EMBRACE THE CHAOS
AI REGULATION IN THE U.S. REMAINS IN FLUX

BY ALAAP SHAH

Alaap Shah is a Member of Epstein Becker & Green PC. Alaap co-chairs the AI practice group and the privacy, cybersecurity, and data asset management practice group. Mr. Shah's practice focuses on proactive and reactive counseling and defense of health care, life sciences, and technology companies on a variety of legal and regulatory compliance issues. The breadth of Mr. Shah's practice includes supporting clients related to health information technology, artificial intelligence, interoperability, data commercialization, digital health, privacy, cybersecurity, and building trust networks through contracting, compliant technology architecture, and risk allocations strategies.

TechREG CHRONICLE
FEBRUARY 2025

EMBRACE THE CHAOS: AI REGULATION IN THE US REMAINS IN FLUX

By Alaap Shah

The regulation of artificial intelligence ("AI") in health care is, and will likely continue to be, in flux for the foreseeable future. A review of the U.S. regulatory landscape impacting AI reveals a patchwork of existing and emerging rules at both the state and Federal levels, variable definitions of AI, differing approaches with respect to regulation of AI development versus deployment, and a range of risks sought to be addressed. In addition, recent efforts by the Biden administration through Executive Order 14110 to promote safe, secure and trustworthy development and use of AI were recently revoked by the Trump administration. Yet, the Trump administration did not revoke a related Biden administration Executive Order 14141 focused on advancing U.S. leadership in AI Infrastructure. This suggests that the Trump administration seeks to deregulate certain areas of AI innovation and adoption, but perhaps seeks to regulate in other areas that may boost the U.S. competitive position in the AI global economy.

The regulation of artificial intelligence ("AI") in health care is, and will likely continue to be, in flux for the foreseeable future.

A review of the U.S. regulatory landscape impacting AI reveals a patchwork of existing and emerging rules at both the state and Federal levels, variable definitions of AI, differing approaches with respect to regulation of AI development versus deployment, and a range of risks sought to be addressed. In addition, recent efforts by the Biden administration through Executive Order 14110 to promote safe, secure and trustworthy development and use of AI were recently revoked by the Trump administration. Yet, the Trump administration did not revoke a related Biden administration Executive Order 14141 focused on advancing U.S. leadership in AI Infrastructure. This suggests that the Trump administration seeks to deregulate certain areas of AI innovation and adoption, but perhaps seeks to regulate in other areas that may boost the U.S. competitive position in the AI global economy.

01 AI INNOVATION TRENDS

The development and deployment of AI solutions throughout the health care and life sciences ecosystem and across clinical and non-clinical domains continues to increase at a rapid pace. Non-clinical applications of AI aim to streamline administrative tasks like customer engagement, scheduling, billing, supply chain optimization as well as to reduce costs and boost innovation and operations efficiencies with respect to drug discovery, manufacturing and supply chain optimization, pharmacovigilance, and clinical trial recruitment processes. In clinical applications, AI solutions aim to increase access, reduce costs, increase efficiencies and quality of care. A few key examples of clinical AI include supporting diagnostics (e.g., radiology and pathology imaging), patient triage and communication, telemedicine, clinical documentation to reduce clinician burden, patient safety and monitoring, clinical decision support, personalized medicine, and prior authorization and utilization management. Natural Language Processing ("NLP") also continues to transform patient record management, clinical trial recruitment, and population health analytics by extracting actionable insights from unstructured digital data.

While opportunities in the AI space are increasingly available, the space is also very noisy with many companies emerging and led by entrepreneurs with little to no prior track record. This frenzy of development has been spurred in part by the fact that AI innovation continues to outpace comprehensive regulation of the development and use of AI.

