MAYO CLINIC PROCEEDINGS: DIGITAL HEALTH

SPECIAL ARTICLE

Global Harmonization of Artificial Intelligence-Enabled Software as a Medical Device Regulation: Addressing Challenges and Unifying Standards

Sandeep Reddy, MBBS, MSc, PhD

Abstract

The growing incorporation of artificial intelligence (AI) into medical device software offers substantial prospects and regulatory hurdles. As AI software as a medical device (AI-SaMD) continues to advance, ensuring its safety, effectiveness, and security is paramount. Nevertheless, the regulatory environment needs more cohesion, with various regions implementing diverse strategies. This paper underscores the necessity for globally harmonized AI-SaMD regulations by examining key regulatory frameworks from the United States, the European Union, China, and Australia. The article also explores crucial elements for harmonization, including algorithm transparency, risk management, data security, and clinical evaluation. Furthermore, the paper advocates for implementing international standards and global data security protocols, emphasizing the significance of cross-border cooperation to ensure the worldwide safety and efficacy of AI-SaMD.

 ■ Mayo Clin Proc Digital Health 2025;3(1):100191

Artificial intelligence (AI) software as a medical device (AI-SaMD) has the potential to revolutionize patient care, bolster clinical decision-making, and enhance health care systems worldwide.[1] However, the swift progress of these technologies has surpassed the development of regulatory frameworks, calling for harmonized global regulations to safeguard patients, foster trust, and promote innovation.[2,3] As these technologies become increasingly sophisticated and widely adopted, ensuring their safety, effectiveness, and dependability is paramount.[2] The diverse regulatory approaches across different countries and regions pose challenges for manufacturers seeking to enter global markets.[4] This lack of uniformity may impede innovation, limit patient access to cutting-edge medical technologies, and create uncertainty for developers and health care providers. This article examines the pressing need for harmonized global regulations for AI-SaMD, focusing on regulatory frameworks in the United States, the European Union, China, and Australia.

From the Health Management and Leadership Discipline, School of Public Health and Social Work, Faculty of Health, Queensland University of Technology, Brisbane, Queensland

The Current Regulatory Landscape: A Patchwork of Approaches

Artificial intelligence is increasingly being integrated into health care systems worldwide, with various regulatory bodies taking steps to ensure its safe and effective use.[2] Regulatory frameworks are being developed to balance innovation with safety, particularly in the case of AI-driven medical devices.[5] These frameworks often take a risk-based approach, classifying AI systems by their potential impact on patient care and applying more stringent requirements to those with higher risks. In addition to addressing safety concerns, regulators prioritize transparency, accountability, and ethical considerations. Regions such as the United States (US), the European Union (EU), and others are actively shaping their policies, though the specific details and

TABLE 1. Current AI-SaMD Regulatory Landscape in the United States, European Union, China, and Australia

Region	Regulatory Body	Key Regulations and Features
United States	Food and Drug Administration (FDA)	■ AI-SaMD regulation includes the artificial intelligence/machine learning-based software as a medical device action plan. ■ Focus on lifecycle risk management, postmarket surveillance and real-world performance monitoring. ■ Exemptions for certain clinical decision support software under the 21st Century Cures Act.
European Union	Medical devices are regulated at EU member state level but the European Medicines Agency (EMA) is also involved in the regulatory process	■ Most AI-SaMD are classified as a high-risk category under the AI Act. ■ Dual approach by medical device regulation (strict design, development, and postmarket surveillance requirements) and the AI Act (risk-based classification, transparency, human oversight requirements).
China	National medical products administration	■ Development of AI-SaMD regulations as part of China's larger AI development strategy. ■ Focus on balancing innovation with safety. ■ Stringent software registration requirements and regulatory guidance for international manufacturers.
Australia	Therapeutic goods administration (TGA)	■ AI-SaMD falls under the existing medical device regulatory framework. ■ Manufacturers must demonstrate safety and performance with clinical and technical evidence. ■ Includes regulation for AI-SaMD using generative AI, such as chatbots.

AI-SaMD, artificial intelligence into medical device software.

implementation strategies vary.[6] Although the US and the EU have been at the forefront of developing regulatory frameworks for AI-SaMD, other regions, such as China and Australia, are also actively working toward establishing their guidelines and standards (Table 1). This article delineates the diverse regulatory approaches adopted by these regions. The selection of these regions illustrates regulatory measures in regions with substantial AI activity or highlights diverse approaches to regulation.

The United States

The US regulatory approach to AI, particularly in health care, is characterized by a sectoral model that leverages existing federal laws and guidelines and aiming to introduce specific AI legislation and a dedicated federal regulatory authority in the future.[7,8] There needs to be comprehensive federal legislation directly regulating the AI development or prohibiting its use. Instead, the US relies on existing laws like the 21st Century Cures Act, which, for instance, exempts specific clinical decision support software from the Food and Drug Administration (FDA) regulation under conditions. Although comprehensive AI law is still under debate, various frameworks and guidelines offer guidance. These include the SAFE Innovation AI Framework, a bipartisan set of principles encouraging federal AI law-making. However, the FDA plays a central role in regulating the AI-SaMD.[9]

The FDA approaches artificial intelligence/machine learning (AI/ML)-based software from the perspective that if its purpose is to treat, diagnose, cure, mitigate, or prevent diseases, it is classified as a medical device, regardless of its technology.[10] This applies even if the software is consumer-facing, such as an application on a smartphone. This approach is consistent with the FDA's role in ensuring the safety and effectiveness of medical

products. Most AI/ML-based products considered as medical devices are categorized as SaMD. The FDA distinguishes between SaMD and software in a medical device (SiMD). The SiMD is integral to the hardware of a medical device, such as software that controls an X-ray panel. The SaMD, on the contrary, performs its medical purpose without being part of a hardware medical device. The SaMD includes software that aids stroke detection and diagnosis by analyzing magnetic resonance imaging images and computer-aided detection software for detecting breast cancer using medical images.

