Mod Pathol 37 (2024) 100609

MODERN PATHOLOGY

USCAP UNITED STATES AND CANADIAN ACADEMY OF PATHOLOGY
Creating a Better Pathologist

Journal homepage: https://modernpathology.org/

Review Article

Regulatory Aspects of Artificial Intelligence and Machine Learning

Liron Pantanowitz[a,b,*], Matthew Hanna[a,b], Joshua Pantanowitz[c], Joe Lennerz[d], Walter H. Henricks[e], Peter Shen[f], Bruce Quinn[g], Shannon Bennet[h], Hooman H. Rashidi[a,b,*]

[a] *Department of Pathology, University of Pittsburgh Medical Center, Pittsburgh, Pennsylvania;* [b] *Computational Pathology and Artificial Intelligence Center of Excellence, University of Pittsburgh School of Medicine, Pittsburgh, Pennsylvania;* [c] *Medical School, University of Pittsburgh, Pittsburgh, Pennsylvania;* [d] *BostonGene, Waltham, Massachusetts;* [e] *Department of Pathology and Laboratory Medicine, Cleveland Clinic, Cleveland, Ohio;* [f] *Siemens Healthineers, San Jose, California;* [g] *Bruce Quinn Associates LLC, Los Angeles, California;* [h] *Department of Pathology, Mayo Clinic, Rochester, Minnesota*

ARTICLE INFO

Article history:
Received 11 August 2024
Accepted 1 September 2024
Available online 12 September 2024

Keywords:
artificial intelligence
Food and Drug Administration
laboratory-developed test
machine learning
medical device
regulations

ABSTRACT

In the realm of health care, numerous generative and nongenerative artificial intelligence and machine learning (AI-ML) tools have been developed and deployed. Simultaneously, manufacturers of medical devices are leveraging AI-ML. However, the adoption of AI in health care raises several concerns, including safety, security, ethical biases, accountability, trust, economic impact, and environmental effects. Effective regulation can mitigate some of these risks, promote fairness, establish standards, and advocate for more sustainable AI practices. Regulating AI tools not only ensures their safe and effective adoption but also fosters public trust. It is important that regulations remain flexible to accommodate rapid advances in this field to support innovation and also not to add additional burden to some of our preexisting and well-established frameworks. This study covers regional and global regulatory aspects of AI-ML including data privacy, software as a medical device, agency approval and clearance pathways, reimbursement, and laboratory-developed tests.

Introduction

Artificial intelligence (AI) and machine learning (ML) have emerged as transformative forces in health care,[1] with the potential to revolutionize the field of pathology and beyond. The integration of these technologies into clinical practice promises a future in which precision medicine moves from aspiration toward a tangible reality. AI-ML models have demonstrated capabilities for enhancing diagnostic accuracy, automating tasks, predicting patient outcomes, streamlining workflow efficiency, and providing personalized treatment pathways. From pattern recognition in imaging diagnostics to predictive analytics in patient prognosis and diagnostic report generation within generative AI, the range of applications with demonstrated utility is broad.

Several concerns have been raised regarding the precipitous consumption of AI such as safety and security (eg, unintended risks, cybersecurity threats, and malicious misuse), ethical considerations (eg, biases), accountability, trust, and adoption, economic disruption (eg, unfairly impacting workforce), global competitiveness, and harm to the environment.[2] Regulations can help with the following aspects: (1) mitigate many of these risks,[3] (2) ensure that AI-ML is developed and implemented in ways that are fair, transparent, and respectful of human rights, (3) promote the adoption of appropriate guidelines and standards, (4) provide

* Corresponding authors.
E-mail addresses: pantanowitzl2@upmc.edu (L. Pantanowitz), rashidihh@upmc.edu (H.H. Rashidi).

https://doi.org/10.1016/j.modpat.2024.100609

assurance that these technology tools are reliable, safe, and employed responsibly, (5) ensure that the benefits of AI are shared globally, and (6) advocate for sustainable AI practices.

There are various types of regulations including rules devised by public authorities and self-structured, self-imposed, or self-regulated rules for the private sector.[4] In general, it is recommended that AI-related regulations be formulated by public bodies, rather than profit-making private companies.[5] Clearly, regulatory frameworks are critical for the development, validation, implementation, and postdeployment monitoring of AI-based solutions in the health care setting. At the same time, regulatory oversight needs to be dynamic to keep pace with brisk technological advancements.[6,7] It is also important to acknowledge that the generative AI domain contrasts with nongenerative models in its ability to create new and/or synthetic (fake) data that are sometimes indistinguishable from real-world data. Generative AI for use in health care will thus likely need distinct regulations.[8]

This is part 5 of our 7-part AI review AI series (Fig. 1), which is meant to examine the current global state of regulatory affairs concerning AI-ML applications in health care. Current regulations and governing paradigms will be covered, nuances in legislation for generative and nongenerative models will be addressed, and pressure points will be discussed in which regulatory flexibility and adaptation are important to permit AI-ML innovation to help improve health outcomes globally.

