June 2, 2025

Navigating AI in Healthcare: A Complex and Evolving Legal and Regulatory Landscape

The rapid advancement of artificial intelligence (AI) is transforming healthcare and offering opportunities for increased efficiency, improved patient outcomes, and streamlined administrative processes. Hospitals, for example, utilize AI for diagnosing diseases, managing patient flows, and enhancing imaging analysis. Ambulatory surgical centers (ASCs) benefit from AI-driven scheduling optimization and surgical outcome prediction, and physician groups use AI for administrative automation and precision medicine.

While AI is exciting and offers substantial benefits, as discussed in the overview below, providers must critically assess its implementation to ensure safety, fairness, and legal compliance.

Evaluating Accuracy and Performance

AI always should complement, not replace, clinical judgment. In general, providers must implement human review of AI-generated recommendations to ensure accuracy, maintain patient safety, and manage risks overall. Even with that guardrail, the usefulness of AI depends on its accuracy and reliability. Providers must assess performance metrics such as sensitivity, specificity, and predictive value to understand how the AI system functions in real-world settings. Additionally, they should review clinical validation studies that demonstrate AI's effectiveness in comparable patient populations.

Addressing Fairness and Bias Concerns

Ensuring AI models are trained on diverse patient populations is crucial to prevent the underrepresentation of certain demographic groups. Otherwise, AI systems can inadvertently introduce bias, leading to disparities in patient outcomes. A notable example involves an AI algorithm used for clinical decision-making that demonstrated gender bias by performing less accurately for female patients due to being trained predominantly on datasets representing males. This resulted in disparities in treatment recommendations and potential risks to patient safety[1].

To assess risks, providers should require AI vendors to disclose fairness audits that evaluate potential biases in datasets and algorithms. It also is advisable to conduct "red teaming" exercises, which are intended to intentionally challenge clinical decisions leveraging diagnostic algorithms and AI-driven medical tools by presenting diverse scenarios and datasets to uncover inaccuracies, biases, or blind spots. The goal of these steps is to achieve fair, accurate, and equitable patient outcomes across diverse populations. Beyond this initial assessment, ongoing monitoring of AI-generated decisions is necessary to assess and correct any unintended disparities that may arise over time.

Regulatory and Compliance Considerations

Laws, regulations, and industry standards applicable to AI in healthcare are evolving rapidly at all levels of government. Relevant laws include existing federal and international privacy and data protection laws, such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation, and existing regulations, such as those promulgated by the Department of Health and Human Services Office of Civil Rights. In addition, the Federal Trade Commission has broad authority to protect consumer data and has taken enforcement actions [2] and issued advisory notices applicable to telehealth and healthcare apps.[3]

Given changes in the executive branch in the United States, interpretation and enforcement of federal laws may be difficult to predict. Nonetheless, some requirements set forth in federal law may be enforceable at the state level, and similar or additional requirements may be found in state privacy, data protection, and/or AI laws. [4] A few states—Washington, Connecticut, and Nevada—have passed laws or amendments to their existing privacy laws that specifically address health data. Certain state laws, specifically the California Consumer Privacy Act and the Washington My Health My Data Act, have garnered significant attention in part due to their robust potential remedies and private rights of action, which heighten the risk profile for affected companies.

These federal and state laws vary in their requirements and remedies. Many require all or some of the following: reasonable data security measures, transparency, privacy policies, opt-in or opt-out consent for collecting consumer health data, rights for individuals to access and delete their data, and restrictions or prohibitions on the unauthorized sale or use of data for purposes outside the scope of the original consent. These requirements may complicate the ability to deploy AI. For instance, if a patient has provided consent for use of PHI for delivery of or payment for healthcare, such consent does not necessarily cover secondary use for AI training or processing, or change any requirements to honor a patient's request that the entity who has collected the PHI return or delete data, which can be difficult or impossible to do if the data has been added to an AI model's training dataset.

Third-Party Risk Management

Healthcare providers using AI may construct a complex ecosystem that interconnects vendors offering pure AI functionality, existing vendors with new AI functionality built into their service offerings, and/or AI tools custom-built for each provider. In addition to AI, this ecosystem may leverage cloud providers for data storage, link to software-as-a-service tools for specific data or functionality, and leverage human resources from outsourced providers, which may be located in other countries. Such complex ecosystems always require thorough diligence to understand data flows, assess legal and compliance requirements, and reasonably manage risks—and now use of AI adds more layers of complexity, diligence, and risk management.

Conclusion

AI is a wonderful new tool that healthcare providers can deploy to bring substantial benefits to their patients and bottom lines. To do so, as described at a high level above, it is strongly recommended that providers consult with legal counsel about the specific application of laws and regulations for any contemplated use of AI in healthcare.

Day Pitney offers legal counsel on AI governance and compliance to support clients seeking to adopt AI in a responsible and ethical manner. The firm also drafts AI policies, negotiates AI clauses in vendor and customer agreements, and supports AI-related due diligence in mergers and acquisitions and other strategic transactions. These AI-specific capabilities, together with a robust Healthcare practice group, enable Day Pitney to assist healthcare providers in the full spectrum of their needs as they integrate AI into their existing healthcare services and systems. For more information, please visitDay Pitney Healthcare, Day Pitney Data Privacy, Protection & Litigation, or Day Pitney Artificial Intelligence.

---

[1] Natalia Norori, Qiyang Hu, Florence Marcelle Aellen, Francesca Dalia Faraci and Athina Tzovara, 2 Patterns (NY), no. 10, Oct. 8, 2021, available at https://pmc.ncbi.nlm.nih.gov/articles/PMC8515002/.

[2] See Fed. Trade Comm'n, FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising, Press Release (Feb. 1, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising (entering healthcare app accused of violating its representations to users regarding data sharing into a stipulated order imposing a $1.5 million fine, prohibiting the health app from engaging in deceptive practices, and permanently prohibiting use of health information for advertising purposes, among other remedies).

[3] See Fed. Trade Comm'n, Updated FTC Health Breach Notification Rule puts new provisions in place to protect users of health apps and devices, Business Blog (Apr. 26, 2024), https://www.ftc.gov/business-guidance/blog/2024/04/updated-ftc-

health-breach-notification-rule-puts-new-provisions-place-protect-users-health-apps (clarifying that the Health Breach Notification Rule applies to health apps and similar technologies).

[4] If protected health information (PHI) is processed by covered entities, such state laws may be subject to exemptions for HIPAA.

Authors



Magda C. Rodriguez

Partner

Miami, FL | (305) 373-4010

mrodriguez@daypitney.com