The FDA employs a risk-based strategy to oversee all medical devices, including SaMD.[10,11] Devices classified as Class I present the lowest risk, such as programs that merely show readings from a continuous glucose monitor. Most Class II devices, deemed moderate to high-risk, necessitate a 510(k) review.[12] This process requires manufacturers to prove to the FDA that their device is substantially equivalent to an existing device with the same intended purpose. Class III devices carrying the highest risk must undergo premarket approval. The FDA acknowledges that the iterative and adaptive nature of AI/ML software used in SaMD presents a unique regulatory challenge, as the AI/ML algorithms can evolve after the SaMD has been distributed and collects data from real-world usage. This has led the FDA to consider modifying its approach to premarket review for AI/ML-driven software changes.

In April 2019, the FDA issued a discussion paper outlining a proposed regulatory framework for AI/ML-based SaMD modifications to enable manufacturers to enhance performance and safeguarding patients from potential risks.[13] The proposed framework is on the basis of a total product lifecycle (TPLC) approach,[14] enabling the FDA to evaluate and monitor a product from premarket development through postmarket performance. The 4 pillars of the proposed TPLC framework are:

- AI/ML-based SaMD developers to report an established quality system that adheres to appropriate standards and regulations, such as analytical and clinical validation. The FDA also expects developers to use good machine learning practice,[15] a best practice for developing an algorithm.
- AI/ML-based SaMD developers will provide a detailed description of the SaMD and the algorithm it uses in the premarket submission. The FDA expects AI/ML-based SaMD developers to anticipate algorithm modifications and describe those modifications as SaMD pre-specifications guidelines.[13] Developers should also explain the methodology used to make changes to the algorithm in an algorithm change protocol.
- The FDA expects manufacturers to evaluate the risk to patients of modifications to their AI/ML-based SaMD. The FDA may require a premarket review for some changes, even if included in the SaMD pre-specifications. The FDA also expects manufacturers to monitor their products and use a risk management approach when developing, validating, and executing algorithm changes.
- The FDA encourages real-world performance monitoring for AI/ML-based SaMD, which would provide the FDA and manufacturers with more information about how these products are used and how they perform. This information can then be used to inform future regulatory decisions and improve the safety and effectiveness of these products.

In January 2021, the FDA published an Action Plan[11] on the basis of stakeholder feedback on the 2019 discussion paper[13] that describes a multipronged approach to regulating AI/ML-based SaMD. The FDA committed to developing guidance on predetermined change control plans (PCCPs) as part of the action plan. The PCCPs allow manufacturers to prespecify planned modifications to their AI/ML-based SaMD and the methodology they will use to implement them. If the modifications are implemented according to the PCCP, manufacturers would not have to submit a new marketing submission each time a change is made. A PCCP would generally include:

- A detailed description of the planned modifications to the device.
- A modification protocol describing the methodology used to develop, validate, and implement the modifications.
- An impact assessment of the benefits and risks of the changes and the risk mitigations.

The FDA published draft guidance on PCCPs in April 2023.[14] The draft guidance describes the PCCP as an approach that would support the ability to modify ML-enabled device software functions and ensuring patient safety and effectiveness. In addition to developing guidance, the FDA supports research to develop methods for evaluating and improving AI/ML algorithms, including identifying and eliminating bias. The FDA is also working to encourage harmonization among technology developers on the development of good machine learning practice.[8,15] The agency plans to update its regulatory framework further on the basis of stakeholder feedback.

The European Union

The AI Act (AIA) exemplifies the EU's risk-based strategy for regulating AI.[16] This comprehensive legislation establishes uniform guidelines for developing, commercializing, and using AI systems across diverse industries, including the health care sector.[7,16] The EU champions a human-centric philosophy toward AI, emphasizing crucial elements such as AI systems' safety, transparency, responsibility, equity, and environmental sustainability. Within the EU AI Act, AI systems are classified into 4 tiers of risk, each with its own set of stipulations and responsibilities:

- Unacceptable risk: AI systems that pose an unacceptable risk to EU fundamental rights and values are strictly prohibited. Examples include systems that manipulate human behavior to circumvent free will or exploit vulnerabilities of specific groups.
- High-risk: This category encompasses AI systems with potentially detrimental impacts on an individual's health, safety, or fundamental rights. High-risk AI systems undergo stringent conformity assessments, either through internal control (self-declaration) or in the case of medical devices, through notified body involvement. The AIA aims to align conformity assessments with sectoral legislations like the medical devices regulation (MDR) and in vitro diagnostic medical devices regulation to ensure consistency and facilitate adherence.
- Limited risk: AI systems with limited risk because of transparency concerns are subject to information and transparency requirements. This ensures users are aware that they interact with an AI system, fostering trust and informed decision-making.
- Minimal risk: AI systems with minimal risk to people face no additional legal obligations under the AIA. However, the legislation encourages providers to voluntarily adhere to the requirements for high-risk AI systems through codes of conduct.

In addition to the AIA, other relevant EU regulations impact AI in health care, such as the general data protection regulation, which governs the processing of personal data and the MDR, which regulates medical devices, including those incorporating AI.[17,18] The MDR, under which AI-SaMD falls, mandates stringent requirements for the design, development, clinical evaluation, and postmarket surveillance of medical devices, including AI-powered ones.[17] The EU's regulatory framework for AI is still under development, with the AIA representing an important milestone in establishing comprehensive rules for this rapidly evolving field.[7,16] The EU's approach emphasizes a balance between fostering innovation and mitigating risks, aiming to establish itself as a global leader in trustworthy AI.

