REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

AVANÇOS E DESAFIOS NA PROTEÇÃO DOS DADOS PESSOAIS DOS USUÁRIOS DA TELESSAÚDE NO MUNICÍPIO DE MANAUS, AMAZONAS

ADVANCES AND CHALLENGES IN PROTECTING THE PERSONAL DATA OF TELEHEALTH USERS IN THE MUNICIPALITY OF MANAUS, AMAZONAS

Ciências Humanas, Ciências Sociais Aplicadas • 02/11/2026

REGISTRO DOI: 10.70773/revistatopicos/793469317

Maria Glades Rodrigues Guedes[1]

Alcian Pereira de Souza[2]

Danielle Costa de Souza Simas[3]

RESUMO

O artigo analisa em que medida a expansão da telessaúde municipal em Manaus foi acompanhada por evidências públicas de governança e proteção de dados pessoais sensíveis. Adota abordagem qualitativa, bibliográfica e documental, com contextualização normativa entre 2020 e 2026 e exame de quatro instrumentos municipais de planejamento e prestação de contas. A coleta foi encerrada em outubro de 2026; os resultados assistenciais examinados alcançam o primeiro quadrimestre desse ano. O referencial articula a Constituição Federal, a Lei Geral de Proteção de Dados Pessoais, o marco da telessaúde, a jurisprudência constitucional e a literatura de 2023 a 2026. Uma matriz relaciona categorias jurídicas, documentos, localização das evidências e limites interpretativos. Identificam-se institucionalização do serviço, previsão de capacitação, integração de autenticação ao Gov.br e planejamento de infraestrutura de cópias de segurança. Entretanto, os documentos não demonstram integralmente bases legais por operação, retenção, compartilhamento, gestão de acessos e resposta a incidentes específicos da telessaúde. Conclui-se que há evidências parciais de governança, sem elementos suficientes para certificar conformidade ou afirmar descumprimento. Propõem-se registros de tratamento, transparência acessível, controles proporcionais ao risco e acompanhamento público das medidas adotadas.

Palavras-chave: Telessaúde; Proteção de dados; LGPD; Governança; Manaus.

ABSTRACT

This article examines whether the expansion of municipal telehealth in Manaus has been accompanied by public evidence of governance and sensitive personal data protection. It adopts a qualitative approach based on legal, bibliographic and documentary research,

covering the regulatory context from 2020 to 2026 and four municipal planning and accountability documents. Data collection ended on October, 2026; service delivery results cover the first four months of that year. The framework combines the Brazilian Constitution, the General Data Protection Law, telehealth legislation, constitutional case law and academic literature published between 2023 and 2026. An analytical matrix connects legal categories, documents, evidence locations and interpretive limits. Findings include institutional planning, proposed training, integration with Gov.br authentication and backup infrastructure planning. However, the documents do not fully demonstrate operation-specific legal bases, retention rules, data sharing, access management or telehealth incident response. The study concludes that governance is partially documented, without sufficient evidence to certify compliance or establish violations. Recommendations include records of processing activities, accessible transparency, risk-based safeguards and public monitoring of adopted measures.
Keywords: Telehealth; Data protection; General Data Protection Law; Governance; Manaus.

1. INTRODUÇÃO

A saúde digital deixou de ser recurso periférico para integrar a organização contemporânea dos serviços de saúde. A mediação tecnológica permite aproximar profissionais, usuários e pontos assistenciais, reduzir deslocamentos e apoiar a continuidade do cuidado. Em Manaus, município marcado por extensa área territorial, desigualdades intraurbanas e conexão regional com comunidades rurais e ribeirinhas, essa possibilidade possui especial relevância. A utilidade social, contudo, não elimina os riscos jurídicos associados ao tratamento intensivo de informações clínicas, cadastrais e

comportamentais. Quanto mais o cuidado depende de plataformas, cadastros, registros, comunicações e integrações, maior é a necessidade de demonstrar por que os dados são coletados, quem pode acessá-los, por quanto tempo serão conservados e quais medidas reduzem usos indevidos.

A telessaúde envolve circulação de informações clínicas entre usuários, profissionais, unidades e sistemas. A ampliação dos pontos de atendimento torna necessário verificar quais salvaguardas acompanham essa circulação. Este artigo delimita seu objeto à governança documental dos dados pessoais sensíveis na telessaúde pública municipal de Manaus, especialmente teleconsulta, teleconsultoria e telemonitoramento. O período de 2020 a 2026 contextualiza a evolução normativa; a análise empírica concentra-se nos instrumentos municipais identificados na metodologia, sem pretender reconstruir todos os atendimentos desse intervalo.

Pergunta-se em que medida a expansão desses serviços foi acompanhada pela evidenciação documental de mecanismos juridicamente adequados de governança e proteção de dados, à luz da Constituição, da LGPD e do marco da telessaúde. A hipótese é que a institucionalização assistencial não corresponde necessariamente ao mesmo grau de demonstração pública das salvaguardas informacionais. A hipótese não pressupõe irregularidade: a inexistência de informação no conjunto examinado não prova a inexistência de uma prática administrativa.