Data Privacy and Regulatory Environment for Artificial Intelligence and Machine Learning in Health Care

In health care, extensive and tight regulatory controls and safeguards are in place with the primary goal of protecting patients. Anyone seeking to develop and/or deploy AI-ML solutions in health care environments must comply with such regulations.[9] Failure to adhere to regulatory requirements may result in substantial penalties for organizations and individuals. Regulations that are most applicable to AI-ML in health care are those enacting the following aspects: (1) safeguards to protect patient privacy such as the Health Insurance Portability and Accountability Act (HIPAA) or General Data Protection Regulation (GDPR), (2) rules regarding ethics involving human subjects such as the "Common Rule" and those proposed by recognized ethics committees such as an Institutional Review Board (IRB), and (3) federal agencies responsible for protecting the public such as the US Food and Drug Administration (FDA). HIPAA and GDPR protect individuals' personal health information (PHI). The Common Rule and IRBs protect human subjects in research and development. The FDA regulations protect public health through controls on the manufacture and marketing of medical devices.

Given the rapid advances within the field of AI, the government and other agencies constantly have to develop new regulations. For example, the Department of Health and Human Services in the United States was recently tasked, under an executive order from President Biden, to establish contemporary health care–specific AI programs and policies.[10] This executive order requires agencies to increase algorithmic transparency, include human oversight where necessary, offer long-term safety and real-world performance monitoring, and that stakeholders use technical tools such as privacy-enhancing technologies. Based on the Health Data, Technology, and Interoperability Final Rule, developers of predictive decision support interventions must provide end users with sufficient technical performance information to determine if these health information technology tools are fair, appropriate, valid, effective, and safe.[11]

Health Insurance Portability and Accountability Act

The aim of HIPAA, a US federal law since 1996, is to protect sensitive PHI from being disclosed without a patient's consent or knowledge.[12,13] The cornerstone of HIPAA is the definition of PHI as individually identifiable health information. PHI is information that identifies an individual and that relates to their physical or mental health condition, provision of health care, or payment of health care provision to an individual. HIPAA regulations contain provisions that address the allowable use, exchange, privacy, and security of PHI.

The Privacy Rule of HIPAA places limits on the allowable use and disclosure of an individual's PHI. The HIPAA Security Rule establishes standards for protection from threats to electronic PHI security, integrity, and impermissible disclosures. These rules require covered health care entities to have administrative, technical, and physical safeguards to protect PHI. Administrative safeguards include policies and procedures. Technical safeguards relate to electronic control of data access (eg, passwords). Physical safeguards include mechanisms and equipment to control access to data (eg, encrypted drives). HIPAA also includes rules that require notification following a breach of unsecured PHI, standards related to secure electronic exchange of health care data, and guidelines for investigating violations and noncompliance.

HIPAA also includes regulations that apply when a health care entity works with external parties or subcontractors that have access to its PHI. Under HIPAA, a business associate is any third party that provides the health care entity with functions or services that involve PHI. Such health care entities must have a Business Associate Agreement (BAA) in place, as applicable.[14] BAAs specify safeguards on a business associates' use and disclosure of PHI. It is a health care entity's responsibility to cure a business associate's PHI breach or violation of its BAA. Under HIPAA, business associates are subject to penalties for uses and disclosures of PHI that are not authorized by its BAA contract or required by law. A business associate is also liable for failing to

Figure 1.
Your journey through this 7-part review article series. AI, artificial intelligence; ML, machine learning.

safeguard electronic PHI in accordance with the HIPAA Security Rule.

In the United States, HIPAA applies to the use of AI in health care. Business associates dealing with AI solutions and AI systems handling PHI must comply with the same privacy and security standards as human operators. For example, if patient data are pushed to the cloud for AI algorithm analysis, this process must ensure that PHI is protected (eg, via encryption, access control, and deidentification). For AI-ML in health care, BAAs may significantly affect external AI-ML developers and health care entities that plan to work together on the development or implementation of AI-ML solutions. Health care organizations that are using and/or codeveloping AI tools must ensure that their industry partners comply with HIPAA regulations.

International Regulations

The popularity of AI technologies has raised moral, legal, and social concerns around the world. Hence, it is not surprising that many countries besides the United States have started to adopt transnational legislation to regulate the development, deployment, and use of AI in health care.[15] The Law Library of Congress in Washington, DC (2023), listed around 40 jurisdictions in the world where legislation exists that specifically refer to AI.[16] Their survey also identified several international organizations (eg, United Nations, North Atlantic Treaty Organization, and United Nations Educational, Scientific and Cultural Organization) that have strategies dealing with the adoption of AI. Some of these laws provide general frameworks (eg, ethics rights), whereas others govern specific applications of AI systems (eg, image generation).

AI-ML–based devices tend to be approved in Europe before the United States, possibly due to less rigorous evaluation of medical devices in Europe.[17] Similar to HIPAA, the European Union's (EU) GDPR is a comprehensive data privacy regulation that applies to all member states.[18] The GDPR sets out principles such as consent, purpose limitation, and transparency, and gives individuals more control over their personal data. As in the United States, organizations in the EU using AI in health care must adhere to the GDPR's core principles by ensuring that they have adequate security measures in place to protect personal data, a legal contract that proves there is a lawful basis for processing personal data, and notify authorities in the event of a breach. The GDPR also imposes restrictions on automated decision-making and, similar to many other countries, limits the international transfer of personal data. In the EU, the AI Act complements the GDPR.

China is another country that is starting to establish itself as a global leader in the field of AI. Administration in China has accordingly established various regulations that control AI growth and operations (eg, Chinese Cybersecurity Law and New Generation AI Development Plan).[19] Various bodies in China (eg, AI Strategy Advisory Committee and AI Plan Promotion Office) provide central guidance to enforce these regulations and incentivize local projects that fulfill national government policy aims (eg, subsidize technology start-ups). Countries such as Canada have also been proactive by introducing government-led programs (eg, Pan-Canadian AI Strategy, Canadian AI Ethics Council, Personal Information Protection, and Electronic Documents Act) that advocate for the responsible development and use of AI. In Australia, the ethical development and implementation of AI is centered around their National Artificial Intelligence Ethics Framework.

