ReGeo
ISSN: 2177-3246

SOFTWARE COMO DISPOSITIVO MÉDICO (SAMD) E A REGULAÇÃO PELA ANVISA: DESAFIOS E OPORTUNIDADES

SOFTWARE AS A MEDICAL DEVICE (SAMD) AND ANVISA'S REGULATORY FRAMEWORK: CHALLENGES AND OPPORTUNITIES

SOFTWARE COMO DISPOSITIVO MÉDICO (SAMD) Y LA REGULACIÓN DE ANVISA: DESAFÍOS Y OPORTUNIDADES

10.56238/revgeov16n5-070

Rodrigo Martos de Morais
Mestrando em Direito Médico
Instituição: Universidade Santo Amaro (UNISA)
Lattes: https://lattes.cnpq.br/4403582235652496
Orcid: https://orcid.org/0009-0007-0322-6979

RESUMO
A regulamentação de Software como Dispositivo Médico (SaMD) pela Agência Nacional de Vigilância Sanitária (ANVISA) tornou-se crucial frente ao avanço das tecnologias digitais em saúde, em especial aquelas baseadas em inteligência artificial (IA). Este artigo analisa os fundamentos conceituais do SaMD, a classificação de risco aplicada pela ANVISA e o processo regulatório associado ao registro, monitoramento e validação de softwares médicos. A partir de uma revisão comparativa das normas nacionais e internacionais — incluindo diretrizes do International Medical Device Regulators Forum (IMDRF) —, discutem-se as exigências de segurança cibernética, rastreabilidade, validação clínica e vigilância pós-mercado. Os resultados evidenciam desafios na adequação das normas ao ritmo acelerado da inovação tecnológica, além de oportunidades para fortalecer a governança digital em saúde. Conclui-se que uma regulação adaptativa, alinhada a padrões globais e à Lei Geral de Proteção de Dados (LGPD), é essencial para garantir a segurança dos pacientes e estimular a inovação sustentável no ecossistema de saúde brasileiro.

Palavras-chave: Software Como Dispositivo Médico. ANVISA. Regulação Sanitária. Inteligência Artificial em Saúde. Segurança Cibernética. LGPD.

ABSTRACT
The regulation of Software as a Medical Device (SaMD) by Brazil's National Health Surveillance Agency (ANVISA) has become essential amid the rapid growth of digital health technologies, particularly those based on artificial intelligence (AI). This paper examines the conceptual foundations of SaMD, ANVISA's risk classification system, and the regulatory process for registration, monitoring, and validation of medical software. Drawing on a comparative analysis of national and international guidelines—especially those issued by the International Medical Device Regulators Forum (IMDRF)—the study highlights requirements for cybersecurity, traceability, clinical validation, and post-market surveillance. Findings reveal challenges in aligning existing regulations with the fast pace of technological innovation, while also identifying opportunities to enhance digital health governance in Brazil. The article concludes that an adaptive and transparent regulatory framework, harmonized

with global standards and compliant with Brazil's General Data Protection Law (LGPD), is vital to ensure patient safety and promote sustainable innovation in the healthcare ecosystem.

Keywords: Software as a Medical Device. ANVISA. Health Regulation. Artificial Intelligence in Healthcare. Cybersecurity. Data Protection.

RESUMEN
La regulación del Software como Dispositivo Médico (SaMD) por parte de la Agencia Nacional de Vigilancia Sanitaria (ANVISA) de Brasil se ha vuelto fundamental ante el avance acelerado de las tecnologías digitales en salud, especialmente las basadas en inteligencia artificial (IA). Este artículo analiza los fundamentos conceptuales del SaMD, la clasificación de riesgo establecida por la ANVISA y el proceso regulatorio para el registro, la validación y la vigilancia poscomercialización de los softwares médicos. Mediante una comparación con las directrices internacionales del International Medical Device Regulators Forum (IMDRF), se examinan los requisitos de ciberseguridad, trazabilidad y validación clínica. Los resultados evidencian los desafíos de adaptar la regulación a la velocidad de la innovación tecnológica, pero también las oportunidades de fortalecer la gobernanza digital en salud. Se concluye que un marco regulatorio flexible, coherente con las normas globales y con la Ley General de Protección de Datos de Brasil (LGPD), es clave para garantizar la seguridad del paciente y fomentar la innovación responsable en el sistema sanitario.