O objetivo geral é avaliar a proteção de dados que pode ser demonstrada pelos documentos públicos selecionados. Especificamente, busca-se reconstruir a evolução normativa, distinguir bases legais e consentimentos, identificar evidências

municipais e propor medidas proporcionais às lacunas encontradas. A contribuição consiste em converter obrigações jurídicas em critérios documentais verificáveis, sem apresentar uma auditoria tecnológica ou uma certificação de conformidade.

A pesquisa é qualitativa, exploratória e descritiva, com revisão bibliográfica narrativa e análise documental orientada por categorias jurídicas. A discussão avança do marco histórico e constitucional para o método, a matriz de resultados e as recomendações. O tratamento da inteligência artificial permanece restrito às perspectivas de governança.

2. FUNDAMENTAÇÃO TEÓRICA

2.1. Evolução Histórica e Normativa da Telessaúde

O dever de resguardar informações obtidas no cuidado antecede a informatização dos serviços. A passagem dos registros em papel para prontuários eletrônicos e plataformas remotas modifica, contudo, a escala de acesso e reprodução. Informações antes consultadas em um estabelecimento podem transitar entre serviços, fornecedores e equipes, inclusive fora do momento da consulta. A proteção precisa alcançar as operações que tornam possível o atendimento e os usos posteriores dos registros.

Zaganelli e Binda Filho (2023) vinculam a confidencialidade dos dados de saúde aos direitos da personalidade e ao sigilo médico. Essa contribuição permite compreender por que a transformação digital não reduz o dever de reserva. Ao mesmo tempo, a confidencialidade profissional, isoladamente, não resolve decisões sobre armazenamento, reutilização, compartilhamento e conservação. A LGPD fornece critérios para examinar esse ciclo,

inclusive quando o dado circula entre agentes que não integram diretamente a relação médico-paciente.

Há, assim, quatro conceitos complementares. Privacidade protege a esfera pessoal e a autonomia; sigilo médico estabelece um dever profissional de confidencialidade; proteção de dados disciplina a legitimidade e os limites das operações informacionais; segurança da informação organiza medidas para preservar confidencialidade, integridade e disponibilidade. Uma plataforma tecnicamente segura pode tratar dados em excesso. Um tratamento dotado de base legal pode continuar vulnerável se os acessos forem inadequados. A avaliação jurídica deve enfrentar ambos os problemas.

A pandemia acelerou o emprego de serviços remotos, mas não constitui a origem da telemedicina. A Lei nº 13.989/2020 autorizou seu uso durante a crise sanitária e determinou esclarecimento ao paciente sobre limitações da modalidade, especialmente as decorrentes da impossibilidade de exame físico. O diploma deve ser tratado como marco histórico, pois foi expressamente revogado pela Lei nº 14.510/2022 (Brasil, 2020a; 2022b).

A Lei nº 14.510/2022 inseriu o Título III-A na Lei nº 8.080/1990 e estabeleceu disciplina nacional para a telessaúde, abrangendo as profissões de saúde regulamentadas. O regime reúne autonomia profissional, consentimento informado, confidencialidade, qualidade assistencial e responsabilidade digital. Seu art. 26-A, III, garante atendimento presencial sempre que solicitado. Não cabe substituir essa garantia por uma condição genérica de conveniência administrativa ou disponibilidade da plataforma.

Santin e Tonial (2024) examinam a transição pandêmica e a convivência entre direito à saúde e proteção de dados. A consolidação legislativa demanda que soluções emergenciais sejam convertidas em serviços sustentáveis, com fluxos conhecidos e responsabilidades definidas. A autorização da modalidade não dispensa a avaliação da adequação clínica de cada atendimento, nem legitima qualquer uso das informações coletadas.

No campo médico, a Resolução CFM nº 2.314/2022 disciplina a telemedicina e suas exigências de registro, confidencialidade e segurança. Sua incidência deve respeitar o âmbito profissional: telessaúde é categoria mais ampla, e as demais profissões possuem regulamentação própria. A análise municipal utiliza a resolução como parâmetro dos atos médicos, sem estendê-la indistintamente a todos os trabalhadores da rede (Conselho Federal de Medicina, 2022).

2.2. Proteção Jurídica dos Dados Pessoais Sensíveis

A Constituição de 1988 assegura intimidade e vida privada, além do direito à saúde. A Emenda Constitucional nº 115/2022 acrescentou ao art. 5º o inciso LXXIX, que reconhece expressamente a proteção dos dados pessoais, inclusive nos meios digitais. A emenda também atribuiu à União competência privativa para legislar sobre a matéria. Isso não afasta o dever municipal de implementar salvaguardas na execução de suas políticas (Brasil, 1988; 2022a).

