declaração, registro ou preservação do original;
- se há texto educativo e contexto suficiente quando exigido pelo CFM;
- se o pacote de evidência está completo;
- se existe mecanismo de revogação acessível;
- se o uso foi registrado para auditoria;
- se há envolvimento de crianças, adolescentes, pessoas com deficiência, pessoas vulneráveis ou terceiros incidentais;
- se fornecedores, agência e plataformas atuam dentro de instruções aprovadas;
- se eventual transferência internacional foi mapeada;
- se a publicação deve ser bloqueada por risco ético, jurídico, técnico ou reputacional.



BIBLIOGRAFIA

Referências

ASGHAR, M. R.; LEE, T.; BAIG, M. M.; ULLAH, E.; RUSSELLO, G.; DOBBIE, G. A Review of Privacy and Consent Management in Healthcare: A Focus on Emerging Data Sources. IEEE 13th International Conference on eScience, 2017. DOI: 10.1109/eScience.2017.84.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27037:2013, Tecnologia da informação, técnicas de segurança, diretrizes para identificação, coleta, aquisição e preservação de evidência digital. Rio de Janeiro: ABNT, 2013.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Enunciado CD/ANPD nº 1, de 22 de maio de 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023, Regulamento de Dosimetria e Aplicação de Sanções Administrativas.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Resolução CD/ANPD nº 15, de 24 de abril de 2024, Regulamento de Comunicação de Incidente de Segurança.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Resolução CD/ANPD nº 19, de 23 de agosto de 2024, Regulamento de Transferência Internacional de Dados.

BRASIL. Código Civil, Lei nº 10.406, de 10 de janeiro de 2002.

BRASIL. Código de Processo Civil, Lei nº 13.105, de 16 de março de 2015.

BRASIL. Código de Processo Penal, Decreto-Lei nº 3.689, de 3 de outubro de 1941.

BRASIL. Código Penal, Decreto-Lei nº 2.848, de 7 de dezembro de 1940.

BRASIL. Lei nº 8.069, de 13 de julho de 1990, Estatuto da Criança e do Adolescente.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990, Código de Defesa do Consumidor.

BRASIL. Lei nº 12.965, de 23 de abril de 2014, Marco Civil da Internet.

BRASIL. Lei nº 13.146, de 6 de julho de 2015, Estatuto da Pessoa com Deficiência.

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

BRASIL. Lei nº 14.063, de 23 de setembro de 2020, dispõe sobre o uso de assinaturas eletrônicas.



BRASIL. Lei nº 15.211, de 17 de setembro de 2025, Estatuto Digital da Criança e do Adolescente.

BRASIL. Lei nº 15.352, de 25 de fevereiro de 2026.

BRASIL. Decreto nº 12.880, de 18 de março de 2026.

BRASIL. Decreto nº 12.881, de 18 de março de 2026.

BRASIL. Medida Provisória nº 2.200-2, de 24 de agosto de 2001, institui a Infraestrutura de Chaves Públicas Brasileira, ICP-Brasil.

CONSELHO FEDERAL DE MEDICINA. Código de Ética Médica, Resolução CFM nº 2.217/2018.

CONSELHO FEDERAL DE MEDICINA. Resolução CFM nº 2.314/2022, dispõe sobre a Telemedicina.

CONSELHO FEDERAL DE MEDICINA. Resolução CFM nº 2.336/2023, dispõe sobre publicidade e propaganda médicas.

CONSELHO FEDERAL DE MEDICINA. Manual de Publicidade Médica, versão vigente na data de acesso.

IETF. RFC 7515, JSON Web Signature, JWS.

IETF. RFC 8785, JSON Canonicalization Scheme, JCS.



Sobre o autor

Dr. Júlio Cesar Garcia é advogado, pós-doutor pela Levin College of Law, University of Florida, doutor pela UFPR, mestre pela UEM, professor e pesquisador do PPGD UNIVEL, coordenador do ITDS e editor da REDIR.

Sua atuação acadêmica e profissional situa-se na interface entre Direito, tecnologia, inovação, compliance, governança, sustentabilidade e proteção de dados.

Nesta obra, sua contribuição parte da experiência acumulada como advogado, pesquisador e professor, bem como de sua atuação técnica na concepção de soluções aplicadas à governança de dados sensíveis, proteção de dados, integridade probatória e confiança digital.

CONTATO julio.garcia@univel.br