Palabras clave: Software Como Dispositivo Médico. ANVISA. Regulación Sanitaria. Inteligencia Artificial en Salud. Ciberseguridad. Protección de Datos.

1 INTRODUÇÃO

O avanço das tecnologias digitais e da inteligência artificial (IA) vem transformando profundamente o campo da saúde, tanto na prática clínica quanto na gestão de sistemas e políticas públicas. Entre as inovações emergentes, o Software como Dispositivo Médico (SaMD) ocupa papel central, pois permite que algoritmos e aplicações desempenhem funções diagnósticas, terapêuticas ou de monitoramento sem depender de hardware médico dedicado. Essa nova categoria de produto traz consigo benefícios evidentes, como automação, precisão diagnóstica e acesso remoto, mas também desafios inéditos à regulação sanitária, especialmente em países com arcabouços normativos ainda em consolidação, como o Brasil.

A Agência Nacional de Vigilância Sanitária (ANVISA) é o órgão responsável pela regulação e fiscalização de dispositivos médicos no país. Desde o início dos anos 2000, a agência busca adaptar suas normas às transformações tecnológicas que alteram o conceito tradicional de "dispositivo médico". O surgimento dos SaMDs, sobretudo os baseados em IA e aprendizado de máquina (*machine learning*), exige da ANVISA mecanismos regulatórios mais flexíveis e responsivos, capazes de acompanhar ciclos de inovação mais curtos e modelos de atualização contínua de software.

O termo *Software as a Medical Device (SaMD)* foi consolidado pelo International Medical Device Regulators Forum (IMDRF), grupo que reúne autoridades regulatórias de referência, como a FDA (EUA), EMA (União Europeia) e TGA (Austrália). Segundo o IMDRF (2013), SaMD é "qualquer software destinado a uma ou mais finalidades médicas, que realiza essas funções sem ser parte de um dispositivo médico de hardware". Essa definição amplia a fronteira entre software de uso clínico e sistemas de apoio à decisão, incorporando inclusive aplicações baseadas em IA que processam dados para diagnóstico, prognóstico ou recomendação terapêutica.

No Brasil, a regulamentação dos SaMDs está ancorada principalmente na RDC nº 185/2001, que classifica dispositivos médicos de acordo com o risco à saúde. No entanto, esse marco foi originalmente concebido para produtos físicos, o que impõe limitações interpretativas quando aplicado a softwares autônomos. Em resposta, a ANVISA passou a integrar grupos de trabalho internacionais do IMDRF, adotando gradualmente terminologias e classificações harmonizadas. Ainda assim, persistem desafios na aplicação prática dessas diretrizes, sobretudo no que diz respeito à validação de algoritmos, segurança cibernética e atualização de versões.

O ritmo acelerado da inovação digital faz com que as normas regulatórias frequentemente se tornem desatualizadas antes mesmo de sua implementação plena. Softwares médicos podem sofrer modificações substanciais em poucos meses, alterando parâmetros clínicos, fluxos de dados e interações com o usuário. Tais mudanças desafiam a lógica tradicional do registro estático, que pressupõe um produto fixo e inalterado ao longo do tempo.

Outro desafio reside na avaliação da eficácia clínica e da segurança dos algoritmos de IA, cujos comportamentos podem variar conforme o conjunto de dados utilizado no treinamento. Esse fenômeno, conhecido como *data drift*, demanda estratégias regulatórias específicas, como validação contínua, monitoramento pós-mercado e auditorias algorítmicas. No entanto, a literatura científica e os documentos regulatórios brasileiros ainda oferecem pouca orientação detalhada sobre como operacionalizar esses mecanismos em larga escala.

