FIOCRUZ | Brasília
ISSN: 2358-1824
Cadernos Ibero-Americanos de Direito Sanitário
Cuadernos Iberoamericanos de Derecho Sanitario

Artigo

Proteção de dados pessoais sensíveis na saúde digital: desafios jurídico-regulatórios da telemedicina e da inteligência artificial

Protection of sensitive personal data in digital health: legal and regulatory challenges of telemedicine and artificial intelligence

Protección de datos personales sensibles en la salud digital: desafíos jurídico-regulatorios de la telemedicina y la inteligencia artificial

Célio Ramos Farias[1]
Universidade Santa Cecília, Santos, SP.
https://orcid.org/0009-0001-9178-4167
celiofariasadv@gmail.com

Verônica Scriptore Freire e Almeida[2]
Universidade Santa Cecília, Santos, SP.
https://orcid.org/0000-0001-5811-7779
veronicafreire@unisanta.br

Resumo

Objetivo: analisar os desafios jurídico-regulatórios da governança da saúde digital no contexto da telemedicina e da inteligência artificial, tendo a proteção de dados pessoais sensíveis como eixo transversal da análise, com foco nas tensões entre privacidade, transparência, responsabilidade jurídica e segurança da informação. **Metodologia:** estudo qualitativo baseado em revisão bibliográfica e análise documental. Foram examinados marcos regulatórios nacionais e internacionais, diretrizes técnicas, resoluções profissionais e estudos publicados entre 2020 e 2025, selecionados pela pertinência, para a análise dos desafios jurídico-regulatórios da saúde digital. Os resultados foram organizados a partir das categorias privacidade e transparência da informação; opacidade e explicabilidade de sistemas algorítmicos; princípios de segurança da informação; e base legal do tratamento de dados pessoais sensíveis. **Resultados:** a digitalização ampliou o acesso aos serviços de saúde e favoreceu a continuidade assistencial, especialmente por meio da telemedicina, mas revelou fragilidades relacionadas à infraestrutura, à interoperabilidade, à responsabilidade profissional e à proteção de dados sensíveis. A inteligência artificial apresentou avanços relevantes no apoio diagnóstico e na organização de fluxos clínicos, coexistindo com riscos jurídicos e éticos associados a vieses algorítmicos, opacidade decisória, baixa explicabilidade e insuficiente validação em ambientes clínicos reais. **Conclusão:** a consolidação da saúde digital exige marcos regulatórios adaptativos, transparência, rastreabilidade, supervisão humana contínua e governança de dados estruturada, além de integração entre inovação tecnológica, governança ética e segurança jurídica, sob pena de aprofundamento de desigualdades, quando limitações socioeconômicas e de literacia digital não são consideradas.

Palavras-chave: Telemedicina; Inteligência Artificial; Governança Digital; Proteção de Dados; Saúde Digital.

[1] Bacharel em Direito, Universidade Santa Cecília, Santos, SP, Brasil.
[2] Doutora Direito Econômico, Universidade de Coimbra, Coimbra, Portugal. Professora Titular, Universidade Santa Cecília, Santos, SP, Brasil.

CC BY
OPEN ACCESS

Abstract

Objective: to analyze the legal and regulatory challenges of digital health governance in the context of telemedicine and artificial intelligence, considering the protection of sensitive personal data as a transversal axis of analysis, with emphasis on the tensions between privacy, transparency, legal responsibility, and information security. **Methodology:** this is a qualitative study based on a literature review and documentary analysis. National and international regulatory frameworks, technical guidelines, professional resolutions, and studies published between 2020 and 2025 were examined, selected for their relevance to the analysis of legal and regulatory challenges in digital health. The results were organized according to the categories of privacy and information transparency; opacity and explainability of algorithmic systems; principles of information security; and the legal basis for the processing of sensitive personal data. **Results:** the digitalization of healthcare has expanded access to health services and strengthened continuity of care, particularly through telemedicine. However, it has also revealed vulnerabilities related to infrastructure, interoperability, professional responsibility, and the protection of sensitive data. Artificial intelligence has shown significant advances in diagnostic support and clinical workflow organization, while also presenting legal and ethical risks associated with algorithmic bias, decision opacity, limited explainability, and insufficient validation in real clinical environments. **Conclusion:** the consolidation of digital health requires adaptive regulatory frameworks, transparency, traceability, continuous human oversight, and structured data governance. It also demands the integration of technological innovation, ethical governance, and legal security, since ignoring socioeconomic constraints and digital literacy limitations may deepen inequalities in access to healthcare.

Keywords: Telemedicine; Artificial Intelligence; Digital Governance; Data Protection; Digital Health.

Resumen

Objetivo: analizar los desafíos jurídico-regulatorios de la gobernanza de la salud digital en el contexto de la telemedicina y la inteligencia artificial, considerando la protección de los datos personales sensibles como eje transversal del análisis, con énfasis en las tensiones entre privacidad, transparencia, responsabilidad jurídica y seguridad de la información.

Metodología: estudio cualitativo basado en revisión bibliográfica y análisis documental. Se examinaron marcos regulatorios nacionales e internacionales, directrices técnicas, resoluciones profesionales y estudios publicados entre 2020 y 2025, seleccionados por su pertinencia para el análisis de los desafíos jurídico-regulatorios de la salud digital. Los resultados se organizaron a partir de las categorías de privacidad y transparencia de la información; opacidad y explicabilidad de los sistemas algorítmicos; principios de seguridad de la información; y base legal del tratamiento de datos personales sensibles. **Resultados:** la digitalización ha ampliado el acceso a los servicios de salud y ha favorecido la continuidad asistencial, especialmente a través de la telemedicina. No obstante, también ha evidenciado fragilidades relacionadas con la infraestructura, la interoperabilidad, la responsabilidad profesional y la protección de datos sensibles. La inteligencia artificial ha presentado avances relevantes en el apoyo diagnóstico y en la organización de los flujos clínicos, coexistiendo con riesgos jurídicos y éticos asociados a sesgos algorítmicos, opacidad decisoria, baja explicabilidad e insuficiente validación en entornos clínicos reales. **Conclusión:** la consolidación de la salud digital exige marcos regulatorios adaptativos, transparencia, trazabilidad, supervisión humana continua y una gobernanza de datos estructurada. Asimismo, requiere la integración entre innovación tecnológica, gobernanza ética y seguridad jurídica, ya que la desconsideración de las limitaciones socioeconómicas y de alfabetización digital puede profundizar desigualdades en el acceso a la atención en salud.