Various international organizations (eg, United Nations and Organization for Economic Co-operation and Development) have been working on global guidelines to aid in regulating AI. Their efforts underscore the importance of cooperation among countries, universal standardization of approaches and guidelines, and using AI to realize global benefits and sustainability, as well as collectively respond to global challenges. The International Medical Device Regulators Forum, a global network of medical device regulators, also focuses on AI in the context of medical devices.[20]

Common Rule and Institutional Review Boards

The need to respect and protect individuals who participate in research, and related development, has long been recognized. Under the Federal Policy for the Protection of Human Subjects,[21] regulations in the United States have been enacted that govern ethics and safeguards for the use of human subjects in research. These regulations are typically referred to as the "Common Rule."[22]

The Common Rule establishes requirements for IRBs as the mechanism for local oversight and control of research in organizations performing human subject research. Local IRB functions, composition, and policies must comply with the Common Rule. The purpose of an IRB committee is to protect the rights, safety, and welfare of individuals recruited for research studies. One of the responsibilities of IRBs is to assure that risks to participants are minimized, participation is voluntary, and informed consent is obtained when appropriate. Hence, IRBs play an important role in AI research in health care involving human data because they ensure ethics oversight, conduct a risk-benefit analysis, require transparency and accountability, check that research design includes measures to mitigate bias and ensure fairness, as well as measures that protect data privacy and security. They also necessitate compliance (eg, monitoring and reporting) of AI research projects.

Food and Drug Administration and Regulatory Counterparts

Manufacturers of medical devices and software in the United States must obtain clearance or approval from the US FDA.[23,24] The FDA is an agency within the US Department of Health and Human Services that has a mission to protect public health by assuring safety, effectiveness, quality, and security of products that fall under its regulatory jurisdiction.[25] The FDA favors regulating AI software based on function, rather than technical components or indicated use.[26] Software as a medical device (SaMD) is defined as software intended to be used for medical purposes (Fig. 2) that performs these purposes without being part of an actual hardware medical device (ie, the software itself is the device).[27,28] This broad definition encompasses a wide range of applications, from simple mobile applications that provide diagnostic support to complex systems leveraging AI-ML algorithms for predicting patient outcomes. Unlike embedded software or firmware, SaMD operates on general-purpose computing platforms (eg, smartphones, tablets, and personal computers) rather than being integrated into a specific hardware device. Examples of SaMD include clinical decision support tools, which assist health care professionals in making diagnoses or treatment recommendations, and imaging analysis software that helps pathologists and radiologists detect abnormalities in medical images. Clinical decision support includes computer-aided detection for the identification of an

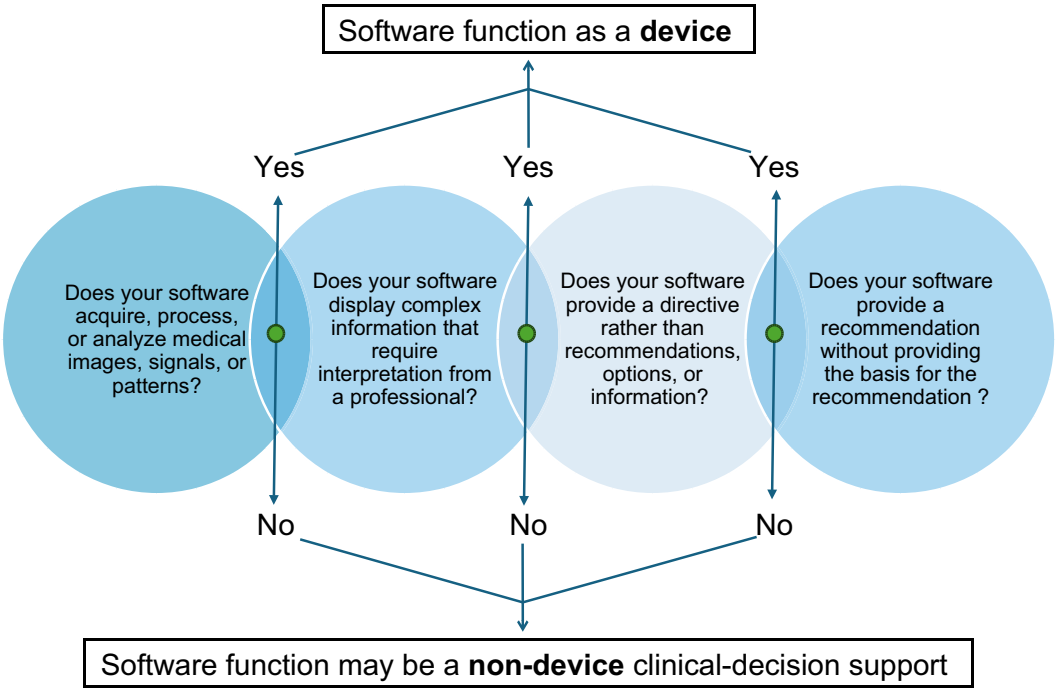

Figure 2.
A schematic distinguishing software as a medical device (eg, computer-aided diagnosis using image analysis) versus nondevice (eg, educational software). A nondevice is not subject to the stringent regulatory requirements that apply to a medical device.

abnormality, and computer-aided diagnosis for the identification and assessment of the detected abnormality.