The EU also emphasizes international collaboration in AI governance, particularly with the United States.[19] Aligning AI governance between these regions ensures a democratic approach to AI development and deployment (Table 2). The EU actively participates in international regulatory cooperation to facilitate information exchange on the safety

TABLE 2. Similarities and Differences Between the Current AI-SaMD Regulatory Landscape in the US and EU

Aspect	United States (FDA)	European Union (MDR & AI Act)	Common Features	Differences
Regulatory approach	Centralized through the FDA	Combination of MDR and the horizontal AI Act	Both adopt a risk-based approach to determine regulatory requirements	The US has a centralized regulatory structure, whereas the EU combines multiple regulatory frameworks.
Scope of regulation	Primarily focused on AI-SaMD	Broader scope under the AI Act, potentially capturing more AI systems	Both frameworks focus on lifecycle monitoring and continuous assessment of AI-SaMD	The EU's AI Act has a broader scope, potentially regulating more AI systems than the FDA.
Digital sovereignty	Less emphasis on digital sovereignty	Strong focus on digital sovereignty and data protection (GDPR)	Both stress the importance of transparency in AI algorithms and decision-making processes	The EU places a stronger emphasis on digital sovereignty and data protection (GDPR).
Lessons for harmonization	■ Offers insights into balancing innovation and safety ■ Highlights the importance of adaptive regulation to keep pace with AI development	■ Provides a model for comprehensive risk classification on the basis of the AI Act ■ Emphasizes data protection and digital sovereignty	Both frameworks recognize the need for adaptive regulation to accommodate rapidly evolving AI technologies	Regulatory structure, scope of regulation, and emphasis on digital sovereignty differ considerably.

AI-SaMD, artificial intelligence into medical device software; AI Act, artificial intelligence act; EU, European Union; MDR, medical devices regulation; GDPR, general data protection regulation US, United States.

of medical devices and to promote the adoption of global regulatory guidelines that ensure equivalent levels of health and safety protection globally.[7]

China

The Chinese government's strategy for regulating AI is marked by a dynamic and proactive approach, combining top-down directives with specific regulations for various AI applications.[20] The primary aim is to ensure AI development aligns with national objectives, such as preserving social stability, stimulating economic growth, and achieving technological supremacy, as outlined in documents like the new generation AI development plan (2017).[7,20]

China's regulatory framework for AI considerably emphasizes algorithms employed in content recommendation and synthetic content creation.[7,20] This is exemplified by the provisions on the administration of deep synthesis internet information services, which addresses AI-driven generation or modification of online content, including deepfakes.[7] These regulations underscore China's apprehension regarding AI's potential to disseminate misinformation and disrupt social order. They mandate content labeling, adherence with information controls, and measures to prevent misuse, reporting a pre-emptive approach to mitigating potential risks associated with AI-generated content. Furthermore, China has been shown swift action in response to the rise of generative AI, as evidenced by the draft measures for the management of generative AI services after the widespread adoption of Chat Generative Pretrained Transformer.[7]

The Chinese model of AI governance adopts a phased implementation strategy, beginning with specific regulations on recommendation algorithms and profound synthesis.[20] These initial regulations serve as a foundation for a comprehensive national AI law, indicating China's intention to establish a robust and all-encompassing legal

framework for AI.[7] This approach enables iterative development and refinement of regulations in response to technological advancements and emerging risks. China's strategy reflects a delicate balance between controlling AI's potential risks and fostering innovation to achieve global AI leadership by 2030. The government acknowledges the need to address ethical concerns and potential societal impacts of AI whereas cultivating an environment conducive to technological progress.[20] This is evident in the ongoing discourse surrounding the balance between information control and the promotion of technological development, particularly in the context of generative AI.

The cyberspace administration of China has emerged as a prominent regulatory body for online content, shaping AI governance related to algorithms and content generation.[7] However, the Ministry of Science and Technology influences AI's ethical development and use. The development of AI regulations involves various stakeholders, including think tanks, academics, and industry experts, highlighting a collaborative approach to policymaking, even within a politically constrained environment. In addition to the specific AI regulations, other laws, like the Personal Information Protection Law, influence data handling practices and impact AI development within China.[7]

China is actively developing its regulatory framework for AI-SaMD as part of its broader AI development plan.[20] Critical aspects of China's approach, include the publication of proposals and standards for AI-based medical devices, a focus on balancing innovation promotion with ensuring safety and effectiveness, stringent requirements for software registration, and an emphasis on comprehensive regulatory guidance for international manufacturers. As China continues refining its approach to AI-SaMD regulation, it aims to create a framework that fosters innovation although maintaining high patient safety and product efficacy standards.

Australia

Much like the US, Australia's current approach to AI regulation is characterized by a voluntary and principles-based framework, primarily guided by the AI ethics principles[21] published in 2019. Although not legally binding, these principles aim to foster the development and implementation of safe, secure, and reliable AI. The AI ethics principles prioritize human, societal, and environmental well-being, emphasizing human-centered values and fairness in AI systems. This focus underscores Australia's commitment to ensuring AI benefits all Australians and minimizing potential harm. Australia still needs to enact specific laws or regulations directly governing AI. Existing laws like the Online Safety Act 2021 and the Australian Consumer Law can be applied to address AI-related Issues.[7] However, there is a recognized need for a more comprehensive regulatory framework tailored explicitly to AI.