Palabras clave: Telemedicina; Inteligencia Artificial; Gobernanza Digital; Protección de Datos; Salud Digital.

Introdução

A transformação digital da saúde intensificou a adoção de tecnologias como a telemedicina, a inteligência artificial e sistemas avançados de análise de dados, criando um cenário de oportunidades e desafios jurídicos e éticos. Floridi destaca que a expansão dessas ferramentas redefine não apenas processos clínicos, mas também a produção, interpretação e uso de dados, exigindo novos referenciais normativos para assegurar responsabilidade e transparência[1].

A telemedicina consolidou-se como instrumento relevante de ampliação do acesso à assistência, especialmente após a pandemia de COVID-19, contribuindo para a expansão da cobertura e a redução de desigualdades territoriais[2]. No Brasil, sua prática foi regulamentada pela Resolução CFM nº 2.314/2022, que define normas para modalidades de atendimento remoto e para o arquivamento digital de informações clínicas[3]. Apesar dos avanços, persistem lacunas relacionadas à rastreabilidade dos atos médicos, ao consentimento informado e à confidencialidade dos dados, indicando a necessidade de aprimoramento regulatório contínuo[1].

A inteligência artificial em saúde apresenta potencial para apoiar o diagnóstico e a organização dos fluxos assistenciais; contudo, estudos indicam que modelos algorítmicos podem reproduzir vieses decorrentes de dados historicamente desiguais, comprometendo a equidade no cuidado e a responsabilização jurídica[4]. Esses riscos evidenciam a necessidade de mecanismos regulatórios capazes de assegurar a validação, a transparência e a supervisão dos sistemas algorítmicos utilizados em contextos clínicos. Nesse sentido, análises sobre os processos de aprovação conduzidos pela *Food and Drug Administration* (FDA) têm evidenciado lacunas na certificação de dispositivos médicos habilitados para inteligência artificial, reforçando a necessidade de marcos regulatórios que garantam validação independente, auditoria contínua, transparência e governança ética ao longo do ciclo de vida dessas tecnologias[5].

A proteção de dados pessoais sensíveis constitui pilar central da saúde digital. No Brasil, a Lei Geral de Proteção de Dados estabelece requisitos específicos para o tratamento de informações clínicas, como finalidade legítima, minimização, segurança e responsabilização[6]. Apesar disso, estudos e relatórios institucionais apontam a persistência de falhas de segurança em instituições de saúde, incluindo acessos indevidos a prontuários e vulnerabilidades em plataformas digitais, comprometendo a privacidade e a confiança dos usuários[7].

No plano internacional, a Organização Mundial da Saúde orienta que a transformação digital esteja fundamentada em princípios de inclusão, equidade, governança e segurança, conforme expresso na Estratégia Global de Saúde Digital 2020-2025[8]. Nesse contexto, a interoperabilidade dos sistemas é frequentemente apontada como condição para a continuidade do cuidado, embora também amplie riscos relacionados à proteção de dados, exigindo salvaguardas técnicas, jurídicas e organizacionais rigorosas, conforme previsto pela legislação brasileira.

Sistemas fragmentados e pouco protegidos tendem a apresentar maior vulnerabilidade a ataques cibernéticos, como o *ransomware*, cuja incidência no setor saúde tem sido amplamente documentada, com impactos diretos sobre a disponibilidade dos serviços e a segurança do paciente[9]. Além disso, a efetividade das tecnologias digitais depende da capacitação de profissionais e usuários, uma vez que a literacia digital passou a constituir um determinante relevante de saúde, influenciando o acesso e a qualidade do cuidado[10].

Diante desse cenário, torna-se imprescindível analisar de forma integrada os componentes tecnológicos, éticos e jurídicos que estruturam a saúde digital contemporânea. O objetivo deste artigo

é examinar os desafios jurídico-regulatórios da governança da saúde digital a partir da incorporação da telemedicina e da inteligência artificial, tendo a proteção de dados pessoais sensíveis como eixo transversal da análise.

Metodologia

A metodologia deste estudo foi estruturada a partir de revisão documental e revisão bibliográfica, de natureza qualitativa, com o objetivo de analisar os desafios jurídico-regulatórios da governança da saúde digital. A análise tem como eixos a telemedicina e a inteligência artificial em saúde, considerando a proteção de dados pessoais sensíveis como elemento transversal.

A revisão documental concentrou-se na análise de marcos regulatórios e diretrizes institucionais nacionais e internacionais relacionados à governança da saúde digital. No âmbito nacional, foram examinados a Lei Geral de Proteção de Dados Pessoais[6], a Resolução CFM nº 2.314/2022[3], que disciplina a prática da telemedicina no Brasil, bem como documentos institucionais da Autoridade Nacional de Proteção de Dados (ANPD), com destaque para o Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais[11] e o Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Dados Pessoais[12].

No plano internacional, organismos multilaterais têm destacado a necessidade de marcos éticos e regulatórios específicos para o uso da inteligência artificial em saúde, com ênfase na governança, na explicabilidade e na supervisão humana, conforme orientações da Organização Mundial da Saúde e da proposta regulatória da Comissão Europeia para sistemas de inteligência artificial de alto risco[13]. Também foram considerados estudos científicos que examinam os processos regulatórios da *Food and Drug Administration* (FDA) aplicáveis a dispositivos médicos baseados em inteligência artificial, conforme a literatura especializada.

Quadro 1. Documentos normativos e institucionais analisados na revisão documental

Âmbito	Documento / Fonte	Instituição / Órgão	Ano	Descrição
Nacional	Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709[6]	Congresso Nacional / Brasil	2018	Estabelece princípios, direitos, bases legais e obrigações para o tratamento de dados pessoais, incluindo dados pessoais sensíveis no setor da saúde.
Internacional	Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act)[14]	Comissão Europeia	2021	Propõe um marco regulatório baseado em risco para sistemas de inteligência artificial, incluindo aplicações classificadas como de alto risco no setor da saúde.
Internacional	Ethics and Governance of Artificial Intelligence for Health[13]	Organização Mundial da Saúde (OMS)	2021	Estabelece princípios éticos e diretrizes de governança para o uso seguro, transparente e responsável da inteligência artificial em saúde.