A lacuna de conhecimento identificada neste estudo refere-se, portanto, à necessidade de compreender como a ANVISA pode estruturar um modelo regulatório adaptativo que assegure a segurança do paciente sem inibir a inovação. Embora existam referências internacionais consolidadas, o contexto jurídico e institucional brasileiro impõe particularidades que merecem análise aprofundada.

Diante desse cenário, o presente artigo tem como objetivo analisar os principais desafios e oportunidades na regulamentação de softwares como dispositivos médicos (SaMD) pela ANVISA, destacando convergências e divergências em relação a modelos regulatórios internacionais. A pesquisa busca:

- Descrever a estrutura normativa vigente aplicável aos SaMDs no Brasil;
- Comparar as abordagens da ANVISA com as diretrizes do IMDRF e de outras agências reguladoras (FDA, EMA);
- Identificar lacunas e oportunidades para o aprimoramento do processo regulatório;
- Discutir implicações éticas, técnicas e institucionais da adoção de IA em produtos de saúde.

A principal contribuição do estudo está em oferecer uma visão sistematizada e crítica da regulação de SaMD no Brasil, com enfoque em como a agência pode equilibrar inovação tecnológica e proteção sanitária. O artigo também propõe reflexões sobre governança adaptativa, interoperabilidade normativa e cooperação internacional como pilares para o futuro da regulação digital.

O artigo está estruturado em cinco seções. Após esta introdução, a Seção 2 apresenta o conceito de *Software como Dispositivo Médico* e discute sua classificação de risco sob a ótica da ANVISA e do IMDRF. A Seção 3 descreve os requisitos técnicos e regulatórios aplicáveis aos SaMDs, incluindo aspectos de segurança cibernética, rastreabilidade e validação clínica. A Seção 4 analisa os principais desafios enfrentados pela ANVISA na implementação de uma regulação dinâmica, além das oportunidades de inovação para o setor de saúde digital brasileiro. Por fim, a Seção 5 sintetiza as conclusões e propõe recomendações para o aprimoramento do arcabouço regulatório nacional.

2 SOFTWARE COMO DISPOSITIVO MÉDICO (SAMD) - (SOFTWARE AS A MEDICAL DEVICE)

O termo *Software como Dispositivo Médico* (*Software as a Medical Device – SaMD*) foi cunhado pelo International Medical Device Regulators Forum (IMDRF) para designar qualquer software que realize uma função médica independente de hardware dedicado. Em outras palavras, o SaMD é um produto de software que executa uma finalidade médica autônoma, como diagnóstico, monitoramento ou recomendação terapêutica, sem depender fisicamente de um equipamento médico específico.

A definição do IMDRF (2013) estabelece quatro princípios fundamentais:

1. O software deve ter finalidade médica primária, isto é, estar diretamente relacionado à prevenção, diagnóstico, tratamento ou mitigação de uma condição de saúde;
2. Deve atuar de modo autônomo, ainda que se integre a outros sistemas;
3. O software deve processar dados clínicos ou fisiológicos para gerar resultados de valor médico.
4. Sua função principal não deve ser meramente administrativa ou de apoio logístico, como gestão de agenda ou faturamento hospitalar.

Com base nesses princípios, a fronteira entre "software médico" e "software de gestão" tornou-se mais nítida, embora a aplicação prática dessa distinção ainda gere desafios interpretativos. Por exemplo, sistemas de apoio à decisão clínica baseados em IA podem tanto ser classificados como ferramentas de apoio (fora do escopo da regulação) quanto como SaMDs, dependendo do grau de autonomia e do impacto clínico da decisão gerada.

No Brasil, a ANVISA incorporou progressivamente a terminologia de SaMD a partir de 2019, em consonância com as diretrizes do IMDRF. Embora a RDC nº 185/2001 ainda constitua o principal marco regulatório para dispositivos médicos, a agência passou a reconhecer a necessidade de diferenciar softwares de uso médico autônomo de sistemas embarcados em equipamentos físicos. Em 2022, a RDC nº 657/2022 introduziu ajustes procedimentais e reforçou a importância da validação de desempenho e segurança de software, incluindo aspectos de cibersegurança e rastreabilidade.