In Australia, the Therapeutic Goods Administration (TGA) oversees the regulation of all medical devices, such as software, mobile applications, and AI-based systems.[22] The TGA classifies AI as a medical device designed for diagnosing, preventing, monitoring, predicting, forecasting, treating, or alleviating diseases, injuries, or disabilities.[23] This broad definition encompasses numerous AI applications within the health care sector. The regulatory framework for AI medical devices in Australia is governed by the Therapeutic Goods Act 1989 and the Therapeutic Goods (medical devices) Regulations 2002.[7] AI medical devices must be listed on the Australian register of therapeutic goods to be legally distributed in Australia.[22]

Like large language models, software incorporating generative AI is regulated as a medical device if it meets the TGA's definition.[23] This includes AI text-based products like generative pretrained transformer-4, highlighting the TGA's proactive approach to regulating emerging AI technologies. The TGA mandates that developers of AI medical devices, including those using generative AI, provide clinical and technical evidence reporting the product's safety, reliability, and performance.[22,23] This ensures that AI medical devices meet the same rigorous standards as other medical devices. The TGA emphasizes that developers adapting or incorporating large language models into products offered in Australia are considered the manufacturers and are thus responsible for meeting all regulatory obligations,

including those related to privacy, data security, cybersecurity, and advertising.

Australia's approach to AI regulation is evolving. Although the current framework relies on voluntary principles and the application of existing laws, the government is actively exploring more comprehensive regulations, particularly for high-risk AI applications.[7] The TGA's proactive approach to regulating AI as a medical device, including emerging technologies like generative AI, reports a commitment to ensuring AI's safe and effective integration into health care in Australia.

Harmonized Regulation

The varied regulatory frameworks across nations and regions create obstacles for manufacturers aiming to penetrate global markets.[4,5] This inconsistency may hinder progress, restrict patients' access to state-of-the-art medical technologies, and generate ambiguity for developers and health care professionals. Also, the varied regulatory structures may hinder multicenter AI clinical trials.[24,25] There is also likely to be a risk of regulatory arbitrage where AI vendors may market less safe or less efficacious applications in regions with less stringent regulatory processes.[26] There is an urgent requirement for standardized worldwide regulations concerning AI-SaMD that tackle crucial issues in transparency, risk management, data protection, and clinical evidence.[22,27] To ensure patient safety and foster innovation, regulatory frameworks must establish clear guidelines for accountability, risk assessment, data protection, and performance evaluation. This comprehensive approach can build trust among stakeholders and accommodating AI's unique characteristics in health care. The following are the critical components for consideration in developing harmonized regulation (Table 3).

Transparency and Accountability

Transparency and accountability are imperative for fostering trust in AI-SaMD.[2,27] Regulatory frameworks must mandate comprehensive documentation of AI models and decision-making processes for effective

TABLE 3. Critical Components for Harmonized Regulation of AI-SaMD

Component	Key Considerations
Transparency and accountability	- Explainability: Manufacturers must provide clear explanations of how AI models make decisions, particularly for high-risk applications. - Documentation: Detailed records of training data, model architecture, and performance metrics are required. - Accountability: Clear lines of responsibility and liability for developers and manufacturers. - Audit Trails: Systems to track and record decision-making processes for post-hoc analysis.
Risk management	- Continuous risk assessment: ongoing risk evaluation throughout the AI system's lifecycle. - Bias detection and mitigation: manufacturers should identify and address biases, especially those leading to disparate patient outcomes. - Performance monitoring: real-world monitoring for emerging risks. - Adaptive regulation: flexibility to accommodate rapid AI advancements and ensuring safety.
Data security	- Data encryption: Mandate robust encryption for data storage and transmission. - Access controls: Strict access controls to prevent unauthorized access. - Adversarial attack mitigation: resilience against attacks that manipulate AI outputs. - Privacy-preserving techniques: use of privacy-enhancing technologies such as federated learning and differential privacy.
Clinical evidence and performance	- Standardized metrics: establish performance metrics for comparison across AI-SaMD products. - Real-world evidence: guidelines for using real-world data to supplement traditional clinical trials. - Performance monitoring: ongoing postmarket surveillance to ensure performance. - Transparency in reporting: clear reporting of clinical performance and outcomes to inform stakeholders.

AI, artificial intelligence; AI-SaMD, artificial intelligence into medical device software.

oversight. Manufacturers should elucidate their AI models' decision-making, particularly in high-risk applications, and maintain detailed training data records, model architecture, and performance metrics. Systems should track and record decision-making processes for post-hoc analysis. These measures collectively enhance transparency and accountability within the AI-SaMD ecosystem.

Beyond documentation, transparency and accountability encompass rigorous development, deployment, and continuous monitoring of AI technologies.[27] Regulatory frameworks should necessitate regular audits and inspections to verify safety and efficacy, particularly for high-risk medical applications.[13,15,27] Clear guidelines for reporting adverse events or unexpected outcomes should be established to ensure expeditious issue resolution and patient safety. Manufacturers should also implement user-friendly interfaces, enabling health care professionals to comprehend and interpret AI-generated recommendations. This transparency facilitates clinicians in making informed decisions rather than uncritically after automated suggestions. By promoting openness and responsibility, these measures engender public trust and ensure the ethical development and utilization of AI in health care.

Risk Management

Risk management in AI-SaMD faces distinct challenges due to AI's adaptability and potential biases.[2,27] Harmonized regulatory frameworks must integrate comprehensive risk assessment methodologies to ensure patient safety, considering the AI's dynamic nature, which necessitates ongoing risk evaluation throughout the product lifecycle. Frameworks should mandate manufacturers to identify and mitigate biases in AI models, especially those affecting different patient populations. Real-world performance monitoring is essential to identify and address emerging risks.[15] In addition, regulatory frameworks must be flexible to keep pace with AI advancements although upholding stringent safety standards.[1,28] Regular audits and inspections by independent third parties should verify adherence and ensure continuous safety and efficacy. Manufacturers must also implement robust cybersecurity measures to protect AI-SaMD systems from threats and unauthorized access. Finally, a standardized reporting system for AI-SaMD adverse events should be established to identify and resolve issues quickly.