Nacional	Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Dados Pessoais[12]	Autoridade Nacional de Proteção de Dados (ANPD)	2021	Apresenta diretrizes sobre medidas técnicas e organizacionais para a proteção de dados pessoais e mitigação de riscos à segurança da informação.
Nacional	Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado[11]	Autoridade Nacional de Proteção de Dados (ANPD)	2022	Esclarece os papéis de controlador, operador e encarregado, orientando a responsabilização e a governança no tratamento de dados pessoais, inclusive em contextos de saúde.
Nacional	Resolução CFM nº 2.314[3]	Conselho Federal de Medicina (CFM)	2022	Define e disciplina a prática da telemedicina no Brasil, estabelecendo responsabilidades profissionais, requisitos técnicos, éticos e limites para o uso de tecnologias digitais na assistência à saúde.

Fonte: Elaborado pelos autores, com base em análise manual do corpus identificado por meio de buscas no *Google Scholar*.

A revisão bibliográfica teve como objetivo analisar produções científicas sobre telemedicina, inteligência artificial em saúde e proteção de dados pessoais sensíveis, considerando seus desdobramentos éticos, regulatórios e sociais no contexto da transformação digital. Foram incluídos artigos científicos, revisões e estudos empíricos, de modo a assegurar uma abordagem abrangente do tema.

As buscas foram realizadas nas bases PubMed, LILACS, SciELO e *The Lancet*, priorizando publicações disponíveis na íntegra em português, inglês e espanhol, com recorte temporal entre 2020 e 2025. Foram excluídos materiais duplicados, estudos fora do escopo e publicações sem acesso ao texto completo, garantindo consistência metodológica e qualidade científica do corpus analisado.

A estratégia de busca bibliográfica foi estruturada a partir de três eixos analíticos: telemedicina, inteligência artificial em saúde e proteção de dados pessoais sensíveis. Foram utilizados descritores dos vocabulários DeCS e MeSH, como *Telemedicine*, *Digital Health*, *Artificial Intelligence*, *Data Protection* e *Cybersecurity*, combinados pelo operador booleano AND, conforme as especificidades de cada base de dados.

Embora o recorte temporal tenha priorizado estudos a partir de 2020, produções anteriores foram incluídas pontualmente por seu caráter teórico. O corpus bibliográfico foi composto por 22 estudos, sintetizados no Quadro 2, segundo título, autoria, ano e veículo de publicação.

Quadro 2. Síntese do corpus bibliográfico analisado

Título	Autor(es)	Ano	Veículo de publicação
The ethics of information	Floridi L[1]	2013	Oxford University Press
What it will take to achieve the as-yet-unfulfilled promises of health information technology	Kellermann AL, Jones SS[7]	2013	Health Affairs
What Is Trust? Ethics and Risk Governance in Precision Medicine and Predictive Analytics	Adjekum A, Ienca M, Vayena E[15]	2017	OMICS
European Union regulations on algorithmic decision-making and a “right to explanation”	Goodman B, Flaxman S[16]	2017	AI Magazine
Good intentions are not enough: how informatics interventions can worsen inequality	Veinot TC, Mitchell H, Ancker JS.[17]	2018	Journal of the American Medical Informatics Association
Dissecting racial bias in an algorithm used to manage the health of populations	Obermeyer Z, Powers B, Vogeli C, Mullainathan S[4]	2019	Science
Artificial intelligence and deep learning in ophthalmology: A review of clinical applications	Ting DSW, et al.[18]	2019	British Journal of Ophthalmology
Machine learning in medicine	Rajkomar A, Dean J, Kohane I[19]	2019	New England Journal of Medicine
Da privacidade à proteção de dados pessoais	Doneda D[20]	2019	Revista dos Tribunais
Telemedicine in the era of COVID-19	Portnoy J, Waller M, Elliott T[2]	2020	Journal of Allergy and Clinical Immunology: In Practice
The role of telehealth during COVID-19 outbreak: a systematic review	Monaghesh E, Hajizadeh A[21]	2020	BMC Public Health
Covid-19 and health care’s digital revolution	Keesara S, Jonas A, Schulman K[22]	2020	New England Journal of Medicine
Telehealth transformation: COVID-19 and the rise of virtual care	Wosik J. et al.[23]	2020	Journal of the American Medical Informatics Association
Explainability for artificial intelligence in healthcare: a multidisciplinary perspective	Amann J et al.[24]	2020	BMC Medical Informatics and Decision Making
Video consultations for covid-19	Greenhalgh T, et al.[25]	2020	BMJ
The ethics of AI in health care: a mapping review	Morley J, et al.[26]	2021	Social Science & Medicine
Inequities in health care services caused by the adoption of digital health technologies: scoping review	Yao R, et al.[27]	2022	Journal of Medical Internet Research
Liability for use of artificial intelligence in medicine	Price WN II, Gerke S, Cohen IG[28]	2022	Research Handbook on

			Health, AI and the Law
Marketing and US Food and Drug Administration clearance of artificial intelligence and machine learning enabled software in and as medical devices: a systematic review	Clark P, Kim J, Aphinyananaphongs Y[5]	2023	JAMA Network Open
Digital literacy as a new determinant of health: A scoping review	Arias López MDP, et al.[10]	2023	PLOS Digital Health
Aplicação de inteligência artificial ao Direito: análise de parâmetros da literatura, da regulação e da percepção de atores sobre limites éticos	Junquilho TA[29]	2023	Universidade de Brasília
Ethical and regulatory challenges of AI technologies in health care: a narrative review.	Mennella C, et al.[30]	2024	Heliyon

Fonte: Elaborado pelos autores a partir da sistematização do corpus bibliográfico identificado nas bases PubMed, LILACS, SciELO e *Google Scholar*.

A sistematização do corpus bibliográfico apresentada no Quadro 2 permitiu identificar convergências, lacunas analíticas e diferentes abordagens teóricas acerca da telemedicina e da inteligência artificial em saúde, especialmente no que se refere aos desafios jurídico-regulatórios da proteção de dados pessoais sensíveis. A partir dessa organização, foi possível estruturar a análise crítica dos estudos selecionados, destacando como a literatura científica aborda as tensões entre privacidade e transparência da informação, explicabilidade de sistemas algorítmicos, segurança da informação e definição de bases legais para o tratamento de dados em saúde.

Resultados e discussão

Os resultados da análise documental e bibliográfica indicam que a transformação digital na saúde tem impactado os modelos assistenciais, as relações jurídico-profissionais e as demandas regulatórias relacionadas à proteção de dados pessoais sensíveis. Essas mudanças se expressam na consolidação da telemedicina, na incorporação da inteligência artificial e no aumento das vulnerabilidades associadas à segurança da informação, exigindo o fortalecimento de estruturas éticas e regulatórias para assegurar transparência, privacidade e segurança no uso de dados em saúde[26].