Segundo a ANVISA, um software pode ser enquadrado como SaMD quando:

- realiza funções de diagnóstico, monitoramento ou terapia diretamente relacionadas a condições médicas;
- possui impacto potencial sobre decisões clínicas;
- opera de forma autônoma em relação a dispositivos físicos;
- e apresenta risco mensurável à saúde em caso de mau funcionamento.

Softwares de automonitoramento pessoal (por exemplo, *apps* de bem-estar ou contagem de passos) geralmente não são considerados SaMDs, a menos que forneçam informações interpretativas que possam influenciar o tratamento clínico.

A classificação de risco é um elemento central na regulação sanitária de dispositivos médicos. A RDC nº 185/2001 adota quatro classes de risco (I a IV), de acordo com a gravidade potencial do dano à saúde em caso de falha do produto. Para fins de compatibilidade com o IMDRF e com a FDA (Food and Drug Administration), esta pesquisa agrupa as classes brasileiras de forma simplificada em três níveis de risco funcional (baixo, moderado e alto):

Tabela 1

Nível de risco	Descrição	Exemplos típicos
Baixo (Classe I)	Software que executa funções administrativas ou de apoio, sem interferência direta no diagnóstico ou tratamento.	Aplicativos de gestão de saúde, controle de consultas, lembretes de medicação.
Moderado (Classe II)	Software que auxilia na tomada de decisão clínica, mas cuja recomendação é validada por um profissional de saúde.	Sistemas de apoio ao diagnóstico por imagem, monitoramento remoto de pacientes.
Alto (Classes III–IV)	Software que realiza funções críticas ou automatiza decisões médicas com impacto direto no diagnóstico ou terapia.	Algoritmos de triagem de câncer, prescrição automatizada, softwares de radiologia com decisão autônoma.

Fonte: elaborada por mim.

Essa categorização é alinhada às práticas internacionais e permite modular o rigor do processo de registro conforme o risco potencial do produto. Softwares de alto risco demandam estudos clínicos e dossiês técnicos detalhados, enquanto os de baixo risco podem seguir via cadastro simplificado.

O processo de registro de SaMDs na ANVISA envolve avaliação documental e técnica. O fabricante ou detentor do registro deve apresentar um dossiê técnico contendo:

- Descrição completa do software, arquitetura e funcionalidades;
- Evidências de validação e verificação funcional;
- Relatórios de segurança cibernética (conformidade com normas ISO/IEC 27001 e 62304);
- Plano de gerenciamento de riscos segundo a ISO 14971;
- Evidências clínicas de desempenho, quando aplicável;
- Estratégia de monitoramento pós-comercialização (*post-market surveillance*).

A ANVISA adota abordagem baseada em risco, ou seja, quanto maior o potencial impacto do software, mais robustas devem ser as evidências apresentadas. Essa lógica é coerente com a política regulatória internacional e com o princípio de proporcionalidade aplicado pela FDA e pela EMA.

Além disso, a agência exige que os SaMDs mantenham rastreabilidade de versões, com registro de alterações significativas no código-fonte ou na base de dados de treinamento (no caso de IA). Cada atualização que modifique parâmetros clínicos ou resultados diagnósticos deve ser comunicada e, dependendo do impacto, pode requerer reavaliação formal do produto.

Os softwares médicos baseados em IA, particularmente aqueles que utilizam aprendizado de máquina (*machine learning*), introduzem complexidades adicionais. Por natureza, esses algoritmos podem evoluir com o uso, aprendendo com novos dados e alterando seu comportamento ao longo do tempo. Tal característica desafia o modelo regulatório tradicional, que parte do pressuposto de produto estático.

A ANVISA, acompanhando discussões do IMDRF, reconhece a necessidade de um modelo de regulação contínua, baseado em ciclos de atualização controlados e monitoramento de desempenho pós-mercado. Nesse contexto, surgem duas estratégias complementares:

1. *Locked algorithms*: algoritmos fixos, cujas versões permanecem imutáveis após a aprovação. São mais simples de validar, mas menos adaptáveis;
2. *Adaptive algorithms*: algoritmos que se atualizam automaticamente. Requerem mecanismos de controle, auditoria e documentação contínua de desempenho.