The FDA encourages Good Machine Learning Practice to ensure that AI-ML systems are transparent, explainable, and reliable. Guiding principles include leveraging multidisciplinary expertise throughout the product life cycle, making sure that model design incorporates good software engineering, embracing good data quality and cybersecurity practices, as well as ensuring that training data sets are independent of test sets. From a regulatory perspective, the Total Product Lifecycle evaluates medical devices from premarket to postmarket. Therefore, following approval, the FDA will undertake postmarket surveillance, which requires manufacturers to report diagnostic errors and adverse events.[29]

To ensure appropriate oversight, the FDA categorizes medical devices, including SaMD, based on levels of risk to patients and regulatory controls that are needed.[30] This classification system is critical for determining the level of regulatory control necessary to assure safety and effectiveness. The FDA's risk-based framework considers factors such as the severity of the disease being diagnosed or managed, the importance of the information provided by the SaMD to clinical decision-making, and the potential risks associated with inaccurate outputs. This risk-based classification consists of the following 3 medical device categories: class I for low-risk devices, class II for moderate-risk devices, and class III for high-risk devices.[30,31] These categories accordingly require increasing levels of regulatory control and rigor of evaluations.

Not all regulations that pertain to software regulation fall cleanly into the categories of data privacy (eg, HIPAA) versus Medical Device Regulation (eg, FDA). For example, the Office of the National Coordinator of Health Innovation Technology in the United States recently released extensive new requirements for interoperability, but included in the same rulemaking a number of requirements for predictive and AI software.[32] Some experts advocate for reforming FDA regulations to keep in step with the rapid advancements in medical AI. One such paradigm is for the FDA to therefore shift from product-focused to firm-based regulation.[6] With this approach, the FDA would perform inspections and audits of an AI firm's processes, not just its product(s), to ensure production quality and safety of its AI tools.

There are several international regulatory counterparts of the FDA. They work similarly to the FDA in their respective regions to ensure the safety, efficacy, and security of medical devices, including AI software. Some of these agencies include Health Canada, Medicines and Healthcare products Regulatory Agency in the United Kingdom, Pharmaceuticals and Medical Devices Agency in Japan, National Medical Products Administration in China, Central Drugs Standard Control Organization in India, and Therapeutic Goods Administration in Australia. In the EU, manufacturers must obtain a Conformité Européenne mark (meaning conformity in French) in adherence with their Medical Device Regulation. Similar to the FDA, regulatory controls and marketing pathways in the EU are also risk based. However, it is currently easier to get a Conformité Européenne mark than FDA approval.[7] For this reason, several companies elect to first launch their product outside the United States. FDA clearance or approval is often a more lengthy and expensive process. Launching an AI-based tool for clinical use in multiple markets poses significant challenges, because separate regulatory clearance or approval may be needed in each country.

Food and Drug Administration Regulatory Programs for Applying Software as a Medical Device to Artificial Intelligence and Machine Learning

The US FDA regulatory program oversees the development and deployment of medical devices, including SaMD, that incorporate AI-ML technologies. However, the FDA's approach to SaMD

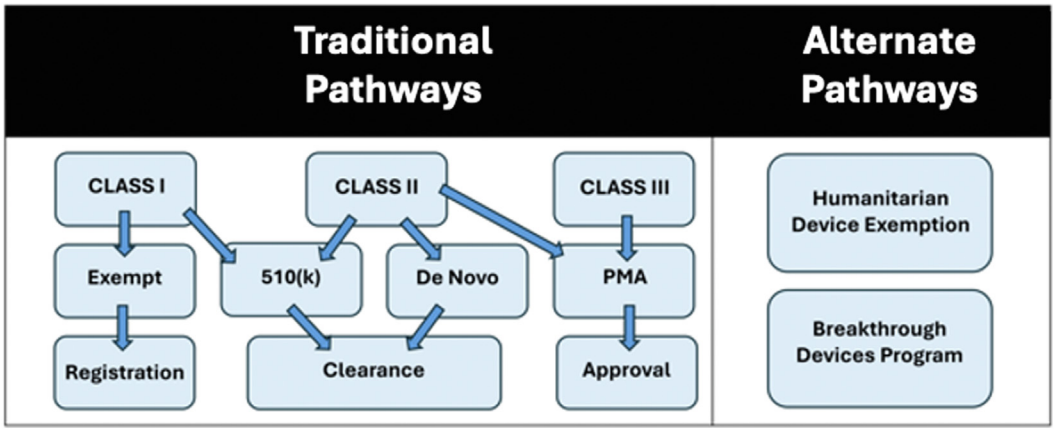

Figure 3.
A schematic overview of various pathways involved in medical device technology evaluation by the Food and Drug Administration (adapted from Liang et al[35]). Low-risk devices that are exempt do not require approval. Evolutionary devices with a moderate risk and in which predicate technology already exists require approval via the 510(k) pathway. Revolutionary devices without a predicate device can get approved by the de novo, premarket approval (PMA, most stringent), or alternate pathways.

regulation is designed to be adaptive, recognizing the iterative nature of AI-ML software development.[33,34] This allows for the continuous improvement of SaMD while maintaining the integrity of patient care. The FDA's guidelines provide a structured pathway for developers to navigate the regulatory landscape, fostering innovation while ensuring that these cutting-edge technologies meet the stringent requirements of health care regulation. As the field advances, an ongoing dialog between regulators and stakeholders will be essential to refine the framework, ensuring it remains robust yet flexible enough to accommodate the rapid pace of technological change in AI-ML applications within health care.