A análise da literatura selecionada indica que a digitalização dos sistemas de saúde tem produzido, de forma concomitante, oportunidades de inovação e novos riscos jurídicos relacionados ao uso de dados pessoais sensíveis, à interoperabilidade e à incorporação de tecnologias digitais complexas, conforme discutido por Mennella *et al.*[30]. Os autores destacam que a rápida incorporação de soluções baseadas em inteligência artificial no setor saúde exige o fortalecimento de estruturas regulatórias capazes de assegurar segurança da informação, transparência e proteção de direitos fundamentais no tratamento de dados em saúde.

Nesse sentido, a literatura aponta que a adoção acelerada de tecnologias digitais em saúde acentua não apenas o potencial de melhoria da qualidade assistencial, mas também os riscos éticos, normativos e desafios de governança relacionados ao uso de inteligência artificial — em especial

quando há deficiências em explicabilidade, responsabilidade e proteção de dados[24]. Esses riscos tornam evidente a necessidade de marcos regulatórios capazes de acompanhar a complexidade tecnológica e assegurar práticas clínicas seguras, transparentes e juridicamente responsáveis.

A análise das fontes selecionadas organizou os achados do estudo em três eixos: a evolução da telemedicina, a expansão e os desafios da inteligência artificial em saúde e o aprofundamento das vulnerabilidades relacionadas à privacidade, à proteção de dados e à segurança da informação. Esses eixos sintetizam tendências e lacunas regulatórias que demandam aprimoramento normativo à luz dos marcos jurídicos brasileiros e das referências internacionais.

A telemedicina tem se consolidado como ferramenta relevante para ampliar o acesso à saúde, reduzir desigualdades regionais e promover a continuidade assistencial, especialmente no contexto da pandemia de COVID-19, conforme analisado por Monaghesh e Hajizadeh[21]. Os autores destacam que a expansão global da telessaúde permitiu estender o cuidado a populações historicamente afastadas dos grandes centros, sobretudo em regiões remotas, embora persistam obstáculos relacionados à conectividade, à alfabetização digital e à sustentabilidade tecnológica.

No cenário internacional, a telemedicina ganhou protagonismo como mecanismo essencial para a continuidade do cuidado durante a pandemia. Nesse sentido, Keesara *et al*.[22] identificam que essa modalidade atuou como infraestrutura crítica de resposta sanitária, reestruturando fluxos assistenciais e viabilizando o cuidado remoto em larga escala, com a posterior consolidação de modelos híbridos que combinam atendimento presencial e virtual, o que impõe debates permanentes sobre responsabilidade civil, normas técnicas e ética profissional.

De forma complementar, análises conduzidas por Wosik *et al.* indicam que a expansão acelerada da telemedicina evidenciou desafios regulatórios relevantes, especialmente relacionados à interoperabilidade, à segurança da informação e à equidade no acesso, reforçando a necessidade de marcos normativos capazes de acompanhar a complexidade tecnológica e assegurar práticas assistenciais seguras e inclusivas[23].

Evidências indicam que a telemedicina pode manter padrões adequados de segurança e efetividade quando sustentada por protocolos técnicos e capacidade institucional. Wosik *et al*. demonstram que, durante a pandemia de COVID-19, o teleatendimento garantiu continuidade assistencial e apoio à gestão de condições crônicas, desde que apoiado por infraestrutura interoperável e equipes capacitadas[23], evidenciando implicações diretas para o direito sanitário.

Contudo, parcela expressiva dessas tecnologias ainda carece de validação robusta em ambientes clínicos reais, o que suscita preocupações jurídicas, sobretudo quanto a danos ao paciente e à responsabilização civil[18]. No contexto brasileiro, Junquilho sustenta que a adoção de sistemas algorítmicos no setor público demanda estruturas de governança capazes de assegurar transparência informacional, direito à explicação, supervisão humana significativa e mecanismos efetivos de controle e responsabilização institucional, especialmente diante do risco de opacidade decisória e reprodução de vieses em ambientes automatizados[29].

Outro aspecto crítico refere-se à explicabilidade dos sistemas algorítmicos. Rajkomar, Dean e Kohane demonstram que, apesar do elevado desempenho técnico, a complexidade dos algoritmos de aprendizado profundo dificulta a compreensão dos critérios que orientam recomendações clínicas, comprometendo a supervisão profissional e o consentimento informado, o que reforça a necessidade de normativas que assegurem auditabilidade, rastreabilidade e segurança jurídica no uso da inteligência artificial em saúde[19].

A explicabilidade figura entre os principais desafios da inteligência artificial em saúde. Amann *et al*. apontam que sistemas de inteligência artificial sem mecanismos adequados de interpretação dificultam a responsabilização, fragilizam a governança algorítmica e podem ampliar desigualdades quando vieses não são identificados ou corrigidos[24]. Esses achados indicam que a adoção de inteligência artificial deve ser acompanhada de protocolos que assegurem transparência, supervisão humana e mecanismos auditáveis de decisão.

A literatura também destaca o papel central da confiança do paciente na aceitação de tecnologias digitais. Adjekum, Ienca e Vayena demonstram que a confiança depende diretamente da qualidade dos dados, da segurança, da transparência e da possibilidade de supervisão humana, sendo determinante para a adoção segura de sistemas baseados em inteligência artificial[15]. A fragilização desses fatores compromete a legitimidade social e a efetividade da inovação tecnológica nos serviços de saúde.

A proteção de dados e a segurança da informação permanecem como desafios críticos na saúde digital. Relatórios internacionais, como o *Cost of a Data Breach Report*, elaborado pela IBM Security, indicam que o setor da saúde continua sendo um dos mais afetados por incidentes envolvendo informações sensíveis, incluindo vazamentos, acessos indevidos e ataques cibernéticos. Destacam-se, nesse contexto, os ataques do tipo *ransomware*, caracterizados pela invasão de sistemas com bloqueio ou sequestro de dados mediante exigência de resgate financeiro, os quais têm provocado impactos significativos na continuidade dos serviços assistenciais[31].

Apesar dos avanços regulatórios impulsionados pela Lei Geral de Proteção de Dados[6] no contexto brasileiro, persistem fragilidades estruturais relacionadas à gestão de riscos, criptografia, controle de acesso e auditoria dos sistemas, indicando a necessidade de maior amadurecimento institucional, regulatório e operacional nas práticas de segurança da informação em saúde.

