



U.S. Based Artificial Intelligence Regulations: Federal Guidance & State Laws

As of April 21, 2025

Whitepaper

Presented by:

Jim Rough

President

SunHawk Consulting, LLC

Jim@SunHawkConsulting.com

602-334-5522

Sam Cunningham, RHIA, CCS

Director

SunHawk Consulting, LLC

sam.cunningham@SunHawkConsulting.com

215-510-7209

Table of Contents

<i>Executive Summary.....</i>	<i>3</i>
<i>Introduction</i>	<i>3</i>
<i>Current Landscape of AI Regulations.....</i>	<i>4</i>
<i>State Laws</i>	<i>6</i>
<i>Conclusion.....</i>	<i>8</i>
<i>References.....</i>	<i>9</i>

Executive Summary

This whitepaper provides practical guidance for healthcare compliance organizations, particularly in smaller multi-system hospital settings with limited IT resources, to navigate the evolving landscape of Artificial Intelligence (AI) U.S. based regulations at the federal and state levels, with a particular focus on the healthcare industry. As AI continues to transform healthcare operations, compliance programs, and internal audit groups, understanding the legal framework surrounding its use is critical.

Currently, there are no overarching federal laws specifically governing AI in healthcare. However, multiple existing regulations, such as HIPAA, the 21st Century Cures Act, and the Affordable Care Act (ACA) address AI applications in different capacities. Regulatory bodies, including the Food and Drug Administration (FDA), the Department of Justice (DOJ), the Centers for Medicare and Medicaid Services (CMS), the Federal Trade Commission (FTC), and the Equal Employment Opportunity Commission (EEOC), have issued guidelines affecting AI use in areas like data privacy, patient care, compliance, and employment practices.

In addition to federal oversight, individual states have enacted their AI-related regulations, which vary widely in scope and application. A number of States have implemented specific laws addressing AI in employment, consumer protection, facial recognition, and healthcare applications. This fragmented regulatory environment underscores the importance of staying informed about both federal and state-level requirements.

As AI regulations rapidly evolve, healthcare organizations must proactively develop compliance strategies that align with emerging legal and ethical considerations. This includes implementing robust data governance policies, ensuring transparency in AI-driven decision-making, and mitigating risks related to both perceived and actual bias and discrimination. Organizations should also monitor ongoing regulatory updates to adapt to new requirements effectively.

This whitepaper serves as a first step guide for healthcare professionals, compliance officers, and policymakers to help locate US based AI regulations and guidance.

Introduction

AI refers to the simulation of human intelligence in machines, enabling them to perform tasks that typically require human cognition. These tasks include learning, reasoning, problem-solving, perception, language understanding, and decision-making. AI technologies encompass machine learning, deep learning, natural language processing, computer vision, and robotics.

The integration of AI into the healthcare industry has led to significant advancements in diagnostics, treatment planning, and medical research. AI enhances operational efficiency by automating administrative tasks, optimizing resource allocation, and improving patient outcomes through data-

driven insights. As AI applications continue to evolve, they bring both opportunities and challenges, particularly in areas such as compliance, ethical considerations, and regulatory oversight.

Given AI's growing role in healthcare, organizations must stay informed about emerging laws and best practices. This paper explores the current regulatory landscape governing AI, examines key federal and state-level regulations, and provides high-level insights for compliance and risk mitigation.

Current Landscape of AI Regulations

The regulatory landscape for AI in healthcare is rapidly evolving, with various federal and state laws addressing different aspects of AI deployment, compliance, and oversight. While there is no single federal law governing AI in healthcare, several existing regulations and regulatory bodies provide guidance on specific AI applications.

At the federal level, multiple agencies have established guidelines and enforcement mechanisms:

- **The Department of Justice (DOJ)**ⁱ issued the *Evaluation of Corporate Compliance* (updated September 2024), which emphasizes the role of AI in compliance monitoring and the need for organizations to integrate data analytics and AI-driven risk assessment tools. Part of the use of these tools is to answer the following three questions:
 1. Is the corporation's compliance program well designed?
 2. Is the program being applied earnestly and in good faith?
 3. Does the corporation's compliance program work in practice?

One of the key elements addressed in this document is the use of data analytics tools and models and if compliance personnel have sufficient and direct access to these tools and data for timely and effective monitoring and/or testing of policies, controls, and transactions. Conversely, the document also specifies management of emerging risk to ensure compliance with applicable laws. As AI laws and regulations are actively changing, organizations also need to mitigate risk associated with the use of new AI technology.