General pathways for medical device approval by the FDA include premarket approval (PMA), premarket notification 510(k), 510(k) exempt, de novo classification, and humanitarian device exemption (Fig. 3).[35] The 21st Century Cures Act provides guidelines about software that is exempt and hence does not require FDA approval for distribution.[7] Manufacturers may request de novo classification if their novel medical device has no legally marketed predicate device. This was the pathway followed by which the FDA permitted marketing of the Philips IntelliSite Pathology Solution for primary diagnosis using whole-slide imaging.[36] In the United States, humanitarian device exemption is employed when a medical device is used for patients with a rare condition (<8000 individuals/y). The Breakthrough Devices Program can be used to expedite FDA approval if a manufacturer's AI product warrants providing patients with timely access to their medical device. In addition, pathways specialized for software products include the FDA's pilot Precertification Program and Predetermined Change Control Plan (PCCP). These latter pathways have been designed to explore new approaches to regulatory science while both ensuring patient safety and fostering innovation in the medical software industry.

Premarket Approval

PMA is the most stringent type of device marketing application required by the FDA, typically for class III medical devices. It involves nonclinical and clinical studies, as well as comprehensive evaluation to ensure that the device is safe and effective for its intended use. An FDA "approved" device indicates that the agency has concluded that the benefits of the product outweigh the risks. For AI-ML SaMD, the PMA process requires collecting extensive clinical data, detailed algorithmic explanations, and robust validation protocols. Given the adaptive nature of AI-ML technologies, the FDA also considers the ability of these systems to learn and evolve over time. For PMA applications in the new AI-ML space, developers must provide clear documentation on how the AI-ML SaMD will maintain its performance postdeployment, including strategies for managing algorithmic changes and ensuring continued safety and effectiveness over time.

510(k) Clearance

510(k) Clearance is a premarket submission made to the FDA to demonstrate that a device, including SaMD, is at least as safe and effective as another legally marketed predicate (similar) device.[37] This process typically involves demonstrating substantial equivalence to the predicate through performance data and risk assessment. Under 510(k), the FDA recognizes the unique challenges posed by emerging technologies, such as the potential for significant changes to an algorithm over time. Developers are expected to characterize an AI-ML algorithm's performance, including its ability to adapt without compromising safety or effectiveness. They must also provide transparency about the data used for training and validation, as well as any foreseeable risks associated with AI-ML SaMDs within routine operation.

Food and Drug Administration Precertification Program

The FDA piloted a Software Precertification Program from 2017 to 2022, envisioned as an innovative approach aimed at streamlining the regulatory process for SaMD.[38] The aim was to precertify developers who demonstrated a robust culture of quality and organizational excellence, allowing for a more efficient market entry while ensuring patient safety. The Software Precertification Program emphasized the importance of real-world performance monitoring and risk management strategies that account for the iterative nature of AI-ML technologies. Similar to PMA and 501(k) expectations, the program encouraged continuous learning and improvement by developers, with a focus on transparency and the ability to quickly address potential safety issues as the software evolved. However, the FDA has noted that a

new regulatory framework would be beneficial for the AI-ML software, which would require congressional action.

Predetermined Change Control Plan

The PCCP is one of the FDA's newest processes that emphasizes a structured approach that outlines how changes to a software product, such as updates or enhancements, will be managed postmarket.[39] A PCCP is particularly critical owing to the inherent evolutionary nature of AI-ML technologies. It includes the types of changes that can be implemented without requirements for additional regulatory review, along with the processes for evaluating and documenting those changes. The plan should detail how the software's performance will be monitored and evaluated following updates or modifications. It must also specify the thresholds for when a change might necessitate a new premarket submission. The FDA encourages the use of PCCPs to ensure that AI-ML SaMD remains safe and effective throughout its lifecycle, even as it adapts and improves. This approach will likely be the basis for most AI-ML products as the community learns to best navigate its requirements and structural needs.

Reimbursement Issues for Artificial Intelligence and Machine Learning in Health Care

The reimbursement landscape for AI-ML applications in health care is complex and evolving. Outside the United States, reimbursement for AI in health care varies based on differences in health care systems, regulations, and policies. To secure reimbursement, manufacturers of AI products in all countries need to demonstrate the clinical and economic value of their technology. We focus particularly on scenarios in which regulated software devices deliver clinical analytical services to a health care practitioner. We refer to these as algorithm-based health care services (ABHSs). These contrast with unregulated or less formal uses of generative AI to answer clinical questions or with AI that streamlines operational tasks. ABHSs use AI-ML to produce clinical outputs for the diagnosis and/or treatment of a patient's condition.

In many health payment systems in the United States, the existing payment conventions are not yet well suited to accommodate the unique characteristics of ABHS technologies. Traditional fee-for-service systems may lack specific billing codes for ABHS services, so currently there are less conventional pathways available for reimbursement for such services. However, there is growing recognition of the value that ABHS tools bring to health care, such as improved diagnostic accuracy and efficiency gains. This has prompted some payers and regulatory bodies to explore new pathways for reimbursement. For the US Medicare system, the Medicare Payment Advisory Committee recently released a 30-page report on the agency's successes and challenges in AI reimbursement.[40] Many stakeholders hope to shift reimbursement toward value-based payment models (eg, extra payment for better patient outcomes), not least to incentivize the adoption of innovative technologies that demonstrate clear clinical benefits and cost-effectiveness within our ecosystem. In short, however, software reimbursement strategies remain undeveloped.