No contexto brasileiro, a literatura jurídica e institucional tem incorporado as diretrizes da Autoridade Nacional de Proteção de Dados (ANPD) como referenciais centrais para a aplicação da Lei Geral de Proteção de Dados no setor da saúde. O Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais[11] contribui para a delimitação das responsabilidades entre controladores e operadores, aspecto particularmente relevante em ambientes de telemedicina e no uso de sistemas de inteligência artificial em saúde. Complementarmente, o Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Dados Pessoais[12] enfatiza a necessidade de adoção de medidas técnicas e organizacionais proporcionais aos riscos, reforçando a centralidade da segurança da informação e da governança de dados como eixos estruturantes da saúde digital.

O relatório da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) intitulado *Health Data Governance: Privacy, Monitoring and Research* indica que modelos eficazes de governança de dados em saúde dependem da integração entre privacidade, interoperabilidade e qualidade da informação, elementos essenciais para o uso confiável e responsável dos dados em ambientes digitais[32]. A ausência desses pilares compromete a consistência informacional e eleva riscos clínicos e decisórios, indicando a necessidade de padrões técnicos claros, equipes capacitadas e processos estruturados de gestão da informação.

A segurança cibernética em saúde constitui outro desafio central. Documento da Agência Europeia de Cibersegurança (ENISA) aponta que hospitais, clínicas e plataformas de telemedicina figuram entre os principais alvos de ataques digitais, em razão do alto valor dos dados e da crescente dependência de infraestrutura digital[33]. A literatura indica que a falta de políticas integradas de

segurança e falhas humanas recorrentes ampliam riscos sistêmicos, reforçando a necessidade de capacitação contínua e de fortalecimento da cultura organizacional de segurança da informação.

Documento da Organização Mundial da Saúde, o relatório *Ethics and Governance of Artificial Intelligence for Health*, indica que o uso responsável da inteligência artificial em saúde depende da adoção de princípios éticos e de estruturas robustas de governança, como equidade, transparência, segurança, proteção de dados e supervisão humana contínua, a fim de mitigar vieses algorítmicos e preservar o julgamento clínico[13]. No Brasil, a Pesquisa TIC Saúde 2024 evidencia que, apesar do avanço da informatização, o uso de sistemas mais complexos de inteligência artificial permanece restrito a poucas instituições, coexistindo com lacunas na capacitação profissional, na governança de dados e nas práticas de segurança da informação, sobretudo no setor público[34].

A literatura indica que a transformação digital na saúde amplia o acesso e qualifica a tomada de decisão clínica, mas também impõe desafios regulatórios, éticos e operacionais. Morley *et al*. destacam que a incorporação acelerada de tecnologias digitais exige estruturas robustas de governança capazes de assegurar transparência, proteção de dados pessoais sensíveis e supervisão profissional adequada[26]. À luz dessa análise, o Quadro 3 sintetiza comparativamente os principais benefícios, riscos e desafios regulatórios associados à telemedicina, à inteligência artificial e à proteção de dados no contexto da saúde digital.

Quadro 3. Síntese integrada dos achados sobre telemedicina, Inteligência artificial e proteção de dados na saúde digital

Eixo Analítico	Benefícios Identificados	Riscos e Fragilidades	Demandas Regulatórias e Éticas
Telemedicina	Ampliação do acesso; redução de barreiras territoriais; continuidade do cuidado; eficiência assistencial.	Lacunas na rastreabilidade; limitações de exame físico; perda de pistas não verbais; dependência de conectividade.	Protocolos claros; definição de escopo clínico; segurança da transmissão; consentimento informado; padronização nacional.
Inteligência Artificial em Saúde	Apoio diagnóstico; triagem automatizada; otimização de fluxos; análise preditiva.	Vieses algorítmicos; opacidade decisória; baixa explicabilidade; validação insuficiente; risco de erro automatizado.	Auditorias contínuas; supervisão humana qualificada; transparência; documentação técnica robusta; responsabilidade civil clara.
Proteção de Dados e Segurança da Informação	Fortalecimento da governança; aumento da confiabilidade; apoio à continuidade do cuidado.	Vulnerabilidades cibernéticas; acessos indevidos; incidentes de segurança; riscos para grupos vulneráveis e crianças.	Controles de acesso; criptografia; minimização de dados; avaliação de impacto; conformidade com LGPD e diretrizes internacionais.

Fonte: Elaborado pelos autores, a partir de sistematização analítica manual do corpus bibliográfico e documental, com buscas realizadas no *Google Scholar*.

Um ponto central identificado refere-se à constatação de que o avanço da saúde digital demanda marcos regulatórios atualizados e coerentes, capazes de responder às transformações

introduzidas por tecnologias baseadas em dados e algoritmos. Conforme analisado por Morley *et al*.[26], a incorporação de sistemas de inteligência artificial na saúde produz um ecossistema dinâmico e interdependente, no qual dispositivos conectados, algoritmos clínicos e plataformas digitais operam de forma integrada, exigindo modelos regulatórios flexíveis, interdisciplinares e orientados à mitigação de riscos.

A necessidade de atualização regulatória também é reiterada em análises internacionais sobre políticas de saúde digital. Estudos conduzidos por Wosik *et al*. evidenciam que países com sistemas avançados de telessaúde — como Canadá, Reino Unido e Austrália — avançaram na implementação de modelos híbridos de atendimento, mas continuam a enfrentar desafios estruturais semelhantes aos observados no Brasil, especialmente no que se refere à padronização de práticas, interoperabilidade entre plataformas e garantia de qualidade assistencial[23].

No campo da inteligência artificial, a literatura aponta desafios jurídicos relevantes relacionados à responsabilidade civil, uma vez que, embora sistemas de inteligência artificial possam ampliar a precisão diagnóstica e a eficiência clínica, também introduzem riscos associados a erros algorítmicos, vieses e limitações de explicabilidade. Price, Gerke e Cohen destacam que a questão central não se limita à definição de quem responde por eventuais falhas, mas à forma como essas tecnologias se integram à cadeia decisória clínica e aos padrões de supervisão profissional que devem ser estabelecidos[28].

Nesse sentido, Goodman e Flaxman argumentam que decisões algorítmicas extrapolam as estruturas tradicionais de responsabilização, exigindo modelos regulatórios que assegurem transparência, explicabilidade e mitigação de vieses[16]. Assim, a utilização segura da inteligência artificial em saúde depende da adoção de mecanismos de auditoria, supervisão humana e governança adaptativa, capazes de acompanhar a evolução tecnológica sem comprometer a segurança assistencial e os direitos fundamentais.