Para ambos os casos, a ANVISA recomenda evidências de transparência, interpretabilidade e mitigação de vieses algorítmicos, conforme princípios éticos da OMS e da LGPD (Lei nº 13.709/2018). Assim, a agência começa a consolidar uma política de governança algorítmica em saúde, que integra segurança técnica e responsabilidade ética.

Em comparação com outras jurisdições, o Brasil apresenta avanços normativos importantes, mas ainda carece de orientações específicas para softwares baseados em IA. A FDA, por exemplo, emitiu o *Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning-Based Software as a Medical Device* (2019), que prevê planos pré-aprovados de modificação algorítmica (*predetermined change control plans*). A União Europeia, por sua vez, incorporou o SaMD ao *Medical Device Regulation* (MDR 2017/745), estabelecendo padrões mais claros para auditoria de desempenho e documentação técnica.

A harmonização com o IMDRF é estratégica para o Brasil, pois facilita o reconhecimento internacional de registros e reduz barreiras comerciais para *healthtechs* nacionais. Contudo, a implementação dessa harmonização exige investimento institucional em capacitação técnica, interoperabilidade de sistemas e atualização de procedimentos internos da ANVISA.

O conceito de *Software como Dispositivo Médico (SaMD)* redefine o papel da regulação sanitária na era digital. Ao reconhecer o software como produto médico autônomo, a ANVISA amplia seu escopo de atuação e se aproxima das práticas regulatórias internacionais. Entretanto, os desafios relacionados à rapidez da inovação, à complexidade dos algoritmos e à proteção de dados sensíveis

demandam uma abordagem regulatória mais adaptativa e dinâmica, baseada em princípios de risco, transparência e ética tecnológica.

3 REQUISITOS DE SEGURANÇA E EFICÁCIA

A segurança e a eficácia constituem os pilares fundamentais da regulação de qualquer dispositivo médico, inclusive os baseados em software. No caso dos SaMD, esses princípios se traduzem em protocolos de desenvolvimento, validação e monitoramento contínuo que asseguram a confiabilidade dos resultados clínicos e a proteção do paciente.

A ANVISA estabelece que todo software médico deve ser projetado de modo a minimizar riscos previsíveis durante o ciclo de vida do produto. Essa exigência se fundamenta no princípio da precaução sanitária, previsto na legislação brasileira e harmonizado com as diretrizes internacionais da ISO 14971, que trata da gestão de riscos para dispositivos médicos.

Conforme essa norma, o fabricante deve identificar perigos potenciais (por exemplo, falhas de cálculo, vulnerabilidades cibernéticas ou interpretações errôneas de dados clínicos), avaliar a probabilidade de ocorrência e adotar medidas de mitigação. A cada atualização do software, o relatório de avaliação de risco deve ser revisto, garantindo que novas versões não introduzam riscos não controlados.

Com a crescente integração de SaMDs em ecossistemas digitais, a segurança cibernética tornou-se dimensão crítica da vigilância sanitária. Softwares médicos frequentemente processam dados sensíveis, como históricos clínicos, imagens diagnósticas e parâmetros fisiológicos, cuja exposição pode causar danos éticos e legais significativos.

A ANVISA recomenda que fabricantes implementem protocolos de segurança baseados nas normas ISO/IEC 27001 e IEC 62304, incluindo:

- criptografia de dados em repouso e em trânsito;
- autenticação multifatorial para acesso administrativo;
- registro de logs para auditoria e rastreabilidade de ações;
- planos de resposta a incidentes e correção de vulnerabilidades.

Essas práticas convergem com as disposições da Lei Geral de Proteção de Dados (LGPD), que classifica informações de saúde como dados pessoais sensíveis. Assim, qualquer violação de confidencialidade ou uso indevido de dados em SaMDs pode implicar responsabilidade administrativa e civil, além de penalidades sanitárias.