As part of a recent [SunHawk Consulting](#) survey of healthcare compliance professionals regarding the use of AI within healthcare organizations, over 80% of respondents did not have a program in place to track internal use of AI by employees.

- **HIPAA** does not deviate from the already established Privacy Rule, Security Rule, Business Associate Agreements (BAAs), and Breach Notification Rule. The same applications of HIPAA would apply to any software used for the safeguard of patient information.
- **21st Century Cures Act** provides guidelines for the access to electronic health information (EHI) and interoperability requirements (e.g., HL7 and FHIR standards). However, like HIPAA,

the rules and guidance are similar to the use of other software applications in the healthcare space.

- **The Centers for Medicare and Medicaid Services (CMS)**ⁱⁱ provides guidance on using algorithms or AI to make coverage determination decisions. AI alone cannot be used as the basis to deny admission or downgrade to an observation stay (§422.101(c)), and predictive algorithms or software tools cannot apply other internal coverage criteria that have not been explicitly made public and adopted in compliance with the evidentiary standard in (§ 422.101(b)(6)).
- **The Office for Civil Rights Office of the Secretary, Department of Health and Human Services (HHS)**ⁱⁱⁱ issued a Final Rule on May 6, 2024, within Section 1557 of the Affordable Care Act (ACA) prohibiting the use of AI from discrimination and bias and authorizes the Secretary of the Department of HHS to promulgate regulations to implement the nondiscrimination requirements.
- **Food and Drug Administration (FDA)**^{iv} published draft guidance proposes both lifecycle considerations and specific recommendations to support marketing submissions for AI-enabled medical devices. Notably, this draft guidance is specific to AI-enabled medical devices. Additionally, the FDA makes recommendations with regards to the use of AI in supporting the development of drug and biological products.
- **The Equal Employment Opportunity Commission (EEOC)** enforces federal laws that make it illegal for an employer, union, or employment agency to discriminate against an applicant or employee. In addition to the EEOC's enforcement activities on discrimination related to AI and automated systems, the EEOC issued a technical assistance document explaining how the Americans with Disabilities Act applies to software, algorithms, and AI in making employment-related decisions about job applicants and employees.
- **Federal Trade Commission (FTC) Act**^v has made statements regarding AI and unfair or deceptive changes in terms and conditions. It may be unfair or deceptive for a company to adopt more permissive data practices. For example, to start sharing consumers' data with third parties or using that data for AI training, and to only inform consumers of this change through a surreptitious, retroactive amendment to its terms of service or privacy policy. The FTC Act prohibits companies from unilaterally applying material privacy policy changes to previously collected data.
- **The Consumer Financial Protection Bureau (CFPB)**^{vi} published a circular confirming that federal consumer financial laws and adverse action requirements apply, regardless of the technology used (*e.g.*, machine learning and AI). The circular also made clear that the fact that the technology used to make a credit decision is too complex, opaque, or new is not a defense for violating these laws.

- **Federal Communication Commission (FCC)**^{vii} has made AI-generated voices in robocalls illegal as of February 8, 2024, as part of the Telephone Consumer Protection Act (TCPA).
- **President Trump's AI Executive Order**^{viii} *Removing Barriers to American Leadership in Artificial Intelligence* (dated January 23, 2025) revoked the October 30, 2023 Biden Executive Order which discussed eight principles and priorities governing AI. President Trump's AI Executive Order states the administration aims to "develop AI systems that are free from ideological bias or engineered social agendas" and to solidify the United States' position as the global leader in AI.
- **Federal Agencies**^{ix} *Joint Statement on Enforcement of Civil Rights, Fair Competition, Consumer Protection, and Equal Opportunity Laws in Automated Systems* was published April 4, 2024, which includes guidance and links to specific agencies' statements, and commitments to enforcements to protect civil rights, fair competition, consumers and equal opportunity from unlawful bias and discrimination.
- **HHS Secretary Advisory Committee of Human Research Protection**^x *Institutional Review Board (IRB) Considerations on the use of Artificial Intelligence in Human Subjects Research*, dated October 19, 2022, addresses the concern for AI or AI validation activities as they might meet the Common Rule definition of research that is "designed to develop or contribute to generalizable knowledge" and Common rule exemptions found in 45 CFR 46.104 (d)(4). "Similarly, information gleaned from "de-identified" medical records was collected during the course of medical care, and such collection is a condition of receiving care, depriving individuals of the ability to choose whether or not to participate in research. Further, the value of de-identification is questionable, given advancing technology and the ability to combine disparate sources of data, leaving subjects vulnerable to harms consequent on exposure of sensitive and identifiable personal data."