Antes dessa alteração, o STF já havia enfrentado o problema no referendo da medida cautelar na ADI nº 6.387/DF, julgado em 7 de maio de 2020. A controvérsia envolvia o compartilhamento de dados de usuários de telecomunicações com o IBGE, previsto na Medida

Provisória nº 954/2020. Ao manter a suspensão da medida, a Corte exigiu justificativa suficiente para a finalidade, necessidade e proteção das informações. Trata-se de precedente cautelar sobre outro contexto, e não de julgamento específico da telessaúde de Manaus (Brasil, 2020b).

A aproximação com o presente objeto é interpretativa: o interesse público não elimina a necessidade de demonstrar a proporcionalidade do tratamento. A autodeterminação informativa também não confere poder absoluto de impedir toda operação estatal. Seu conteúdo exige conhecimento dos usos relevantes, exercício de direitos e proteção contra decisões informacionais opacas. Na assistência pública, transparência e fundamentação devem acompanhar inclusive os tratamentos que prescindem de consentimento.

O art. 5º, II, da LGPD inclui informações de saúde entre os dados pessoais sensíveis. A proteção reforçada decorre dos riscos de exposição da intimidade e discriminação. Na telessaúde, o exame não pode limitar-se ao campo denominado diagnóstico: uma especialidade, uma prescrição ou o contexto de uma mensagem pode revelar condição clínica. A combinação de registros também pode produzir inferências sensíveis (Brasil, 2018a).

O tratamento dessa categoria deve enquadrar-se no art. 11. Na prestação pública de saúde, são relevantes as hipóteses de cumprimento de obrigação legal ou regulatória, tratamento compartilhado necessário à execução de políticas públicas previstas em leis ou regulamentos e tutela da saúde em procedimento realizado por profissionais, serviços de saúde ou autoridade sanitária. A seleção depende da operação concreta. A expressão interesse

público, desacompanhada de enquadramento e necessidade, não funciona como autorização irrestrita.

É indispensável distinguir o consentimento para o atendimento remoto do consentimento como base legal para tratar dados. O primeiro integra a autonomia do paciente e a disciplina da telessaúde. O segundo somente é exigido quando escolhido e juridicamente adequado à operação, devendo ser específico e destacado para finalidades determinadas no caso dos dados sensíveis. Um termo único não deve reunir assistência necessária, pesquisa e usos facultativos como se fossem equivalentes. O legítimo interesse do art. 7º, IX, tampouco substitui as hipóteses específicas do art. 11.

Os princípios do art. 6º orientam toda a atividade. A necessidade exige coletar apenas informações pertinentes; a adequação relaciona o uso ao contexto informado; a transparência permite compreender o tratamento; a segurança e a prevenção demandam medidas efetivas. A finalidade assistencial não autoriza automaticamente treinamento de modelos, exploração comercial ou compartilhamentos secundários. Cada mudança deve ser examinada quanto à base, compatibilidade, riscos e deveres de informação.

O princípio da responsabilização e prestação de contas, previsto no art. 6º, X, exige demonstração das medidas adotadas e de sua eficácia. O art. 37 trata dos registros das operações, enquanto o art. 50 admite regras de boas práticas e governança. Esses dispositivos justificam a matriz utilizada na pesquisa: examinam-se documentos capazes de tornar verificável a atuação administrativa, preservada a

distinção entre comprovação formal e efetividade operacional (Brasil, 2018a).

No poder público, os arts. 23 a 30 condicionam o tratamento à finalidade pública e ao exercício de competências legais, com informação clara sobre procedimentos e práticas. A definição de controlador e operador deve refletir quem decide e quem executa cada atividade, sem atribuir automaticamente a mesma condição a todo fornecedor. Contratos devem indicar instruções, acessos autorizados, subcontratações, deveres de cooperação e resposta a incidentes.

O usuário precisa encontrar canais para confirmação do tratamento, acesso, correção e demais direitos aplicáveis. A eliminação não é absoluta: deve observar as hipóteses de conservação do art. 16 e a legislação dos prontuários. A Lei nº 13.787/2018 prevê prazo mínimo de vinte anos a partir do último registro para a possibilidade de eliminação, observados seus requisitos. Por isso, minimização não equivale a apagar indiscriminadamente registros clínicos necessários ou legalmente preservados (Brasil, 2018a; 2018b).

A revisão de Lopes et al. (2025) destaca que a implementação da LGPD na telemedicina depende de ajustes tecnológicos, processos e formação contínua. Gonçalo et al. (2025), ao organizar a literatura sobre regulação dos dados em saúde, articulam inovação, LGPD e governança informacional. Os trabalhos apoiam a escolha de categorias que vão além da existência de uma política escrita. Não permitem, contudo, atribuir ao município os resultados encontrados em outros serviços.

Os artigos 46 a 49 da LGPD determinam medidas técnicas e administrativas aptas a proteger dados contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. A lei adota abordagem baseada em risco: a adequação depende da natureza dos dados, contexto, finalidade, estado da técnica e possíveis danos. Em saúde, confidencialidade, integridade e disponibilidade são igualmente relevantes. Um vazamento pode expor diagnóstico; uma alteração pode prejudicar decisão clínica; indisponibilidade pode interromper cuidado.