No contexto internacional, a FDA (EUA) e a EMA (União Europeia) publicaram guias técnicos que associam o cumprimento de normas de cibersegurança à manutenção do registro regulatório. O mesmo caminho começa a ser seguido pela ANVISA, que passou a solicitar planos de manutenção de segurança como parte do dossiê técnico de softwares médicos.

Essa integração entre proteção de dados e vigilância sanitária reflete um movimento global de "regulação convergente", em que requisitos éticos, técnicos e jurídicos formam um sistema integrado de governança digital em saúde.

A eficácia de um SaMD deve ser demonstrada por meio de evidências científicas e clínicas, que comprovem que o software atinge sua finalidade médica com precisão e segurança. Essa exigência varia de acordo com a classe de risco do produto: quanto maior o risco potencial ao paciente, maior o nível de evidência exigido.

A ANVISA segue abordagem compatível com o IMDRF SaMD: Clinical Evaluation Framework (2017), que define três níveis de evidência:

1. Evidência analítica: demonstra a precisão técnica e a reprodutibilidade do algoritmo.
2. Evidência clínica: comprova que os resultados do software são clinicamente válidos e correlacionam-se com práticas médicas reconhecidas.
3. Evidência de uso real: avalia o desempenho em contexto clínico real, com usuários e dados reais, refletindo o impacto do software na prática médica.

A validação clínica é particularmente relevante para softwares que incorporam IA, pois algoritmos podem apresentar viés de treinamento decorrente de bases de dados não representativas. Para mitigar esse risco, a ANVISA recomenda a adoção de conjuntos de dados diversificados e auditáveis, com documentação clara da origem, qualidade e diversidade dos dados.

Além disso, a eficácia deve ser reavaliada periodicamente, por meio de estudos de desempenho pós-mercado, conforme previsto nas normas internacionais de *post-market surveillance*. Esse monitoramento contínuo garante que o software mantenha desempenho satisfatório mesmo diante de atualizações, novos ambientes de uso ou populações clínicas distintas.

A rastreabilidade é condição essencial para a transparência e a responsabilização no uso de SaMDs. O fabricante deve manter registros detalhados de desenvolvimento, versões e decisões algorítmicas, permitindo reconstruir o histórico completo de funcionamento do software.

A ANVISA recomenda que os sistemas incluam:

- identificação única de versão (UID) e histórico de alterações;
- documentação de datasets utilizados em cada etapa de treinamento;
- registro automatizado de decisões clínicas tomadas pelo algoritmo (logs interpretáveis);
- planos de auditoria interna e externa.

Essas medidas são especialmente relevantes em contextos de IA, onde a explicabilidade (*explainability*) é frequentemente limitada. O conceito de auditoria algorítmica emerge, assim, como ferramenta regulatória inovadora: consiste na avaliação independente do comportamento do algoritmo, verificando consistência, precisão e ausência de vieses discriminatórios.

Em consonância com o IMDRF Principles of Transparency for Medical AI (2020), a rastreabilidade também contribui para a construção da confiança pública em tecnologias médicas digitais, um ativo intangível crucial para a adoção sustentável de inovações em saúde.

A regulamentação brasileira prevê que o titular do registro mantenha um sistema de vigilância pós-mercado, com coleta contínua de informações sobre o desempenho e incidentes relacionados ao software. Esse sistema deve contemplar:

- monitoramento ativo de desempenho e falhas;
- registro e comunicação imediata de eventos adversos;
- análise de tendência para identificar deteriorações graduais de desempenho;
- planos de atualização corretiva e revalidação de versões.

Nos casos em que o software opera por meio de aprendizado contínuo, o monitoramento assume caráter dinâmico e preditivo: cada modificação no modelo deve ser acompanhada por métricas de desempenho validadas e armazenadas de forma auditável.

Esse tipo de abordagem, denominada “ciclo de vida regulatório adaptativo”, já é utilizada pela FDA e pela TGA australiana e representa uma tendência crescente nas políticas de regulação de IA médica. A ANVISA vem avançando na direção de incorporar formalmente esse modelo, o que exigirá maior integração entre vigilância sanitária, ciência de dados e engenharia de software.