02 AI REGULATORY TRENDS IN THE UNITED STATES

When reviewing the regulatory landscape in the U.S., both long-standing and emerging regulatory standards exist at the Federal and State levels. This patchwork of regulations shaping AI governance efforts through application of consumer protection laws, medical device regulations, privacy rules, transparency requirements and non-discrimination standards. First, regulations often aim to promote development and use of safe and effective AI. Second, the success of AI continues to hinge on availability of, and rights in, data of sufficient volume, variety and veracity to train and use AI solutions. Accordingly, regulations related to data privacy have increasingly sought to promote responsible collection, use and disclosure of personal data to support AI innovation. Third, regulators have also recognized AI presents risks related to fairness, bias and discrimination. As such, certain regulatory efforts have focused on ensuring adequate risk management and AI governance requirements are placed on developers and deployers to prevent bias and discriminatory impacts of AI. Finally, regulators have also sought to ensure adequate transparency exists to ensure end users of AI and those impacted by AI outputs are provided sufficient notice to be empowered to make reasonable decisions in the context of such AI.

Yet, regulatory gaps remain as comprehensive AI regulation has not yet been successful. In this climate ethical considerations play a critical role in responsible AI development, deployment and use. Looking ahead, federal deregulation may spur innovation, but state-level initiatives could introduce new compliance requirements, making AI governance a complex and evolving landscape.

03 FEDERAL REGULATION

A variety of Federal agencies have authorities under existing regulatory schemes applicable to AI. Key regulatory bodies include the Assistant Secretary for Technology Policy/Office of the National Coordinator for Health Information Technology ("ONC"), the Food and Drug Administration ("FDA"), the Department of Health and Human Services ("HHS"), HHS's Office for Civil Rights ("OCR"), and the Federal Trade Commission ("FTC"), among others. Salient aspects of these existing Federal regulatory authorities in more detail below.

A. Assistant Secretary for Technology Policy/Office of the National Coordinator for Health Information Technology ("ONC")

The ONC leads efforts to improve health care through technology, in part, by establishing certification standards for electronic health records ("EHRs"), promotes interoperability, enhancing data privacy, and supports nationwide health IT adoption to improve patient care, efficiency, and population health. Recently ONC was rebranded to also include the Assistant Secretary for Technology Policy ("ASTP") which is tasked with overseeing national strategies related to technological innovation, digital infrastructure, and emerging tech policies. This role focuses on fostering innovation while ensuring ethical, secure, and equitable technology adoption across sectors. The combined efforts of ONC and ASTP lend themselves to an increasing role in AI policy development and potential regulation under HHS authorities.

On March 11, 2024, ONC's Health Data, Technology, and Interoperability ("HTI-1") Final Rule went into effect, introducing new certification standards for EHR technology, including Predictive Decision Support Interventions ("DSIs"). Predictive DSI is defined as "technology that supports decision-making based on algorithms or models that derive relationships from training data and then produce an output that results in prediction, classification, recommendation, evaluation, or analysis." The rule mandates that EHR developers implement Intervention Risk Management ("IRM") to assess and mitigate risks and adverse impacts related to Predictive DSIs. Developers must also publicly disclose summary information on their IRM practices. Additionally, EHR developers are required to publish 31 source attributes relevant to Predictive DSIs, enabling end users of such Predictive DSIs to evaluate their fairness, appropriateness, validity, effectiveness, and safety ("FAVES").

B. Food and Drug Administration ("FDA")

The FDA has broad regulatory authority to regulate the safety and efficacy of medical devices under the Federal Food, Drug, and Cosmetic Act ("FDC Act"). This oversight mandate includes review of the development, approval, and post-market monitoring of medical devices to ensure compliance with safety and effectiveness standards. Applying a risk-based classification system for medical devices, the FDA imposes more rigorous premarket review requirements on higher-risk medical devices.

The FDA also plays a key role in regulating Software as a Medical Device ("SaMD"), particularly AI-driven health technologies. Over the past decade, AI SaMD applications have surged tenfold, prompting the FDA to issue guidance on development, approval, and governance to maintain safety and effectiveness.