Um incidente pode envolver acesso indevido, envio ao destinatário errado, alteração de registro ou indisponibilidade, sem necessariamente haver divulgação pública. A exposição de dados de saúde pode gerar fraude, constrangimento e discriminação; a perda de integridade ou disponibilidade pode comprometer o cuidado. Essas consequências são riscos a prevenir, não ocorrências identificadas pela presente pesquisa.

A Resolução CD/ANPD nº 15/2024 regulamenta a comunicação quando houver possibilidade de risco ou dano relevante. Seus arts. 6º e 9º estabelecem, em regra, três dias úteis para comunicação à ANPD e aos titulares, contados do conhecimento pelo controlador de que o incidente afetou dados pessoais, observadas as regras e ressalvas do regulamento. O fluxo interno deve viabilizar avaliação tempestiva, contenção e preservação de evidências; nem todo evento técnico gera automaticamente dever de comunicação (ANPD, 2024a).

Quanto à reparação, os arts. 42 a 45 da LGPD demandam exame do tratamento, dano e nexo, com as excludentes legais e os demais

regimes aplicáveis. Zaganelli e Binda Filho (2023) registram divergência doutrinária sobre a natureza da responsabilidade na LGPD. Na administração pública, a discussão também deve considerar o art. 37, § 6º, da Constituição. A ausência de informação no corpus não permite imputar responsabilidade civil, aplicar sanções ou identificar falha profissional.

3. METODOLOGIA

A coleta, encerrada em outubro de 2026, utilizou a página Instrumentos de Gestão da SEMSA. Foram selecionados intencionalmente quatro documentos por sua autoria institucional, acesso público e pertinência à implantação ou execução da telessaúde. A pesquisa não constitui revisão sistemática da literatura nem inventário exaustivo das políticas municipais de privacidade. O marco 2020–2026 situa a evolução normativa; os resultados assistenciais de 2026 referem-se somente a janeiro–abril.

O Quadro 1 identifica o corpus e os trechos centrais. A paginação corresponde à numeração impressa, salvo indicação expressa de página do arquivo PDF. O PMS 2026–2029 reúne partes com numeração própria, razão pela qual se informa também a posição no PDF. Os arquivos da PAS e do RDQA trazem no endereço eletrônico a indicação de submissão à aprovação do conselho; sua publicação permite análise documental, mas não foi tomada como prova autônoma de aprovação definitiva.

Quadro 1. Corpus municipal e localização das evidências.

Código e documento	Localização examinada	Função na análise

D1 PMS 2022–2025	p. 100, meta 1.02.02	Previsão de implantação da telessaúde.
D2 PMS 2026–2029	p. 371 e 379; quadro de metas p. 28 e 30 (PDF p. 420 e 422)	Contexto digital e territorial; metas assistenciais e de infraestrutura.
D3 PAS 2026	p. 43 e 48, metas 3.01.12–14 e 4.01.05	Ações de expansão, capacitação, telemonitoramento e backup.
D4 RDQA 1º quadrimestre de 2026	p. 89–90 e 99–100	Execução informada; autenticação; planejamento de infraestrutura.

Fonte: elaboração própria a partir de Manaus (2022; 2026a; 2026b; 2026c).

A leitura dirigida dos trechos foi acompanhada de busca textual por telessaúde, teleconsulta, LGPD, proteção de dados, privacidade, incidente, backup, encarregado, criptografia e retenção, com conferência do contexto. Menções a incidentes assistenciais ou retenção de usuários não foram consideradas evidência de segurança de dados. Não foram acessados prontuários, ambientes autenticados, contratos internos ou registros individuais.

Empregaram-se dez categorias, apresentadas no Quadro 2. Evidência expressa significa descrição direta de medida específica; evidência parcial indica referência genérica, planejamento ou cobertura incompleta do critério; informação não localizada significa ausência de descrição pertinente no recorte. A classificação recai sobre cada achado, sem pontuação agregada de conformidade. As

inferências são limitadas pela finalidade gerencial dos documentos e pela ausência de verificação técnica independente.

O PMS 2026–2029 descreve obstáculos territoriais e de comunicação no acesso de populações rurais aos serviços (Manaus, 2026a, p. 379). Esse contexto exige considerar situações como conexão instável, aparelhos compartilhados, apoio de familiares e dificuldade de compreender interfaces. São condições relevantes para o desenho da política; o presente estudo não mediu sua frequência entre os usuários da telessaúde.

O atendimento assistido deve preservar a possibilidade de fala reservada e limitar o acesso de terceiros ao necessário. Pessoas idosas, pessoas com deficiência e usuários com baixo letramento digital podem precisar de canais alternativos, recursos acessíveis e orientação presencial. Essas medidas concretizam a autonomia sem transferir ao paciente toda a responsabilidade pela segurança. Avisos incompreensíveis e exigências excessivas de autenticação podem se converter em barreiras ao cuidado, devendo ser avaliados juntamente com o risco de exposição.