Apesar dos avanços normativos, persistem desafios significativos na implementação efetiva desses requisitos. Entre eles:

- Capacitação técnica de avaliadores da ANVISA para compreender modelos complexos de IA;
- Limitações na interoperabilidade entre bases de dados clínicas e sistemas regulatórios;
- Falta de diretrizes nacionais específicas para auditoria e explicabilidade algorítmica;
- Custos elevados de conformidade para pequenas empresas e *startups* do setor *healthtech*.

Contudo, esses desafios também representam oportunidades de inovação institucional e tecnológica. A criação de “sandboxes regulatórios”, ambientes controlados de teste supervisionado, pode permitir o desenvolvimento de SaMDs em condições experimentais, sob acompanhamento da ANVISA, reduzindo riscos e estimulando aprendizado conjunto.

Adicionalmente, a adoção de ferramentas de inteligência regulatória (*RegTech*) pode auxiliar a agência na análise automatizada de documentação técnica, promovendo eficiência e transparência no processo de registro.

Os requisitos de segurança e eficácia para SaMDs constituem um sistema integrado de gestão de riscos, validação científica e governança tecnológica. A ANVISA, ao harmonizar suas práticas com o IMDRF e outras autoridades internacionais, busca equilibrar duas dimensões muitas vezes tensionadas: a proteção do paciente e o incentivo à inovação.

A consolidação de uma regulação adaptativa e baseada em evidências é o caminho para assegurar que o software médico continue sendo um instrumento de confiança, e não um vetor de risco, no ecossistema da saúde digital.

4 CONCLUSÃO

A consolidação do Software como Dispositivo Médico (SaMD) como categoria regulatória autônoma representa um marco decisivo na modernização da vigilância sanitária brasileira. A ANVISA, ao reconhecer a natureza singular dos softwares médicos e os riscos associados à sua dinâmica de atualização, demonstra sensibilidade institucional às transformações tecnológicas que redefinem a prática clínica e o próprio conceito de dispositivo médico.

O estudo permitiu identificar que o principal desafio regulatório não reside apenas na elaboração de novas normas, mas na adaptação contínua dos instrumentos já existentes às especificidades do ambiente digital. O ciclo de vida dos SaMDs, caracterizado por versões sucessivas, aprendizado de máquina e integração em ecossistemas de dados, exige um modelo regulatório adaptativo, fundamentado em evidências e suportado por mecanismos de auditoria e rastreabilidade algorítmica. Esse modelo deve ser suficientemente flexível para permitir inovação, mas rigoroso o bastante para garantir segurança e eficácia.

Ao mesmo tempo, a pesquisa revelou importantes oportunidades de avanço institucional e tecnológico. A adoção de ferramentas de inteligência regulatória (RegTech), o desenvolvimento de "sandboxes" regulatórios e o fortalecimento da cooperação internacional no âmbito do IMDRF são caminhos promissores para ampliar a capacidade da ANVISA de atuar de forma responsiva e integrada ao contexto global. Essas estratégias podem reduzir custos regulatórios, acelerar o tempo de aprovação de tecnologias emergentes e estimular o crescimento do setor de *healthtechs* no Brasil.

Do ponto de vista ético e social, a regulação de SaMDs baseada em IA exige a consolidação de uma governança digital responsável, alinhada aos princípios da Lei Geral de Proteção de Dados (LGPD) e às diretrizes de equidade e transparência da Organização Mundial da Saúde (OMS). O futuro da regulação sanitária depende de mecanismos que conciliem inovação tecnológica, proteção de dados e confiança pública, garantindo que a automação e o uso de algoritmos na saúde sejam conduzidos dentro de parâmetros seguros, auditáveis e justos.