Princípios éticos, embora fundamentais, não são suficientes para assegurar o uso seguro e justo da inteligência artificial. Amann *et al*. destacam que valores como transparência e beneficência carecem de efetividade quando não acompanhados por mecanismos concretos de governança, com padrões mensuráveis e estruturas claras de responsabilização[24], evidenciando a necessidade de que ética e regulação avancem de forma integrada no uso da inteligência artificial em saúde.

Em nível internacional, a regulação da inteligência artificial avançou com a aprovação do *AI Act* pela União Europeia, que adota uma abordagem baseada em risco e impõe requisitos rigorosos a sistemas classificados como de alto risco, incluindo aplicações em saúde[14]. Essa experiência oferece ao Brasil uma referência relevante para a construção de modelos de governança capazes de conciliar inovação, proteção de direitos fundamentais e segurança do paciente.

No campo ético, Floridi e Cowls propõem uma estrutura unificada de cinco princípios — beneficência, não maleficência, autonomia, justiça e explicabilidade — que devem orientar o desenvolvimento e o uso responsável da inteligência artificial, especialmente em contextos sensíveis como a saúde, nos quais decisões automatizadas impactam diretamente a integridade, a privacidade e a autonomia dos pacientes[35].

A literatura também evidencia que a digitalização da saúde pode ampliar desigualdades. Estudos de Yao *et al*. indicam que tecnologias digitais tendem a beneficiar grupos com maior renda e letramento digital, enquanto populações com menor acesso permanecem excluídas[27]. Veinot, Mitchell e Ancker reforçam que intervenções em informática em saúde podem agravar desigualdades

quando desconsideram barreiras estruturais, o que impõe a incorporação da equidade como princípio orientador das políticas públicas no Sistema Único de Saúde[17].

Por fim, Greenhalgh *et al*. apontam que, embora a telemedicina seja eficaz em diversos contextos, limitações como dificuldades de exame físico, problemas de conectividade e barreiras de usabilidade podem comprometer a acurácia clínica, especialmente em casos complexos, reforçando a necessidade de critérios claros e protocolos que delimitem adequadamente o uso do atendimento remoto[25].

Nesse mesmo horizonte regulatório, a proteção de dados pessoais sensíveis assume papel estruturante na governança da saúde digital. Diretrizes emitidas pelo *European Data Protection Board* (EDPB) apontam que sistemas conectados de saúde exigem políticas robustas de segurança da informação, abrangendo controle de acesso, criptografia, minimização de dados, registro de logs e auditorias periódicas[36]. Esses documentos convergem com a Lei Geral de Proteção de Dados[6] ao enfatizar que o tratamento de dados em saúde deve observar finalidades legítimas, limitação ao necessário e a adoção de salvaguardas técnicas e organizacionais adequadas.

No contexto brasileiro, essa compreensão foi construída de forma pioneira por Doneda, ao consolidar a transição do paradigma da privacidade para a proteção de dados pessoais como eixo estruturante da regulação contemporânea[20]. A literatura analisada ressalta que falhas nesse campo comprometem não apenas a privacidade, mas também a confiança na relação terapêutica e a disposição dos pacientes em aderir a soluções digitais.

De forma integrada, a discussão evidencia que o avanço da saúde digital depende de marcos normativos sólidos, governança ética e práticas robustas de segurança da informação. Embora telemedicina e inteligência artificial ampliem o acesso e qualifiquem a decisão clínica, sua utilização segura exige regulamentações claras, supervisão contínua e mecanismos efetivos de transparência, tendo a proteção de dados pessoais como eixo transversal indispensável para a legitimidade e a confiança social no contexto da saúde digital.

Considerações Finais

A análise desenvolvida neste artigo, com base na revisão bibliográfica e documental realizada, evidencia que a consolidação da saúde digital tem promovido transformações relevantes na organização dos sistemas de cuidado, ao mesmo tempo em que expõe desafios jurídicos, éticos e institucionais ainda não plenamente equacionados. A literatura analisada demonstra que telemedicina, inteligência artificial e proteção de dados constituem dimensões interdependentes de um mesmo ecossistema regulatório e assistencial.

No campo da telemedicina, os estudos revisados apontam ganhos consistentes na ampliação do acesso, na continuidade do cuidado e na reorganização dos fluxos assistenciais, especialmente em contextos de escassez de profissionais e situações de emergência sanitária. Contudo, permanecem limitações práticas relevantes, como restrições à avaliação clínica presencial, problemas de conectividade, barreiras de usabilidade e desigualdades no acesso digital, o que reforça a necessidade de protocolos claros, critérios clínicos bem definidos e modelos híbridos de atenção.

Em relação à inteligência artificial em saúde, a literatura evidencia avanços expressivos em aplicações de apoio diagnóstico, triagem e priorização clínica, mas destaca riscos recorrentes associados a vieses algorítmicos, opacidade decisória, fragilidades na qualidade dos dados e insuficiente validação em ambientes clínicos reais. Esses achados indicam que a incorporação de

sistemas de inteligência artificial requer estruturas regulatórias capazes de assegurar supervisão humana, transparência, auditoria contínua e responsabilização institucional.

A proteção de dados pessoais sensíveis emerge como eixo transversal indispensável para a legitimidade da saúde digital. A revisão documental aponta convergência entre diretrizes internacionais e o marco normativo brasileiro quanto à exigência de finalidades legítimas, minimização de dados, segurança da informação e salvaguardas técnicas e organizacionais adequadas. Falhas na governança de dados impactam não apenas a privacidade, mas também a qualidade do cuidado, a relação terapêutica e a adesão dos pacientes às soluções digitais.

Dessa forma, conclui-se que o avanço da saúde digital depende menos da disponibilidade tecnológica e mais da capacidade institucional de integrar inovação, regulação e valores éticos de maneira consistente. Regulamentações atualizadas, governança de dados estruturada, capacitação profissional e políticas de inclusão digital configuram condições concretas para que a digitalização da saúde produza benefícios sustentáveis, seguros e socialmente legítimos.