4. RESULTADOS E DISCUSSÕES OU ANÁLISE DOS DADOS

Os documentos mostram continuidade entre a previsão de implantação em D1 e as metas específicas de D2 e D3. No RDQA, foram informadas 175 teleconsultas e 25 teleconsultorias entre janeiro e abril de 2026, diante de metas anuais de 2.500 e 1.200. O relatório também registra treinamento em andamento para servidores de 30 unidades, redução da equipe de telemonitoramento de 22 para 8 profissionais e integração do login ao Gov.br (Manaus, 2026c, p. 89–90 e 99). Esses dados descrevem

execução e organização; não medem segurança ou satisfação dos usuários.

O Quadro 2 vincula os achados às exigências jurídicas. A anotação de informação não localizada restringe-se a D1–D4 e aos trechos pertinentes ao serviço, sem afirmar que inexista documento específico em outro setor ou canal municipal.

Quadro 2. Matriz de evidências e interpretação jurídica:

Categoria	**Documento e evidência**	**Classificação e interpretação**
1 Finalidade e base legal	D1, p. 100; D2, quadro p. 28; D3, p. 43. Implantação e modalidades assistenciais.	Parcial. Finalidade assistencial identificável; falta vinculação da base legal a cada operação.
2 Necessidade	D3, p. 43, prevê matriz de priorização do telemonitoramento.	Não localizada evidência de minimização. Priorizar atendimento não demonstra redução de campos ou dados.
3 Transparência	D2, p. 371, aborda cultura de proteção de dados; D4 publica metas e execução.	Parcial. Publicidade gerencial não substitui aviso específico sobre o tratamento ao usuário.
4 Controle de acesso	D4, p. 99, meta 4.01.03, registra login integrado ao Gov.br.	Expressa para autenticação declarada; parcial para o eixo. Não demonstra perfis, revisão de privilégios ou auditoria.
5 Segurança e continuidade	D3, p. 48, e D4, p. 100, meta 4.01.05, tratam de expansão e	Parcial. Há planejamento; não há demonstração de testes de recuperação específicos da telessaúde.

	levantamento de backup.	
6 Retenção e compartilhamento	D3, p. 43, prevê qualificação do SIT; prazos e destinatários não são detalhados.	Não localizada informação específica. Integração tecnológica não comprova regras de conservação ou compartilhamento.
7 Capacitação	D3, p. 43, programa formação; D4, p. 89–90, informa capacitação em andamento.	Parcial. Não foi localizada ementa que comprove conteúdo de privacidade e incidentes.
8 Resposta a incidentes	Nos trechos de D1–D4 não foi localizado protocolo de incidentes de dados do serviço.	Informação não localizada. Não permite concluir ausência de protocolo interno ou existência de vazamento.
9 Direitos dos titulares	Não foi localizado, nos trechos examinados, fluxo de pedidos relativos aos dados da telessaúde.	Informação não localizada. Canais gerais de atendimento não comprovam procedimento específico da LGPD.
10 Responsabilização	D3 e D4 identificam áreas responsáveis por metas e resultados.	Parcial. Responsabilidade gerencial não equivale a inventário de operações, matriz de agentes ou avaliação de impacto.

Fonte: elaboração própria. Parâmetros: LGPD, arts. 6º, 11, 18, 23, 37, 46–50; Lei nº 14.510/2022; Resolução CD/ANPD nº 15/2024. D1–D4 conforme Quadro 1.

A institucionalização permite acompanhar metas, mas não demonstra que cada fluxo tenha sido examinado sob a LGPD. Mesmo quando a finalidade assistencial é legítima, permanecem perguntas sobre quais dados são necessários, quais profissionais

devem acessá-los e quais registros precisam ser conservados. A conclusão juridicamente defensável é que o planejamento fornece uma base de organização, cuja tradução em salvaguardas específicas não está integralmente evidenciada.

A autenticação pelo Gov.br é relevante porque identifica uma medida concreta relatada pela gestão. Seu alcance, entretanto, não deve ser ampliado para afirmar eficácia comprovada, cobertura de todos os perfis ou proteção integral. O documento fala em usuários do ecossistema, sem permitir individualizar todos os grupos abrangidos. Autenticar alguém não define quais prontuários essa pessoa pode consultar. A dimensão seguinte da governança envolve autorização, rastreabilidade e revisão de acessos.

Também seria incorreto afirmar ausência completa de preocupação com cópias de segurança. A PAS prevê levantamento da infraestrutura e identificação de dados sensíveis desprotegidos, enquanto o RDQA descreve providências preparatórias para a expansão do backup (Manaus, 2026b, p. 48; 2026c, p. 100). A referência é institucional e não identifica prontuários ou bases específicas afetadas. Por isso, não constitui prova de vazamento, de ausência total de cópias ou de vulnerabilidade determinada da telessaúde.