Data Security

Ensuring data security for AI-SaMD is a complex challenge, necessitating comprehensive regulatory standards and robust technical implementations to address data breaches and sophisticated threats like adversarial and cyberattacks.[27] Essential security controls include robust data storage and transmission encryption to protect sensitive patient information, even if intercepted. Strict access controls and authentication mechanisms must limit data exposure to authorized individuals. Manufacturers must prove their systems' resilience against adversarial attacks, which could manipulate AI model outputs, leading to incorrect diagnoses or treatment recommendations.[13,29] This requires rigorous testing and validation. Privacy-enhancing technologies, such as federated learning and differential privacy, should be encouraged or mandated, allowing AI model development and minimizing individual patient data exposure. These measures collectively form a comprehensive security framework to protect against current threats and future challenges in AI-SaMD.

Clinical Evidence and Performance

Clinical evaluation standards for AI-SaMD are essential for ensuring patient safety and treatment efficacy.[11,27] These standards should include comprehensive performance metrics for objectively comparing different AI-SaMD products, such as precision, recall, specificity, positive and negative predictive values, and algorithmic fairness and bias measures. In addition, guidelines for collecting and using real-world data should complement traditional clinical trial evidence, offering a holistic view of AI-SaMD performance in diverse settings.[15] Standardizing postmarket surveillance across regulatory bodies would enhance the ongoing evaluation process, ensuring consistent assessment after market introduction and detecting unforeseen issues or performance degradation over time.[13] Transparent and standardized reporting guidelines for clinical performance and outcomes should also be established. These guidelines would ensure clear communication of AI-SaMD

capabilities and limitations to health care providers and patients, aiding informed decision-making and appropriate use of these technologies in clinical practice. Implementing these measures would foster greater trust in AI-SaMD and support their responsible integration into health care systems.[27]

Recommendations for Harmonized Global Standards

Harmonized global standards for AI-SaMD are crucial for ensuring patient safety, fostering innovation, and facilitating international collaboration.[4,6] The following recommendations aim to create a more consistent, efficient, and effective global ecosystem for AI-SaMD development and deployment by aligning regulatory practices across jurisdictions.

Adoption of International Standards

Adopting international standards is essential for harmonizing global AI-SaMD regulation. Organizations like the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) are pivotal in this process.[30] Key recommendations include ISO/IEC 27001 for information security, ISO 13485 for quality management in medical devices, IEC 62304 for software lifecycle processes, and ISO/IEC 29119 for software testing.[31] These standards ensure quality, safety, and security in AI-SaMD development and deployment, enabling regulators and manufacturers to collaborate within a common framework and ease market entry across jurisdictions.

Beyond these foundational standards, emerging standards address AI's unique challenges in medical devices. For example, ISO/IEC 42001 is being developed for AI management systems, and IEEE P2801 aims to establish ethical considerations for autonomous systems pertinent to AI-SaMD.[27,30,31] Harmonizing regulation through international standards also promotes interoperability and data sharing, which is critical for developing and validating AI algorithms with large, diverse datasets. Adhering to common standards facilitates multicenter clinical trials and postmarket surveillance, enhancing evidence generation for AI-SaMD safety and efficacy. Standardized data governance, privacy protection, and cybersecurity foster trust among patients, health care providers, and regulatory bodies, which is crucial for the widespread adoption of AI-SaMD in clinical practice.[6,27]

Unified Risk Management Framework

A unified risk management approach for AI-SaMD is essential to maintain global safety and efficacy standards. This framework should include comprehensive guidelines addressing AI's unique health care challenges. Integrating best practices from regulatory bodies like the FDA and the EU AI Act can establish a robust foundation for managing AI-SaMD risks across jurisdictions.[13,16] Key components should include a standardized risk classification system to categorize AI-SaMD on the basis of potential impacts on patient safety and health outcomes, enabling appropriate scrutiny and control measures. Continuous risk assessment throughout the AI-SaMD lifecycle is crucial, given that these systems evolve and adapt over time.[13,15] Ongoing evaluation would help identify and address emerging risks as the AI system learns from new data. The framework should also provide clear guidelines for identifying and mitigating bias in AI models, requiring diverse training data to ensure equitable performance across patient populations. Finally, real-world performance monitoring and reporting standards are essential for maintaining safety and efficacy.[11] These protocols would facilitate collecting and analyzing postmarket data, enabling timely detection of adverse events or performance issues and supporting continuous improvement of AI-SaMD systems.

Global Data Security Standards

Establishing standard data security protocols and ensuring adherence across jurisdictions is vital for mitigating security risks associated with AI-SaMD. This requires a multifaceted strategy encompassing technical, regulatory, and operational measures. Robust data storage and transmission encryption standards, aligned with international best practices, are foundational.[27] These standards should protect sensitive patient information from unauthorized access, interception, or manipulation throughout its lifecycle.[11,27] Developing standards for implementing and auditing access controls in AI-SaMD systems is crucial to

maintaining data integrity and confidentiality, ensuring only authorized personnel can access and modify critical information.

Global guidelines should be established for responding to and reporting data breaches and security incidents, facilitating rapid and coordinated responses to minimize security breaches' impact and fostering trust in AI-SaMD systems. Moreover, adopting privacy-enhancing technologies in AI-SaMD development and deployment should be encouraged to protect patient data.[18,27] Technologies such as differential privacy and federated learning can balance the need for data-driven insights with the imperative of protecting individual privacy.[32] Implementing these measures can create a more secure, trustworthy global AI-SaMD ecosystem that safeguards patient information and enabling innovation in health care technology.