On January 7, 2025, the FDA released AI-specific guidance titled *Artificial Intelligence-Enabled Device Software Functions: Lifecycle Management and Marketing Submission Recommendations*. This document offers manufacturers comprehensive, yet voluntary recommendations for preparing FDA submissions materials in support of AI-enabled medical devices. This guidance emphasizes taking a Total Product Life Cycle ("TPLC") approach to evaluating AI risks and developing documentation. It addresses design considerations, risk management, performance monitoring, and strategies to enhance transparency and mitigate bias throughout a device's lifecycle.[2]

C. HHS, Office for Civil Rights ("OCR")

At the Federal level, OCR remains the predominant regulator of privacy and security in health care pursuant to its authority under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). HIPAA governs use, disclosure and protection of protected health information ("PHI").[3] The jurisdictional reach of HIPAA is limited to "covered entities" and their "business associates." Chiefly, the HIPAA Privacy Rule establishes permissible and impermissible uses and disclosures of PHI and generally requires an individual's authorization before use or disclosure of such individual's PHI unless an exception applies. In the context of AI development where large quantities of data is required for training, HIPAA may create certain hurdles to use of PHI. However, certain uses and disclosures of PHI to develop or use AI may be permissible to the extent such activities relate to a covered entity's treatment, payment or health care operations. It should also be noted that certain efforts to develop AI or use AI to contribute to generalizable knowledge may be considered the conduct of research which may require

[2] See "Artificial Intelligence – Enabled Device Software Functions: Lifecycle Management and Marketing Submission Recommendations" available at https://www.govinfo.gov/content/pkg/FR-2025-01-06/pdf/2024-30983.pdf.

[3] See 45 C.F.R. § 160.103 for the definition of protected health information.

patient authorization and informed consent. To complicate matters further, while HIPAA continues to regulate many traditional health care entities, recent trends suggest that an increasing number of technology companies are entering the health care ecosystem in ways that would not subject them to HIPAA compliance obligations.

OCR also enforces civil rights protections in health care. On April 26, 2024, OCR finalized a rule pursuant to its authority under Section 1557 of the Affordable Care Act, strengthening protections against discrimination in health care.[4] A key provision addresses nondiscrimination by covered entities when utilizing "patient care decision support tools," which are defined as "any automated or non-automated tool, mechanism, method, technology, or combination thereof used by a covered entity to support clinical decision-making in its health programs or activities."[5] The rule generally prohibits covered entities from using such tools in ways that discriminate based on race, color, national origin, sex, age, or disability through the use of patient care decision support tools. The rules also require covered entities to identify and mitigate associated risks.

Additionally, HIPAA has faced criticism for being outdated in today's technologically advanced landscape and for lacking clear, prescriptive security compliance requirements. Originally designed as a flexible framework, HIPAA's security standards were meant to evolve over time. However, due to growing concerns over its limitations, on December 27, 2024, OCR announced a Notice of Proposed Rulemaking to strengthen the HIPAA Security Rule. The proposed changes aim to enhance cybersecurity by modernizing security standards to better address the increasing threats to the health care sector and to account for significant technological advancements.

D. Federal Trade Commission ("FTC")

The FTC enforces consumer protection laws under Section 5(a) of the Federal Trade Commission Act ("FTC Act"), which prohibits unfair and deceptive trade practices. Notably, the FTC has effectively extended HIPAA standards by leveraging its broad authority to take action against companies engaging in deceptive or unfair practices that violate HIPAA or industry best practices. The FTC has investigated and pursued cases against companies for: (1) sufficiently notify consumers about privacy practices; (2) adhere to representations made in privacy policies; and (3) implement reasonable security safeguards to protect PII.[6]

In recent FTC cases involving the improper collection and use of personal data to train AI models, the FTC has taken an aggressive stance, seeking disgorgement of personal data from offending AI systems — at times even demanding the destruction of the AI algorithms themselves. One of the earliest enforcement actions of this kind occurred in 2019, when the FTC ordered Cambridge Analytica to destroy AI models derived from PII collected through allegedly deceptive means. In 2021, the FTC imposed a similar requirement on a photo app developer, forcing it to delete its facial recognition AI. Additionally, the FTC has pursued "algorithmic disgorgement" against a company that allegedly obtained and used children's personal information for AI development in violation of the Children's Online Privacy Protection Act ("COPPA").