One of the primary challenges for ABHS reimbursement is the lack of standardized frameworks for evaluating the efficacy and economic impact of these technologies. The rapid pace of innovation often outstrips the ability of health care systems to assess and approve new tools for coverage. In addition, there is a need for robust evidence demonstrating improved patient outcomes, which can be difficult to generate in the nascent stages of an ABHS application's lifecycle. Another significant barrier is the uncertainty regarding liability and accountability when ABHS applications are used in clinical decision-making. These challenges necessitate a reevaluation of existing reimbursement policies to ensure they align with the innovative nature of ABHS technologies.

To address some of these challenges, potential solutions and opportunities are starting to emerge. One approach is the development of new reimbursement codes specifically for ABHS applications, which would facilitate billing and payment processes, and in the United States to formalize a Medicare payment pathway to ensure separate payment for these applications. Formalizing a Medicare payment pathway could be achieved by establishing the software as a service Add-on Policy into Medicare regulation, allowing for add-on payment opportunities for ABHS through existing reimbursement payment pathways. Collaboration among technology developers, health care providers, payers, and regulatory agencies is crucial to establish evidence-based guidelines and standards for ABHS applications.

Another approach could be to explore pilot programs that implement alternative payment models, such as episode-based or performance-linked reimbursements, that could provide valuable insights into the most effective ways to incentivize the use of ABHS in health care. Furthermore, the integration of real-world data and continuous learning systems can help in monitoring outcomes and refining ABHS tools over time, ensuring that they consistently deliver value. By embracing these solutions, stakeholders can create a more conducive environment for the adoption of ABHS technologies, ultimately leading to enhanced patient care and a more efficient health care system.

Laboratory-Developed Tests and Artificial Intelligence and Machine Learning Platforms

A laboratory-developed test (LDT) in the United States is an in vitro diagnostic device that is developed and used within a single laboratory. Hence, an AI algorithm can be considered an LDT if it is developed and used internally within a single clinical laboratory. As an LDT, such an algorithm should not be sold or distributed to other laboratories. On the other hand, commercial AI algorithms distributed to multiple laboratories are not considered LDTs. If used for clinical work, a laboratory must still validate an AI algorithm for its intended use irrespective of whether it is an LDT, LDT-like, or non-LDT tool. The advent of LDT-like AI platforms certainly introduces novel regulatory dilemmas. In the United States, the use of LDTs has historically fallen under the purview of the Clinical Laboratory Improvement Amendments program instead of the FDA, which sets forth many requirements that aim to ensure the quality of testing in laboratories performing clinical testing. However, in May 2024, the FDA published new regulations that explicitly place LDTs within the medical device regulatory framework.[41] A key question that needs to be answered is under what circumstances AI-ML software is considered an element of the LDT as a single medical device, and under what circumstances it is considered a separate and distinct SaMD.

Addressing Unique Challenges Posed by Generative Artificial Intelligence

Generative AI has emerged as a transformative technology, capable of producing novel content that ranges from images to text and code. However, this rapidly evolving field presents unique regulatory challenges that must be addressed to ensure its safe and beneficial integration into society and medicine. Currently, there are no standardized regulations that address the use of generative AI in health care.

One of the primary concerns is the issue of reproducibility. Generative AI systems often rely on continuous learning mechanisms to improve their outputs, which can lead to models that are dynamic and nondeterministic. This inherent variability poses significant challenges for current regulatory frameworks, which typically assume a level of predictability and consistency that generative AI cannot always guarantee. To mitigate these issues, proposed solutions include the development of adaptive regulatory standards that can account for the evolving nature of generative models, as well as rigorous validation protocols to ensure that the outputs remain reliable over time.

Algorithmic transparency is another critical aspect that demands attention in the context of generative AI. The complexity and often proprietary nature of deep-learning algorithms make them "black boxes," the decision-making processes of which are not easily understood by users or regulators. This lack of transparency raises serious concerns about accountability, bias mitigation, and the potential for misuse. To address these challenges, there is growing consensus on the need for potential approaches such as explainable AI frameworks that can elucidate the internal workings of generative models in an understandable manner. In addition, the implementation of standardized reporting practices could enhance transparency by providing insights into how these systems operate and make decisions.

Regulations regarding generative AI also need to take into consideration data privacy and security issues, as well as copyright infringement and intellectual property rights. Fostering a culture of openness and collaboration among developers, users, and regulators can pave the way for generative AI technologies that are both powerful and trustworthy. In addition, ensuring compliance with regulations is likewise important to ensure that generative AI technologies are developed and used responsibly.

Conclusion

Many generative and nongenerative AI tools have been developed and used for multiple applications in health care. Certain manufacturers of medical devices are also using AI-ML to innovate their products. However, concerns related to AI adoption include safety, transparency, explainability, security, data privacy, interoperability, ethical biases, accountability, trust, economic impact, and environmental effects. Regulation can mitigate many of these risks, ensure fairness, promote guidelines, and advocate for sustainable AI practices. Good governance should also observe ethical requirements, continual monitoring, and ensure compliance.[4] Regulating AI tools not only promotes safe and effective adoption of these technologies in health care but also helps foster public trust. However, developing AI legislation is challenging given the cross-jurisdictional nature of AI issues, overlap with other emerging technologies (eg, robotics and biotechnology), and the impact of AI on the copyright and intellectual property law. Regulators themselves need to understand AI as well as the challenges involved in developing, deploying, and monitoring this technology in health care.[42] In addition, funding is required to create government programs that support dissemination of best practices, standards for the use of AI, AI testing and evaluation infrastructure, a research ecosystem, grand challenges, and leverage public-private partnerships.