Por fim, conclui-se que o fortalecimento da regulação de SaMDs pela ANVISA é condição essencial para a sustentabilidade da transformação digital em saúde. Uma política regulatória proativa, baseada em risco e orientada por evidências, será determinante para posicionar o Brasil como referência regional em inovação responsável. O desafio de equilibrar velocidade tecnológica e prudência sanitária permanecerá no centro desse processo — e dele dependerá a construção de um ecossistema de saúde digital seguro, ético e inclusivo.

REFERÊNCIAS

AGÊNCIA NACIONAL DE VIGILÂNCIA SANITÁRIA (ANVISA). **Resolução RDC nº 185, de 22 de outubro de 2001.** Dispõe sobre o registro, alteração, revalidação e cancelamento de registro de produtos médicos. *Diário Oficial da União*, Brasília, DF, 2001.

AGÊNCIA NACIONAL DE VIGILÂNCIA SANITÁRIA (ANVISA). **Resolução RDC nº 657, de 24 de março de 2022.** Dispõe sobre os requisitos sanitários aplicáveis a softwares médicos e produtos de tecnologia da informação em saúde. *Diário Oficial da União*, Brasília, DF, 2022.

AGÊNCIA NACIONAL DE VIGILÂNCIA SANITÁRIA (ANVISA). **Guia para submissão de Software como Dispositivo Médico (SaMD).** Brasília: ANVISA, 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965/2014 (Lei Geral de Proteção de Dados Pessoais – LGPD). *Diário Oficial da União*, Brasília, DF, 2018.

FOOD AND DRUG ADMINISTRATION (FDA). **Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning-Based Software as a Medical Device (SaMD).** Silver Spring, MD: FDA, 2019. Disponível em: https://www.fda.gov/medical-devices/software-medical-device-samd.

INTERNATIONAL MEDICAL DEVICE REGULATORS FORUM (IMDRF). **Software as a Medical Device (SaMD): Key Definitions.** IMDRF/SaMD WG/N10FINAL:2013. Disponível em: https://www.imdrf.org/.

INTERNATIONAL MEDICAL DEVICE REGULATORS FORUM (IMDRF). **Software as a Medical Device: Clinical Evaluation.** IMDRF/SaMD WG/N41FINAL:2017. Disponível em: https://www.imdrf.org/.

INTERNATIONAL MEDICAL DEVICE REGULATORS FORUM (IMDRF). **Principles of Transparency for Medical Artificial Intelligence.** IMDRF/SaMD WG/N67FINAL:2020. Disponível em: https://www.imdrf.org/.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO).
ISO 14971:2019 – **Medical devices – Application of risk management to medical devices.** Geneva: ISO, 2019.

INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC).
IEC 62304:2006 – **Medical device software – Software life cycle processes.** Geneva: IEC, 2006.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO).
ISO/IEC 27001:2022 – **Information security, cybersecurity and privacy protection – Information security management systems – Requirements.** Geneva: ISO, 2022.

EUROPEAN COMMISSION. **Medical Device Regulation (MDR) 2017/745 of the European Parliament and of the Council.** Official Journal of the European Union, Brussels, 2017.

ORGANIZAÇÃO MUNDIAL DA SAÚDE (OMS). **Guidance on Ethics and Governance of Artificial Intelligence for Health.** Geneva: WHO, 2021. Disponível em: https://www.who.int/publications/i/item/9789240029200.

ORGANIZAÇÃO MUNDIAL DA SAÚDE (OMS). **Global Strategy on Digital Health 2020–2025.** Geneva: WHO, 2020. Disponível em: https://www.who.int/docs/default-source/documents/gs4dh.pdf.

SAMPAIO, R.; SABBATINI, M.; LIMONGI, R. **Diretrizes para o uso ético e responsável da inteligência artificial generativa: um guia prático para pesquisadores.** São Paulo: Intercom, 2024.

UNITED STATES FOOD AND DRUG ADMINISTRATION (FDA). **Artificial Intelligence/Machine Learning-Based Software as a Medical Device Action Plan.** Silver Spring, MD: FDA, 2021.

WORLD HEALTH ORGANIZATION (WHO). **Classification of Digital Health Interventions v2.0.** Geneva: WHO, 2018.