A capacitação prevista e em andamento deve ser distinguida da formação comprovada em proteção de dados. A conclusão da primeira não certifica a segunda. Essa leitura é compatível com Lopes et al. (2025), que relacionam adequação a tecnologia, processos e educação profissional. A evidência necessária para aprofundar o diagnóstico seria uma ementa, acompanhada de

registros de realização e avaliação, preservados os dados pessoais dos participantes.

O estudo revela uma assimetria documental: os instrumentos tornam mais visíveis metas e produção assistencial do que decisões sobre o ciclo dos dados. A finalidade dos documentos explica parte dessa diferença, pois foram concebidos para planejamento e prestação de contas em saúde. A hipótese recebe apoio apenas nessa dimensão de demonstração pública. Não há base para afirmar que a expansão causou falhas de segurança, que o município descumpre a LGPD ou que o serviço já esteja integralmente conforme.

Como recomendações para o aperfeiçoamento da governança, a primeira medida proposta é consolidar registro das operações de cada modalidade, relacionando finalidade, dados, base legal, responsáveis, destinatários, acessos e conservação. O registro pode orientar uma versão pública simplificada, enquanto informações cuja divulgação gere risco permanecem protegidas. A responsabilidade por sua atualização deve ser definida institucionalmente e exercida com participação da assistência, tecnologia, jurídico e encarregado.

A avaliação de risco deve anteceder novos módulos, integrações e contratações. Recomenda-se considerar relatório de impacto quando o contexto justificar, observadas as hipóteses legais e as determinações da ANPD; o uso de dados sensíveis, por si só, não torna automaticamente obrigatória sua elaboração em toda operação. A ferramenta pode documentar necessidade, alternativas e medidas mitigadoras, sem ser apresentada como certificado definitivo de adequação.

As prioridades operacionais incluem revisão de privilégios, encerramento de acessos após mudança de função, testes de recuperação e regras para fornecedores. Os contratos devem preservar capacidade de supervisão e continuidade, inclusive na troca de plataforma. O diagnóstico preparatório do backup oferece ponto de partida para verificar cobertura e recuperação, sem presumir que capacidade de armazenamento, isoladamente, resolva a segurança.

Propõe-se aviso de privacidade da telessaúde em linguagem simples, com informações sobre finalidades, categorias de dados, compartilhamentos, conservação e canais de direitos. O esclarecimento da modalidade remota deve aparecer de forma distinta das bases legais de tratamento. A apresentação em camadas permite oferecer uma orientação breve antes do atendimento e manter detalhamento disponível para consulta, inclusive nas unidades presenciais.

A formação profissional deve abordar situações concretas: confirmação de identidade, sala reservada, aparelhos compartilhados, envio de documentos e comunicação interna de falhas. O plano de incidentes precisa conciliar contenção, prazos regulatórios e continuidade assistencial. Simulações podem revelar atrasos no acionamento dos responsáveis antes que ocorra um evento real.

O acompanhamento pode incluir proporção de operações mapeadas, acessos revisados, trabalhadores capacitados e tempo de resposta aos titulares, além de testes de recuperação concluídos. São indicadores propostos, sem resultados atribuídos à SEMSA. Sua divulgação agregada, com participação do conselho de saúde, pode

aproximar prestação de contas e experiência do usuário, evitando exposição individual ou publicação de detalhes técnicos exploráveis.

A eventual adoção de triagem automatizada, apoio diagnóstico ou modelos generativos exige avaliação própria. O corpus não demonstra a implantação dessas ferramentas na telessaúde examinada. Farias e Almeida (2026) identificam riscos relacionados a vieses, opacidade e validação clínica, defendendo governança e supervisão humana. Para o município, isso recomenda verificar a população de referência, a qualidade dos dados e a possibilidade de contestar resultados antes da expansão de qualquer solução.

Souza et al. (2024) examinam a atuação da ANPD diante do tratamento de dados pela Meta para treinamento de inteligência artificial. A contribuição pertinente é mostrar a importância da intervenção regulatória e da demonstração de adequação. O caso não envolve prontuários municipais e não autoriza analogia automática sobre ilicitude. Além disso, a suspensão de julho de 2024 foi seguida de autorização de retomada com restrições e plano de conformidade, comunicada pela ANPD em agosto daquele ano (ANPD, 2024b).

O uso assistencial de uma informação não legitima automaticamente sua reutilização para treinar sistemas. Devem ser avaliados base legal, finalidade, necessidade, compartilhamento e riscos de reidentificação. Nos casos abrangidos pelo art. 20 da LGPD, é necessário assegurar o direito de solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado que afetem interesses. A supervisão humana clinicamente adequada é aqui recomendada como salvaguarda, sem atribuir ao dispositivo uma obrigação textual universal de revisão por pessoa natural.