Currently, there is no separate regulatory review process dedicated just for AI-based tools. Nonetheless, novel pathways have been outlined specifically for SaMD. Classifying algorithms into risk tiers is certainly one approach to regulating AI tools, which is currently favored by agencies such as the FDA.[35] However, it is very cumbersome and expensive for vendors to follow this regulatory pathway for each AI algorithm they develop. Traditional legislative processes are also slow and hence likely to be outpaced by developments in AI.[43] It is thus important that regulations remain flexible to accommodate rapid advances in this field (eg, adaptive or continuous learning algorithms vs locked models, and generative chatbots that can create synthetic data) and thereby continue supporting innovation. It may be necessary to even establish legislation for training the pathology workforce to accommodate working in an AI-enabled setting. As AI transcends borders, it is imperative that emerging regulations and standards are created for global markets.

Acknowledgments

This article series is part of the educational effort of Computational Pathology and Artificial Intelligence Center of Excellence at the University of Pittsburgh.

Author Contributions

L.P., M.H., J.L., W.H.H., P.S., B.Q., S.B., and H.H.R. contributed to the manuscript text contents. All images/figures were constructed by J.P.

Data Availability

No data is associated with this review article.

Funding

The authors received no funding for this study.

Declaration of Competing Interest

L. Pantanowitz is a consultant for Hamamatsu Photonics KK, AiXMed, and NTP, serves on the advisory board for Ibex, and is a co-owner of Placenta AI and Lean AP. J. Lennerz is employed by BostonGene. P. Shen is employed by Siemens. B. Quinn is an owner of Bruce Quinn Associates. H.H. Rashidi is a cocreator of STNG, the inventor of MILO, and on the board of MILO-ML Inc. The other authors report no conflicts of interest.

Ethics Approval and Consent to Participate

No original research was conducted that warranted ethics approval or consent.

Declaration of Generative AI and AI-Assisted Technologies in the Writing Process

During the preparation of this work the authors used DALL-E via ChatGPT-4o, as well as Adobe Express Online, to generate de novo artworks for the creation of certain figures or parts of figures. Additionally, a local large language model was used to generate parts of the initial manuscript bullet outline, but the text content of this manuscript is all human generated and did not include generative AI.