Referências

1. Floridi L. The ethics of information. Oxford: Oxford University Press; 2013. 357 p.

2. Portnoy J, Waller M, Elliott T. Telemedicine in the era of COVID-19. J Allergy Clin Immunol Pract [Internet]. maio 2020 [citado em 6 dez. 2025];8(5):1489-1491. Disponível em: https://pmc.ncbi.nlm.nih.gov/articles/PMC7104202/ doi:10.1016/j.jaip.2020.03.008

3. Brasil. Conselho Federal de Medicina. Resolução CFM nº 2.314, de 20 de abril de 2022. Define e regulamenta a telemedicina, como forma de serviços médicos mediados por tecnologias de comunicação. Diário Oficial da União: seção 1, Brasília, DF, p. 227, 5 maio 2022 [citado em 4 dez. 2025]. Disponível em: https://sistemas.cfm.org.br/normas/arquivos/resolucoes/BR/2022/2314_2022.pdf

4. Obermeyer Z, Powers B, Vogeli C, Mullainathan S. Dissecting racial bias in an algorithm used to manage the health of populations. Science [Internet]. out. 2019 [citado em 4 dez. 2025];366(6464):447-453. Disponível em: https://www.science.org/doi/10.1126/science.aax2342 doi:10.1126/science.aax2342

5. Clark P, Kim J, Aphinyanaphongs Y. Marketing and US Food and Drug Administration clearance of artificial intelligence and machine learning enabled software in and as medical devices: a systematic review. JAMA Netw Open [Internet]. jul. 2023 [citado em 4 dez. 2025];6(7):e2321792. Disponível em: https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2806839 doi:10.1001/jamanetworkopen.2023.21792

6. Brasil. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018 [citado em 4 dez. 2025]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

7. Kellermann AL, Jones SS. What it will take to achieve the as-yet-unfulfilled promises of health information technology. Health Aff (Millwood) [Internet]. jan. 2013 [citado em 4 dez. 2025];32(1):63-68. Disponível em: https://www.healthaffairs.org/doi/10.1377/hlthaff.2012.0693 doi:10.1377/hlthaff.2012.0693

8. World Health Organization. Global strategy on digital health 2020-2025 [Internet]. WHO; 2021 [citado em 4 dez. 2025]. Disponível em: https://www.who.int/publications/i/item/9789240020924

9. Alder S. Healthcare data breach statistics [Internet]. HIPAA Journal; 2023 [citado em 4 dez. 2025]. Disponível em: https://www.hipaajournal.com/healthcare-data-breach-statistics/

10. Arias López MDP, Ong BA, Borrat Frigola X, Fernández AL, Hicklent RS, Obeles AJT, et al. Digital literacy as a new determinant of health: a scoping review. PLOS Digit Health [Internet]. 12 out. 2023 [citado em 4 dez. 2025];2(10):e0000279. Disponível em: https://journals.plos.org/digitalhealth/article?id=10.1371/journal.pdig.0000279 doi:10.1371/journal.pdig.0000279

11. Autoridade Nacional de Proteção de Dados. Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado [Internet]. Brasília: ANPD; 2022 [citado em 8 fev. 2026]. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf

12. Autoridade Nacional de Proteção de Dados. Guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte [Internet]. Brasília: ANPD; 2021 [citado em 8 fev. 2026]. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_seguranca_da_informacao_para_atpps___defeso_eleitoral.pdf

13. World Health Organization. Ethics and governance of artificial intelligence for health [Internet]. Geneva: WHO; 2021 [citado em 7 dez. 2025]. Disponível em: https://www.who.int/publications/i/item/9789240029200

14. European Union. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on artificial intelligence [Internet]. Official Journal of the European Union; 12 jul. 2024 [citado em 8 dez. 2025]. Disponível em: http://data.europa.eu/eli/reg/2024/1689/oj

15. Adjekum A, Ienca M, Vayena E. What is trust? Ethics and risk governance in precision medicine and predictive analytics. OMICS [Internet]. 2017 [citado em 7 dez. 2025];21(12):704-710. Disponível em: https://pubmed.ncbi.nlm.nih.gov/29257733/ doi:10.1089/omi.2017.0156

16. Goodman B, Flaxman S. European Union regulations on algorithmic decision-making and a "right to explanation". AI Mag [Internet]. 2017 [citado em 4 dez. 2025];38(3):50-57. Disponível em: https://doi.org/10.1609/aimag.v38i3.2741 doi:10.1609/aimag.v38i3.2741

17. Veinot TC, Mitchell H, Ancker JS. Good intentions are not enough: how informatics interventions can worsen inequality. J Am Med Inform Assoc [Internet]. 1 ago. 2018 [citado em 8 dez. 2025];25(8):1080-1088. Disponível em: https://doi.org/10.1093/jamia/ocy052 doi:10.1093/jamia/ocy052

18. Ting DSW, Pasquale LR, Peng L, Campbell JP, Lee AY, Raman R, et al. Artificial intelligence and deep learning in ophthalmology: A review of clinical applications. Br J Ophthalmol [Internet]. 2019 [citado em 7 dez. 2025];103(2):167-175. Disponível em: https://pubmed.ncbi.nlm.nih.gov/30361278/ doi:10.1136/bjophthalmol-2018-313173

19. Rajkomar A, Dean J, Kohane I. Machine learning in medicine. N Engl J Med [Internet]. 2019 [citado em 7 dez. 2025];380(14):1347-1358. Disponível em: https://www.nejm.org/doi/10.1056/NEJMra1814259 doi:10.1056/NEJMra1814259

20. Doneda D. Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Revista dos Tribunais; 2019. 432 p.

21. Monaghesh E, Hajizadeh A. The role of telehealth during COVID-19 outbreak: a systematic review based on current evidence. BMC Public Health [Internet]. 2020 [citado em 7 dez. 2025];20:1193. Disponível em: https://pmc.ncbi.nlm.nih.gov/articles/PMC7395209/ doi:10.1186/s12889-020-09301-4

22. Keesara S, Jonas A, Schulman K. Covid-19 and health care's digital revolution. N Engl J Med [Internet]. 2020 [citado em 4 dez. 2025];382(23):e82. Disponível em: https://www.nejm.org/doi/10.1056/NEJMp2005835 doi:10.1056/NEJMp2005835

23. Wosik J, Fudim M, Cameron B, Gellad ZF, Cho A, Phinney D, et al. Telehealth transformation: COVID-19 and the rise of virtual care. J Am Med Inform Assoc [Internet]. 2020 [citado em 7 dez. 2025];27(6):957-962. Disponível em: https://academic.oup.com/jamia/article/27/6/957/5820171 doi:10.1093/jamia/ocaa067

24. Amann J, Blasimme A, Vayena E, Frey D, Madai VI. Explainability for artificial intelligence in healthcare: a multidisciplinary perspective. BMC Med Inform Decis Mak [Internet]. 2020 [citado em 4 dez. 2025];20:310. Disponível em: https://pubmed.ncbi.nlm.nih.gov/33256715/ doi:10.1186/s12911-020-01332-6