5. CONSIDERAÇÕES FINAIS

A pesquisa identificou evidências parciais de governança e proteção de dados acompanhando a institucionalização da telessaúde em Manaus. Planejamento, capacitação, autenticação e infraestrutura aparecem no corpus com diferentes graus de detalhamento. Esses achados respondem à pergunta dentro do limite documental adotado: há medidas publicamente descritas, mas elas não permitem aferir integralmente a adequação de todas as operações informacionais.

A hipótese recebeu apoio quanto à diferença entre a visibilidade da expansão assistencial e a demonstração dos controles de dados. A conclusão não equivale à comprovação de descumprimento. Tampouco permite afirmar efetividade clínica, inexistência de incidentes ou conformidade tecnológica. O recorte intencional de documentos gerenciais e a ausência de acesso às rotinas internas limitam o alcance dos resultados.

A análise jurídica mostrou que proteção de dados, sigilo, segurança e autonomia do paciente são dimensões complementares. O consentimento para o atendimento remoto não substitui a identificação de bases legais, e a finalidade pública não dispensa proporcionalidade. A realidade territorial e digital exige soluções que preservem privacidade sem dificultar o acesso à assistência.

Recomenda-se desenvolver registros de tratamento, transparência específica, gestão de acessos, avaliação de riscos e resposta a incidentes, com comprovação das medidas realizadas. A matriz contribui ao relacionar obrigações, documentos e limites de inferência. Pesquisas futuras poderão examinar contratos, protocolos

e experiência de usuários e profissionais, mediante acesso autorizado e requisitos éticos aplicáveis, para avaliar se as salvaguardas documentadas se concretizam no cotidiano do cuidado.

REFERÊNCIAS BIBLIOGRÁFICAS

ANPD. **Meta cumpre exigências da ANPD e poderá retomar, com restrições, o uso de dados pessoais para treinamento de inteligência artificial.** Brasília, DF, 30 ago. 2024b. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/meta-cumpre-exigencias-da-anpd-e-podera-retomar-com-restricoes-o-uso-de-dados-pessoais-para-treinamento-de-inteligencia-artificial. Acesso em: 02 out. 2026.

ANPD. **Resolução CD/ANPD nº 15, de 24 de abril de 2024.** Aprova o Regulamento de Comunicação de Incidente de Segurança. Brasília, DF: ANPD, 2024a. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd. Acesso em: 03 out. 2026.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 out. 2026.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022.** Inclui a proteção de dados pessoais entre os direitos e garantias fundamentais. Brasília, DF: Presidência da República, 2022a. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 12 out. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República, 2018a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 out. 2026.

BRASIL. **Lei nº 13.787, de 27 de dezembro de 2018.** Dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. Brasília, DF: Presidência da República, 2018b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13787.htm. Acesso em: 08 out. 2026.

BRASIL. **Lei nº 13.989, de 15 de abril de 2020.** Dispõe sobre o uso da telemedicina durante a crise causada pelo coronavírus. Brasília, DF: Presidência da República, 2020a. Revogada pela Lei nº 14.510/2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l13989.htm. Acesso em: 09 out. 2026.

BRASIL. **Lei nº 14.510, de 27 de dezembro de 2022.** Autoriza e disciplina a prática da telessaúde em todo o território nacional. Brasília, DF: Presidência da República, 2022b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/l14510.htm. Acesso em: 10 out. 2026.

BRASIL. **Supremo Tribunal Federal. Referendo na medida cautelar na Ação Direta de Inconstitucionalidade nº 6.387/DF.** Relatora: Ministra Rosa Weber. Tribunal Pleno, 7 maio 2020b. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165. Acesso em: 10 out. 2026.

CONSELHO FEDERAL DE MEDICINA. **Resolução CFM nº 2.314, de 20 de abril de 2022.** Define e regulamenta a telemedicina. Diário

Oficial da União: seção 1, Brasília, DF, p. 227, 5 maio 2022. Disponível em: https://sistemas.cfm.org.br/normas/arquivos/resolucoes/BR/2022/2314_2022.pdf. Acesso em: 08 out. 2026.

FARIAS, Célio Ramos; ALMEIDA, Verônica Scriptore Freire e. Proteção de dados pessoais sensíveis na saúde digital: desafios jurídico-regulatórios da telemedicina e da inteligência artificial. **Cadernos Ibero-Americanos de Direito Sanitário,** v. 15, e2026016, 2026. Disponível em: https://www.cadernos.prodisa.fiocruz.br/index.php/cadernos/article/view/1421. Acesso em: 14 out. 2026.

GONÇALO, Wemerson; SOUZA, Maria Clara de; SANTOS, Wellington Pinheiro dos; OLIVEIRA, Fábio Henrique Cavalcanti de. Abordagens regulatórias na proteção de dados em saúde: uma revisão integrativa de 2018 a 2023. **Physis:** Revista de Saúde Coletiva, v. 35, n. 1, e350113, 2025. Disponível em: https://www.scielo.br/j/physis/a/56MHDpw9hrMKXYzCWyB77Cp/?lang=pt. Acesso em: 18 out. 2026.