Standardized Clinical Evaluation Criteria

Establishing uniform clinical evidence criteria and enhancing transparency for AI-SaMD is vital for improving reliability and comparability across jurisdictions. Standardized performance metrics are crucial for evaluating AI-SaMD products, allowing for meaningful comparisons and informed decisions by regulatory bodies. These metrics should include accuracy, sensitivity, specificity, and robustness across diverse patient populations and clinical settings.[15,27] In addition, harmonized guidelines for using real-world data in AI-SaMD evaluation must reflect realistic conditions and intended clinical use.[1]

Consistent requirements for reporting clinical performance enhance transparency in AI-SaMD evaluation.[2,27] This includes clear communication of the device's limitations, intended use, and potential biases, enabling informed decisions by health care providers and patients. Promoting standards for data interoperability is essential for facilitating multicenter evaluations and performance comparisons, leading to more comprehensive assessments across various health care settings and patient populations. By implementing these standardized clinical evaluation criteria, regulatory bodies and health care providers can ensure rigorous assessment of AI-SaMD, ultimately improving patient safety and health care outcomes.

Cross-Border Collaboration

Countries and organizations can collectively tackle regulatory challenges and unify standards for AI-SaMD with collaborative efforts.[33] Creating a global ecosystem for responsible AI-SaMD development and deployment necessitates cross-border cooperation among regulators, manufacturers, nongovernmental organizations, multilateral institutions, researchers, and other stakeholders.[34] This involves sharing best practices, harmonizing regulatory strategies, and jointly addressing emerging challenges and opportunities.[5,6] Such collaboration ensures that AI-SaMD development prioritizes patient safety, efficacy, and ethical considerations. International working groups, conferences, workshops, and shared knowledge platforms can facilitate this process. These initiatives help develop common frameworks for risk assessment, performance evaluation, and postmarket surveillance. Cross-border collaboration addresses data privacy, security, and interoperability issues, essential for AI-SaMD implementation across different health care systems and regions. By fostering a global regulatory and standardization approach, stakeholders can promote innovation although ensuring AI-SaMD technologies meet consistent quality and safety standards worldwide (Figure).

DISCUSSION

Harmonizing regulations for AI-SaMD is crucial to ensure global safety, efficacy, and innovation in health care. This article outlined the varied regulatory approaches across important jurisdictions, each addressing the unique challenges posed by AI technologies in health care. The diversity in these frameworks underscores the urgent need for coordinated global standards to govern AI-SaMD development, deployment, and monitoring. Such harmonization is essential for fostering a global ecosystem that maximizes AI's potential in health care whereas maintaining rigorous patient safety and data security safeguards. Although it may be impractical to expect all regions to possess identical regulatory structures, there exist essential components that can facilitate regulatory harmonization. Foremost among these is

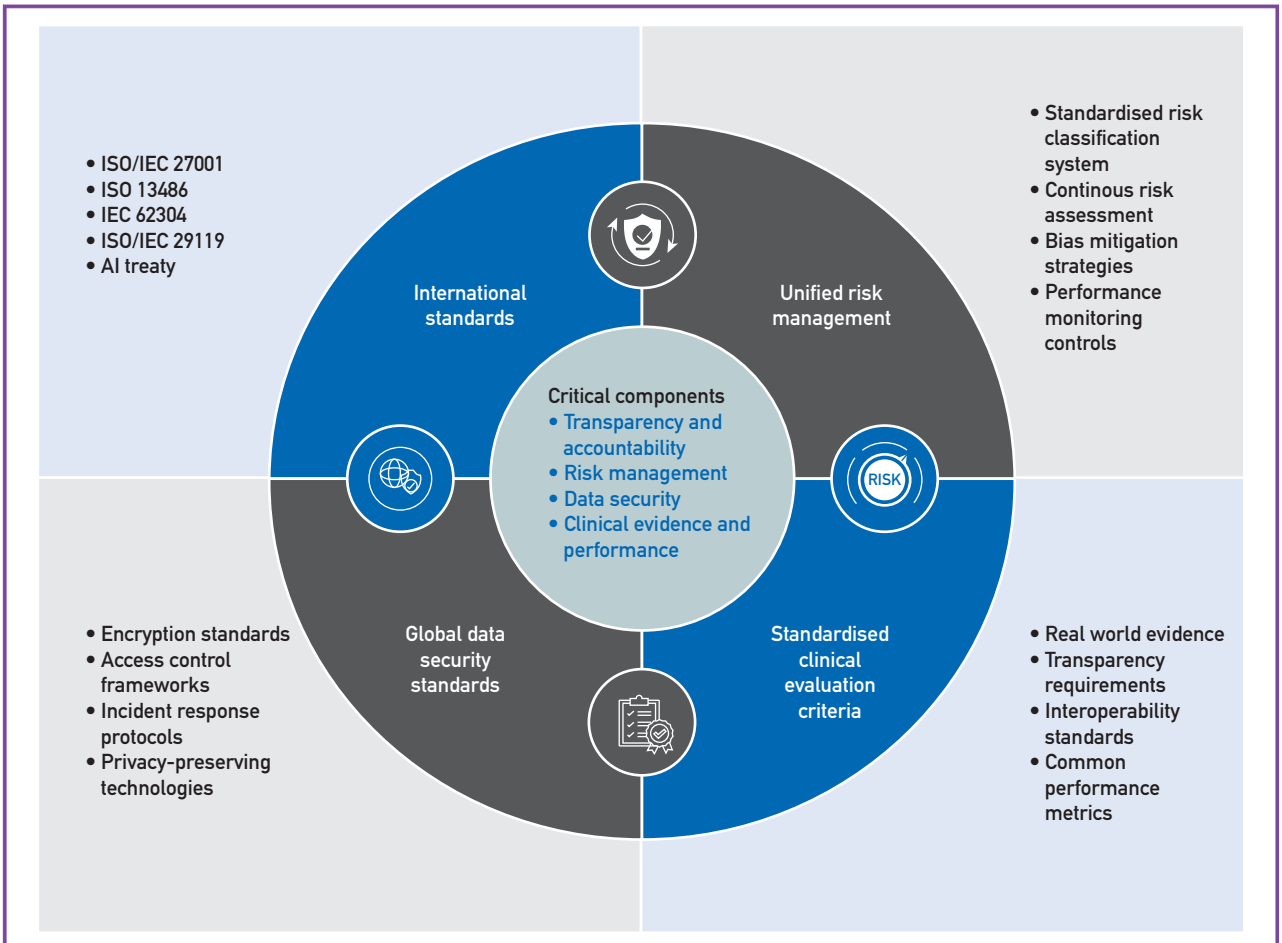

FIGURE. Harmonized regulatory framework for AI-SaMD.