References

1. Zhu S, Gilbert M, Chetty I, Siddiqui F. The 2021 landscape of FDA-approved artificial intelligence/machine learning-enabled medical devices: an analysis of the characteristics and intended use. *Int J Med Inform*. 2022;165:104828.
2. Schulz WL, Durant TJS, Krumholz HM. Validation and regulation of clinical artificial intelligence. *Clin Chem*. 2019;65(10):1336–1337.
3. Parikh RB, Obermeyer Z, Navathe AS. Regulation of predictive analytics in medicine. *Science*. 2019;363(6429):810–812.
4. Hoffmann-Riem W. Artificial intelligence as a challenge for law and regulation. In: Wischmeyer T, Rademacher T, eds. *Regulating Artificial Intelligence*. Springer; 2020:1–29.
5. Turner J. *Robot Rules: Regulating Artificial Intelligence*. Palgrave Macmillan; 2019.
6. Gottlieb S. Congress must update FDA regulations for medical AI. *JAMA Health Forum*. 2024;5(7):e242691.
7. Kohli A, Mahajan V, Seals K, Kohli A, Jha S. Concepts in U.S. Food and Drug Administration regulation of artificial intelligence for medical imaging. *AJR Am J Roentgenol*. 2019;213(4):886–888.
8. Blumenthal D, Patel B. The regulation of clinical artificial intelligence. *NEJM AI*. 2024;1(8). https://doi.org/10.1056/AIpc2400545
9. Duffourc MN, Gerke S. Health Care AI and Patient Privacy-Dinerstein v Google. *JAMA*. 2024;331(11):909–910.
10. Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. The White House. Accessed July 27, 2024. https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/
11. Health Data. Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing (HTI-1) Final Rule. ONC. Accessed July 27, 2024. https://www.healthit.gov/topic/laws-regulation-and-policy/health-data-technology-and-interoperability-certification-program
12. 42 U.S.C. § 1320d et al. Public Law 104-191. Accessed July 18, 2024. https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996
13. 45 CFR. Parts 160, 162, and 164. Accessed July 18, 2024. https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf
14. Business Associate Contracts. Accessed July 18, 2024. https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html
15. Jacob S. AI Regulations around the world: A comprehensive guide to governing Artificial Intelligence. Accessed July 27, 2024. https://www.spiceworks.com/tech/artificial-intelligence/articles/ai-regulations-around-the-world/
16. Cantekin K. *Regulation of Artificial Intelligence Around the World*. Law Library of Congress; 2023.
17. Muehlematter UJ, Daniore P, Vokinger KN. Approval of artificial intelligence and machine learning-based medical devices in the USA and Europe (2015-20): a comparative analysis. *Lancet Digit Health*. 2021;3(3):e195–e203.
18. GDPR. Regulation (EU) 2016/679. Accessed July 18, 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434
19. Roberts H, Cowls J, Morley J, Taddeo M, Wang V, Floridi L. The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation. In: Floridi L, ed. *Ethics, Governance, and Policies in Artificial Intelligence*. Springer; 2021:47–79.
20. Al-Faruque F. IMDRF publishes AI/ML guiding principles echoing US, UK, Canadian regulators. Regulatory Affairs Professionals Society, Regulatory News, July 2024. Accessed October 9, 2024. https://www.raps.org/news-and-articles/news-articles/2024/7/imdrf-publishes-ai-ml-guiding-principles-echoing-u?GA_network=x&GA_device=c&GA_campaign=18448087812&GA_adgroup=&GA_target=&GA_placement=&GA_creative=&GA_extension=&GA_keyword=&GA_loc_physical_ms=9194732&GA_landingpage=https://www.raps.org/news-and-articles/news-articles/2024/7/imdrf-publishes-ai-ml-guiding-principles-echoing-u&gad_source=1&gbraid=0AAAAAD1YgQNrTuTYmPoDyC3VRkh60Hxxb&gclid=Cj0KCQjwsJO4BhDoARIsADDv4vCfuCE00uPqyiXVfBzLnKi8DGajYIhiE6cfvqb_JLneLudHLA0nHEwaAm2ZEALw_wcB
21. Federal Policy for the Protection of Human Subjects ('Common Rule'). Accessed July 18, 2024. https://www.hhs.gov/ohrp/regulations-and-policy/regulations/common-rule/index.html
22. Common Rule. 45 CFR Part 46. Accessed July 18, 2024. https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-A/part-46
23. U.S. Food, Drug & Cosmetic Act (FD&C Act), Section 201(h).
24. 21 CFR chapter I. Accessed July 18, 2024. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-H
25. US Food & Drug Administration. What we do. Accessed July 18, 2024. https://www.fda.gov/about-fda/what-we-do#mission
26. Harvey HB, Gowda V. How the FDA regulates AI. *Acad Radiol*. 2020;27(1):58–61.
27. Software as a Medical Device (SaMD). Accessed July 18, 2024. https://www.fda.gov/medical-devices/digital-health-center-excellence/software-medical-device-samd
28. International Medical Device Regulators Forum (IMDRF). Accessed July 18, 2024. https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-131209-samd-key-definitions-140901.pdf
29. Newman-Toker DE, Sharfstein JM. The role for policy in AI-assisted medical diagnosis. *JAMA Health Forum*. 2024;5(4):e241339.
30. FDA Medical Device Classification Procedures 21 CFR Part 860. Accessed July 18, 2024. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-H/part-860
31. Harvey HB, Gowda V. Regulatory issues and challenges to artificial intelligence adoption. *Radiol Clin North Am*. 2021;59(6):1075–1083.
32. Oullette PG. HHS, ONC HTI-1 Final Rule Introduces New Transparency Requirements for Artificial Intelligence in Certified Health IT. Accessed July 18, 2024. https://www.mintz.com/insights-center/viewpoints/2146/2024-01-08-hhs-onc-hti-1-final-rule-introduces-new-transparency
33. 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. Accessed July 18, 2024. https://www.fda.gov/media/122535/download?attachment
34. FDA Artificial Intelligence and Machine Learning Software as a Medical Device Action Plan. Accessed July 18, 2024. https://www.fda.gov/media/145022/download?attachment
35. Liang NL, Chung TK, Vorp DA. The regulatory environment for artificial intelligence-enabled devices in the United States. *Semin Vasc Surg*. 2023;36(3):435–439.
36. U.S. Food & Drug Administration. IntelliSite Pathology Solution (PIPS, Philips Medical Systems). Accessed August 1, 2024. https://www.fda.gov/drugs/resources-information-approved-drugs/intellisite-pathology-solution-pips-philips-medical-systems
37. Muehlematter UJ, Bluethgen C, Vokinger KN. FDA-cleared artificial intelligence and machine learning-based medical devices and their 510(k) predicate networks. *Lancet Digit Health*. 2023;5(9):e618–e626.
38. FDA Digital Health Software Precertification (Pre-Cert) Pilot Program. Accessed July 18, 2024. https://www.fda.gov/medical-devices/digital-health-center-excellence/digital-health-software-precertification-pre-cert-pilot-program
39. FDA Draft Guidance: Marketing Submission Recommendations for a Predetermined Change Control Plan for Artificial Intelligence/Machine Learning (AI/ML)-Enabled Device Software Functions. Accessed July 18, 2024. https://www.fda.gov/media/166704/download
40. Medicare Payment Advisory Council. Paying for software technologies in Medicare. In: Chernew ME, Navathe A, Masi PB, eds. *Medicare and the Health Care Delivery System*. Washington, DC: MedPAC; 2024:137–168. Accessed July 18, 2024. https://www.medpac.gov/wp-content/uploads/2024/06/Jun24_MedPAC_Report_To_Congress_SEC.pdf
41. FDA. Laboratory Developed Tests: Small Entity Compliance Guide. Accessed July 18, 2024. https://www.fda.gov/media/179543/download
42. Ooi K. Using artificial intelligence in patient care-some considerations for doctors and medical regulators. *Asian Bioeth Rev*. 2024;16(3):483–499.
43. Cochlin FJ, Curran CD, Schmit CD. Unlocking public health data: navigating the new legal guardrails and emerging AI challenges. *J Law Med Ethics*. 2024;52(S1):70–74.