LOPES, Eloisa Karine Braga; LOPES, Filipe Henrique; COLONELLO, Nínive Aguiar; BARROS, Fernando Passos Cupertino de; AVELAR, Renato Silva. Desafios da implementação da Lei Geral de Proteção de Dados em serviços de saúde que fazem uso da telemedicina: uma revisão integrativa. **Cadernos Ibero-Americanos de Direito Sanitário,** v. 14, n. 1, p. 48–61, 2025. Disponível em: https://www.cadernos.prodisa.fiocruz.br/index.php/cadernos/article/view/1238. Acesso em: 04 out. 2026.

MANAUS. Secretaria Municipal de Saúde. **Plano Municipal de Saúde 2022–2025.** Manaus: SEMSA, 2022. Disponível em: https://www.manaus.am.gov.br/semsa/wp-content/uploads/sites/8/2024/12/PMS-2022-2025.pdf. Acesso em: 12 out. 2026.

MANAUS. Secretaria Municipal de Saúde. **Plano Municipal de Saúde 2026–2029.** Manaus: SEMSA, 2026a. Disponível em: https://www.manaus.am.gov.br/semsa/wp-content/uploads/sites/8/2026/01/ilovepdf_merged.pdf. Acesso em: 08 out. 2026.

MANAUS. Secretaria Municipal de Saúde. **Programação Anual de Saúde 2026.** Manaus: SEMSA, 2026b. Disponível em: https://www.manaus.am.gov.br/semsa/wp-content/uploads/sites/8/2026/01/PAS-2026__A-APROVAR-NO-CMS_MAO.pdf. Acesso em: 02 out. 2026.

MANAUS. Secretaria Municipal de Saúde. **Relatório detalhado do 1º quadrimestre de 2026.** Manaus: SEMSA, 2026c. Disponível em: https://www.manaus.am.gov.br/semsa/wp-content/uploads/sites/8/2026/06/RQPC-1o-Quadrimestre-2026__A-APROVAR-NO-CMS.MAO_.pdf. Acesso em: 11 out. 2026.

SANTIN, Janaína Rigo; TONIAL, Maira Dal Conte. Telessaúde e meio ambiente digital no Brasil: post-pandemic innovations. **Revista Direito. UnB,** v. 8, n. 1, p. 215–237, 2024. Disponível em: https://periodicos.unb.br/index.php/revistadedireitounb/article/view/48064. Acesso em: 06 out. 2026.

SOUZA, Alcian Pereira de; SIMAS, Danielle Costa de Souza; JUSTINIANO, Jeibson dos Santos; SOUZA JUNIOR, Albefredo Melo

de; LIMA, Neuton Alves de; CHOY, Marco Aurélio de Lima; SANTOS, Cassio André Borges dos; LIMA, Jonathas Simas de; MARINHO, Vania Maria do Perpétuo Socorro Marques; BARBOSA, Luis Fabian Pereira; SALES, Ricardo Augusto Campolina de; FERNANDES, Tais Batista; BEZERRA, Alessandro de Souza; OLIVEIRA, Lorena Cavalcante de; NUNES, Iza Florêncio. O papel da ANPD na defesa da proteção de dados: análise da suspensão do tratamento de dados pessoais para o treinamento da inteligência artificial pela Meta. **Contribuciones a las Ciencias Sociales,** v. 17, n. 10, e12189, 2024. Disponível em: https://ojs.revistacontribuciones.com/ojs/index.php/clcs/article/view/12189. Acesso em: 02 out. 2026.

ZAGANELLI, Margareth Vetis; BINDA FILHO, Douglas Luis. O sigilo médico e os dados sensíveis na telemedicina à luz da Lei Geral de Proteção de Dados. **RECIIS,** v. 17, n. 3, p. 729–740, 2023. Disponível em: https://www.reciis.icict.fiocruz.br/index.php/reciis/article/view/3689. Acesso em: 02 out. 2026.

---

[1] Pós Graduada em Direito Processual Cível na Universidade Federal do Amazonas – UFAM. Universidade do Estado do Amazonas - UEA. ORCID: https://orcid.org/0009-0005-2867-1839. Lattes: http://lattes.cnpq.br/2423648581014330. E-mail: acesse o artigo original para visualizar o e-mail

[2] Doutor em Ciências pela FEA/USP. Universidade do Estado do Amazonas - UEA. Endereço institucional: Av. Major Gabriel, 767, Centro, Manaus – AM, CEP 69.020-060. ORCID: https://orcid.org/0000-0002-1139-5234. E-mail: acesse o artigo original para visualizar o e-mail

[3] Doutoranda em Direito Ambiental pela Universidade do Estado do Amazonas - UEA. Endereço institucional: Av. Major Gabriel, 767, Centro, Manaus – AM, CEP 69.020-060. ORCID: https://orcid.org/0000-0001-6104-3563. E-mail: acesse o artigo original para visualizar o e-mail