balancing innovation with patient safety and necessitating thoughtful calibration. Transparency and accountability in AI algorithms and decision-making processes are imperative for building trust among health care providers, patients, and regulatory bodies.[27] Developing robust risk management frameworks tailored to AI's adaptive nature and potential for bias is equally crucial. Robust data security standards protect patient information and maintain public trust in AI-SaMD. Standardized clinical evaluation criteria are also indispensable for assessing AI-SaMD performance across jurisdictions, facilitating global collaboration, and ensuring uniform safety and efficacy standards.[11,27]

The path to harmonizing AI-SaMD regulation requires ongoing adaptation to rapidly evolving AI technologies. This entails sustained collaboration among international regulators, manufacturers, and stakeholders to continually refine and update regulatory approaches. Building regulatory capacity, particularly in low-income and middle-income countries, ensures global participation in and adherence to harmonized standards. Addressing emerging ethical considerations and anticipating regulatory challenges posed by developments such as federated learning[32] and edge AI[35] will be critical as AI technologies advance. Of importance, involving patients and the public in developing and evaluating AI-SaMD regulatory frameworks will ensure these technologies serve the needs and respect the rights of those they are designed to benefit.[27]

Addressing these challenges and fostering robust international cooperation will create a regulatory environment that supports responsible AI-SaMD development and deployment, accelerates global health advancements, and improves patient outcomes worldwide.

CONCLUSION

AI-SaMD presents considerable potential to revolutionize health care delivery, offering unprecedented opportunities to enhance patient care and optimize the efficiency of health systems. However, realizing this potential necessitates addressing the fragmented regulatory landscape and fostering greater harmonization of standards and guidelines for AI-SaMD. Through the adoption of international standards, the establishment of a unified risk management framework, the implementation of robust data security protocols, and the prioritization of cross-border collaboration, regulators, manufacturers, and other stakeholders can collectively ensure that AI-SaMD is developed, deployed and utilized safely, effectively, and ethically on a global scale. By embracing a collaborative and forward-looking approach to AI regulation, it is possible to harness the transformative potential of these technologies to create a more equitable and health-oriented future for all.

POTENTIAL COMPETING INTEREST

The author report no competing interests.

Abbreviations and Acronyms: **AI,** artificial intelligence; **AI-SaMD,** AI software as a medical device; **AI/ML,** artificial intelligence/machine learning; **AIA,** artificial intelligence Act; **IEC,** international electrotechnical commission; **ISO,** international organization for standardization; **MDR,** medical devices regulation; **PCCP,** predetermined change control plan; **TGA,** therapeutic goods administration

Correspondence: Address to Sandeep Reddy, MBBS, MSc, PhD, School of Public Health and Social Work, Faculty of Health, Queensland University of Technology, Victoria Park Road, Kelvin Grove, Brisbane-4059, Queensland (sandeep.reddy@qut.edu.au; Twitter: @docsunny100).

REFERENCES

1. Gerke S, Babic B, Evgeniou T, Cohen IG. The need for a system view to regulate artificial intelligence/machine learning-based software as medical device. *npj Digit Med*. 2020;3(1):53. https://doi.org/10.1038/s41746-020-0262-2.
2. Reddy S. Navigating the AI revolution: the Case for precise regulation in health care. *J Med Internet Res*. 2023;25:e49989. https://doi.org/10.2196/49989.
3. Reddy S. Generative AI in healthcare: an implementation science informed translational path on application, integration and governance. *Implement Sci*. 2024;19(1):27. https://doi.org/10.1186/s13012-024-01357-9.
4. McKee M, Wouters OJ. The challenges of regulating artificial intelligence in healthcare Comment on "Clinical Decision Support and New Regulatory Frameworks for Medical Devices: are We Ready for It? — A Viewpoint Paper". *Int J Health Policy Manag*. 2023;12:7261. https://doi.org/10.34172/ijhpm.2022.7261.
5. Palaniappan K, Lin EYT, Vogel S. Global regulatory frameworks for the use of Artificial Intelligence (AI) in the healthcare services sector. *Healthcare (Basel)*. 2024;12(5):562. https://doi.org/10.3390/healthcare12050562.
6. Omabe M. Harmonizing artificial intelligence governance; A model for regulating a high-risk categories and applications in clinical pathology: the evidence and some concerns. *Arch Pathol Clin Res*. 2024;8:001-005.
7. Case W. AI Watch: global regulatory tracker: white and Case. 2024. https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker. Accessed September 3, 2024.
8. Pew. How FDA regulates artificial intelligence in medical products: pew charitable trust; 2021[12th October], https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2021/08/how-fda-regulates-artificial-intelligence-in-medical-products. Accessed September 5, 2024.
9. Wilmerhale. Congress and the White House Announce Framework, Working Group and Plans to Address Risks Associated with AI: WilmerHale. 2023. https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20230628-congress-and-the-white-house-announce-framework-working-group-and-plans-to-address-risks-associated-with-ai. Accessed September 3, 2024.
10. FDA. Artificial intelligence and machine learning in software as a medical device; 2024. Food and Drug Administration. https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device. Accessed September 3, 2024.
11. FDA. Artificial Intelligence/Machine Learning (AI/ML)-Based Software as aMedical Device (SaMD) Action Plan. In: Food and Drug Administration; 2021. https://www.fda.gov/media/145022/download?attachment. Accessed August 29, 2024.
12. FDA. Deciding when to submit a 510(k) for a change to an existing device. In: *Food and Drug Administration*. Administration FaD; 2017. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/deciding-when-submit-510k-software-change-existing-device. Accessed September 2, 2024.
13. FDA. Proposed regulatory framework for modifications to artificial intelligence/machine learning (AI/ML)-based software as a medical device (SaMD) — discussion paper and request for feedback. In: *US Food and Drug Administration*. Administration UFaD; 2019. https://www.fda.gov/files/medical%20devices/published/US-FDA-Artificial-Intelligence-and-Machine-Learning-Discussion-Paper.pdf. Accessed September 3, 2024.
14. FDA. Total product life cycle for medical devices: US food and drug Administation. 2023. https://www.fda.gov/about-fda/cdrh-transparency/total-product-life-cycle-medical-devices. Accessed September 5, 2024.
15. FDA. Good Machine learning practice for medical device development: guiding principles. US Food and Drug Administration. https://www.fda.gov/medical-devices/software-medical-device-samd/good-machine-learning-practice-medical-device-development-guiding-principles. Accessed September 3, 2024.
16. EPRS. *Artificial Intelligence Act*. European Parliament; 2024. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)698792. Accessed September 9, 2024.