04
U.S. STATE REGULATION

Beyond federal regulatory frameworks, U.S. states are increasingly shaping AI regulation, adopting a wide range of approaches that vary in scope, definitions, and focus on AI development versus deployment. Many states, led by California, have integrated AI-related protections into comprehensive consumer privacy laws, granting individuals opt-out rights from "profiling" in automated decision-making processes that carry legal or significant personal consequences.

Expanding on these privacy protections, some states are taking a more comprehensive approach to AI regulation. Colorado has enacted the first-of-its-kind AI consumer protection law, set to take effect in 2026. This law adopts a risk-based framework, requiring developers and deployers of high-risk AI systems to establish AI governance programs that include transparency measures, risk assessments, and risk management strategies. Colorado's approach is paving the way for similar legislation in other states, such as California's AB 2013 and Utah's AI Policy Act.

While the federal government's regulatory direction remains uncertain, states are expected to continue advancing AI oversight through diverse legislative and regulatory measures aimed at safeguarding consumers and addressing emerging risks.

[4] See 45 C.F.R. § 92.210.

[5] See *Id.* at § 92.4.

[6] It is important to note that recent State AG actions in Texas mirror the FTC's enforcement posture related to unfair and deceptive claims about AI efficacy. See August 21, 2024, settlement in the case *In the Matter of State of Texas and Pieces Technologies, Inc.* available at https://texasattorneygeneral.gov/sites/default/files/images/press/Petition%20for%20Approval%20of%20AVC%20Pieces%20File%20Stamped.pdf.

05 AI LITIGATION LANDSCAPE

The landscape of AI regulation is further complicated by an increasing volume of litigation targeting AI developers and deployers based on common law principles. Common claims in these lawsuits include, but are not limited to: negligence, invasion of privacy, breach of contract, unfair and deceptive trade practices, breach of the implied covenant of good faith and fair dealing, unfair claims settlement practices, insurance bad faith, libel/defamation, theft and misappropriation, biometric information privacy violations, violations of the Computer Fraud and Abuse Act, and intellectual property infringement, among others. Plaintiff's attorneys are testing numerous existing and novel theories when filing complaints and this trend is likely to continue in the absence of comprehensive AI regulation.

Many of these lawsuits are recent and still ongoing, making it challenging to identify consistent trends or predict how courts will rule. As case law develops, it is likely to inform risk management practices of AI developers and deployers as well as State and Federal legislatures and regulators with respect to AI regulation moving forward.

06 AI ETHICS AS A KEY TOUCHSTONE

Despite the lag of comprehensive AI regulations, ethical considerations continue to be germane to assessing and managing AI risks. Even where the law falls short in providing guardrails, ethical dimensions are important touchstones for AI governance including, but not limited to, transparency, fairness, safety, accountability, autonomy, privacy, security, and sustainability. Applying the ethics lens is imperative to evaluate the impacts of AI on patients and their families, clinicians and other workforce members, and the reputation and brand of organizations developing or deploying AI. Several consensus-based industry standards and guidance documents, such as the NIST AI Risk Management Framework,[7] have emerged and continue to be developed to assist organizations navigate the risks AI pose by developing reasonable and appropriate AI governance programs rooted in key ethical considerations.

07 CONCLUSION

Innovation in the health care AI space continues to outpace regulation at the Federal and State levels in the U.S. Yet, a cornucopia of Federal and State regulations impacting AI exist, which create a patchwork of compliance obligations. Further, many legislatures and regulators continue to push forward additional AI regulatory schemes. Moving into 2025, the impact of the change of the White House Administration has already signaled significant shifts on AI regulation at the Federal level. Yet, various U.S. States (with Colorado leading the way) continue to make progress on regulating AI in the absence of a comprehensive Federal AI law. Amidst this regulatory flux, and until more a comprehensive regulatory approach to AI emerges in the U.S., the private sector will likely need to continue relying on voluntary, consensus-based standards and industry best practices rooted in ethical principles of responsible development and deployment of trustworthy AI. ■

> *Many of these lawsuits are recent and still ongoing, making it challenging to identify consistent trends or predict how courts will rule*

[7] National Institutes of Standards and Technology, Artificial Intelligence Risk Management Framework version 1.0, available at https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

CPI COMPETITION POLICY® INTERNATIONAL