25. Greenhalgh T, Wherton J, Shaw S, Morrison C. Video consultations for covid-19. BMJ [Internet]. 12 mar. 2020 [citado em 8 dez. 2025];368:m998. Disponível em: https://www.bmj.com/content/368/bmj.m998 doi:10.1136/bmj.m998

26. Morley J, Machado CCV, Burr C, Cowls J, Joshi I, Taddeo M, et al. The ethics of AI in health care: a mapping review. Soc Sci Med [Internet]. 2020 [citado em 4 dez. 2025];260:113172. Disponível em: https://pubmed.ncbi.nlm.nih.gov/32702587/ doi:10.1016/j.socscimed.2020.113172

27. Yao R, Zhang W, Evans R, Cao G, Rui T, Shen L. Inequities in health care services caused by the adoption of digital health technologies: scoping review. J Med Internet Res [Internet]. 2022 [citado em 8 dez. 2025];24(3):e34144. Disponível em: https://pubmed.ncbi.nlm.nih.gov/35311682/ doi:10.2196/34144

28. Price WN II, Gerke S, Cohen IG. Liability for use of artificial intelligence in medicine. In: Solaiman B, Cohen IG, organizadores. Research handbook on health, AI and the law [Internet]. Cheltenham: Edward Elgar Publishing; 2024 [citado em 7 dez. 2025]. p. 150-166. Disponível em: https://ssrn.com/abstract=4115538 doi:10.4337/9781802205657.ch09

29. Junquilho TA. Aplicação de inteligência artificial ao Direito: análise de parâmetros da literatura, da regulação e da percepção de atores sobre limites éticos [Tese]. Brasília: Programa de Pós-Graduação em Direito, Universidade de Brasília; 2023 [citado em 7 dez. 2025]. Disponível em: https://repositorio.unb.br/handle/10482/48472

30. Mennella C, Maniscalco U, De Pietro G, Esposito M. Ethical and regulatory challenges of AI technologies in healthcare: a narrative review. Heliyon [Internet]. 2024 [citado em 4 dez. 2025];10(4):e26297. Disponível em: https://pubmed.ncbi.nlm.nih.gov/38384518/ doi:10.1016/j.heliyon.2024.e26297

31. IBM Security. Cost of a data breach report 2025 [Internet]. IBM; 2025 [citado em 7 dez. 2025]. Disponível em: https://www.ibm.com/reports/data-breach

32. Organisation for Economic Co-operation and Development. Health data governance: privacy, monitoring and research [Internet]. Paris: OECD Publishing; 2015 [citado em 7 dez. 2025]. Disponível em: https://www.oecd.org/en/publications/health-data-governance_9789264244566-en.html doi:10.1787/9789264244566-en

33. European Union Agency for Cybersecurity. ENISA threat landscape for health sector [Internet]. ENISA; 2023 [citado em 7 dez. 2025]. Disponível em: https://www.enisa.europa.eu/publications/health-threat-landscape

34. Núcleo de Informação e Coordenação do Ponto BR. Pesquisa sobre o uso das tecnologias de informação e comunicação nos estabelecimentos de saúde brasileiros: TIC Saúde 2024 [Internet]. São Paulo: Comitê Gestor da Internet no Brasil; 2025 [citado em 28 dez. 2025]. Disponível em: https://cetic.br/media/docs/publicacoes/2/20250512160746/tic_saude_2024_livro_eletronico.pdf

35. Floridi L, Cowls J. A unified framework of five principles for AI in society. Harvard Data Science Review [Internet]. 2 jul. 2019 [citado em 8 dez. 2025];1(1):1-14. Disponível em: https://doi.org/10.1162/99608f92.8cd550d1

36. European Data Protection Board. Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak [Internet]. EDPB; 21 abr. 2020 [citado em 8 dez. 2025]. Disponível em: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf

Informações editoriais

Histórico

Recebido: 19/11/2025
Revisado: 13/03/2026
Aprovado: 18/03/2026

Processo de Avaliação

Avaliação por pares duplo-cego.

Avaliação por pares aberta

As opções de abertura do processo de avaliação por pares, incluindo a publicação dos pareceres, a divulgação de identidade e a interação entre autores e pareceristas, não foram disponibilizadas para este artigo.

Preprint

O manuscrito não é um *preprint*.

Verificação de similaridade

Este artigo foi submetido à verificação de similaridade textual com o software *CopySpider*.

Contribuição dos autores

Farias C.R. contribuiu com análise e interpretação de dados e redação do artigo.
Almeida V.S.F. contribuiu com revisão crítica de seu conteúdo e aprovação da versão final do artigo.

Conflito de interesses

Os autores declararam não haver nenhum conflito de interesse de ordem pessoal, comercial, acadêmica, política e financeira referente a este artigo.

Financiamento

Não se aplica.

Aprovação ética da pesquisa

Não se aplica.

Disponibilidade dos dados de pesquisa

Não se aplica.

Declaração de uso de ferramentas de Inteligência Artificial (IA)

Não se aplica.

Equipe editorial

Editora-chefe: Sandra Mara Campos Alves
Editora assistente: Amanda Nunes Lopes Espiñeira Lemos
Assistentes editoriais: Danilo Silva Santos Rocha, Daphne Sarah Gomes Jacob Mendes, Maria Ester Simões Nogueira
Revisora de texto: Mirna Barcelos

Publisher

Fundação Oswaldo Cruz, Fiocruz, Programa de Direito Sanitário, Brasília, DF, Brasil

Direitos Autorais

Os autores mantêm os direitos autorais sobre suas obras e concedem aos Cadernos Ibero-Americanos de Direito Sanitário (CIADS) o direito de primeira publicação.

Open Access

Este artigo é publicado em Acesso Aberto (*Open Access*), com acesso imediato, gratuito e permanente ao seu conteúdo, sem cobrança de taxas para leitura, download ou compartilhamento.

Licença de Uso

Copyright © 2026 Célio Ramos Farias, Verônica Scriptore Freire e Almeida. Este artigo é licenciado sob a licença Creative Commons Atribuição 4.0 Internacional (CC BY 4.0), que permite o uso, distribuição e reprodução em qualquer meio, desde que a autoria original e a fonte de publicação sejam devidamente citadas.



Como citar (Vancouver)

Farias CR, Almeida VSF. Proteção de dados pessoais sensíveis na saúde digital: desafios jurídico-regulatórios da telemedicina e da inteligência artificial. Cad. Ibero-Am. Direito Sanit. 2026;15:e2026016. doi: 10.17566/ciads.e2026016