17. EUMDR. Step by step guide to compliance for manufacturers: the European Union Medical Device Regulation. 2024. https://eumdr.com/manufacturers/. Accessed September 10, 2024.
18. Wolford B. What is GDPR, the EU's new data protection law?: proton Technologies AG. 2018. https://gdpr.eu/what-is-gdpr/. Accessed September 10, 2024.
19. Commission E. The European Union and the United States of America strengthen cooperation on research in Artificial Intelligence and computing for the Public Good. European Commission; 2023. https://digital-strategy.ec.europa.eu/en/news/european-union-and-united-states-america-strengthen-cooperation-research-artificial-intelligence. Accessed September 10, 2024.
20. Sheehan M. China's AI regulations and how they get made. Carnegie Endowment for International Peace; 2023. https://carnegieendowment.org/research/2023/07/chinas-ai-regulations-and-how-they-get-made?lang=en. Accessed September 15, 2024.
21. DISR. Australia's AI ethics principles: department of industry, science and resources. 2024. https://www.industry.gov.au/publications/australias-artificial-intelligence-ethics-principles/australias-ai-ethics-principles. Accessed September 15, 2024.
22. TGA. Understanding regulation of software-based medical devices: Therapeutic Goods Administration. 2024. https://www.tga.gov.au/resources/guidance/understanding-regulation-software-based-medical-devices. Accessed September 15, 2024.
23. TGA. Artificial Intelligence (AI) and medical device software: Therapeutic Goods Administration. 2024. https://www.tga.gov.au/how-we-regulate/manufacturing/manufacture-medical-device/manufacture-specific-types-medical-devices/artificial-intelligence-ai-and-medical-device-software. Accessed September 15, 2024.
24. MRCT. Impact of privacy laws on clinical research Boston, MA: the multi-regional clinical trials center of Brigham and Women's Hospital and Harvard. 2024. https://mrctcenter.org/project/impact-of-gdpr-and-privacy-laws-on-clinical-research/?utm_source=chatgpt.com. Accessed December 5, 2024.
25. Beaney A. Lack of consistency with data protection poses pain point for biotechs and sponsors. clinical Trials Arena; 2024. https://www.clinicaltrialsarena.com/features/data-protection-laws-difficult-multi-country-trials/?utm_source=chatgpt.com&cf-view. Accessed December 5, 2024.
26. Kelly CJ, Karthikesalingam A, Suleyman M, Corrado G, King D. Key challenges for delivering clinical impact with artificial intelligence. *BMC Med*. 2019;17(1):195. https://doi.org/10.1186/s12916-019-1426-2.
27. World Health Organization. *Regulatory Considerations on Artificial Intelligence for Health*. World Health Organization; 2023. https://iris.who.int/bitstream/handle/10665/373421/9789240078871-eng.pdf. Accessed August 29, 2024.
28. Zhou K, Gattinger G. The evolving regulatory paradigm of AI in MedTech: a review of perspectives and where we are today. *Ther Innov Regul Sci*. 2024;58(3):456-464. https://doi.org/10.1007/s43441-024-00628-3.
29. Wu K, Wu E, Rodolfa K, Ho DE, Zou J. Regulating AI adaptation: an analysis of AI medical device updates. *medRxiv*. 2024. 2024.06.26.24309506.
30. United Nations Educational, Scientific and Cultural Organization. How the ISO and IEC are developing international standards for the responsible adoption of AI. UNESCO; 2024. https://www.unesco.org/en/articles/how-iso-and-iec-are-developing-international-standards-responsible-adoption-ai. Accessed September 5, 2024.
31. Rish T. Ultimate list of ISO standards for medical devices: green-light guru. 2023. https://www.greenlight.guru/blog/iso-standards. Accessed September 5, 2024.
32. Ahmadzai M, Nguyen G. Federated learning with differential privacy on personal opinions: A privacy-preserving approach. *Procedia Comput Sci*. 2023;225:543-552. https://doi.org/10.1016/j.procs.2023.10.039.
33. IMDRF. Artificial intelligence/machine learning-enabled working group: international medical device regulators forum. 2024. https://www.imdrf.org/working-groups/artificial-intelligencemachine-learning-enabled. Accessed September 5, 2024.
34. Gill AS, Germann S. Conceptual and normative approaches to AI governance for a global digital ecosystem supportive of the UN Sustainable Development Goals (SDGs). *AI Ethics*. 2022;2(2):293-301. https://doi.org/10.1007/s43681-021-00058-z.
35. IBM. What is edge AI?; IBM; 2024. https://www.ibm.com/topics/edge-ai. Accessed September 5, 2024.