State Laws

State laws governing AI in the U.S. vary widely, as different states have approached AI regulation with distinct priorities. Here are some key areas where state laws address AI:

AI in Healthcare and Autonomous Systems

- **California AB-303**:^{xi} *Health Care Services: Artificial Intelligence*, effective January 1, 2025, requires disclosures to the patient when GenAI is used.
- **Nevada SB186**:^{xii} introduced February 3, 2025, imposes requirements concerning the use of artificial intelligence and healthcare (i.e., disclosures of the use of GenAI).

AI in Hiring and Employment:

- **Illinois (AI Video Interview Act, 2020):** Regulates the use of AI in analyzing job interview videos, requiring disclosure, consent, and the option for candidates to delete recordings.
- **New York City (Local Law 144, 2023):** Mandates bias audits for automated employment decision tools to prevent discrimination.

AI in Consumer Protection and Privacy:

- **California (California Privacy Rights Act (CPRA), January 1, 2023 & Amendment to California Consumer Privacy Act (CCPA)) AB 2013:^{xiii}** Includes provisions on automated decision-making and requires businesses to provide transparency and opt-out rights for AI-driven profiling.
- **California AI Transparency Act., September 19, 2024, SB-942:^{xiv}** Requires a Covered Provider, a person that creates, codes, or otherwise produces a generative AI system that has over 1M monthly visitors or users and is publicly accessible within the geographic boundaries of the state, to make available an AI detection tool at no cost to the user and to identifies content as AI-generated.
- **Colorado Privacy Act SB 24-205:^{xv}** *Concerning Consumer Protections in Interactions with Artificial Intelligence Systems*, May 17, 2024. Under the law, both developers and deployers must exercise “reasonable care to protect consumers from any known or reasonably foreseeable risks of algorithmic discrimination” in their high-risk AI systems. In addition, the law provides for a rebuttable presumption that the developer or deployer used reasonable care if they comply with the bill’s requirements.
- **Utah, Artificial Intelligence Consumer Protection Amendments, SB-226 and Artificial Intelligence Policy Act., SB-149:^{xvi}** Effective May 7, 2025, requires that a supplier that uses generative AI to interact with an individual in connection with a consumer transaction shall disclose to the individual the use of AI.
- **Virginia Consumer Data Protection Act (VCDPA) HB2250:^{xvii}** Effective July 1, 2026, the act requires a developer of a generative artificial intelligence system or service, defined in the bill, to disclose on the developer's website information about the generative artificial intelligence data set used to train such system or service. It also provides regulations on AI-based opt out of the processing of the consumer’s personal data, profiling and consumer rights regarding automated decisions.

AI in Law Enforcement and Facial Recognition:

- **Massachusetts, General Law – Part 1, Title II, Chapter 6, Section 220:^{xviii}** *The Massachusetts Police Reform Law*, December, 31, 2020, restricts the use of facial recognition by law enforcement without a court order.
- **Washington RCW, Title 43, Chapter 43.386.010 (Facial Recognition Law, effective date July 1, 2021):^{xix}** Among other things, the law requires government agencies to conduct AI accountability reports and obtain warrants before using AI-powered facial recognition.

Deepfake and Synthetic Media Laws

- **California (SB 926 & 981 effective September 19, 2024):^{xx}** Criminalizes malicious deepfake videos used to manipulate elections or distribute fake pornography.
- **Texas Tx. Pen. Code § 21.165, effective November 21, 2023 & introduced SB 1108, February 5, 2025:^{xxi}** Relating to the ban of deepfake videos (i.e., pornography).

Conclusion

AI continues to reshape the healthcare industry, providing innovative solutions to improve patient care, operational efficiencies, and compliance monitoring. However, these advancements also introduce significant challenges, particularly in navigating the complex and evolving regulatory landscape. As AI technologies progress, healthcare organizations must adopt a proactive approach to compliance by integrating ethical AI governance, transparent decision-making processes, and ongoing legal assessments.

Both federal and state governments are taking active steps to establish guidelines that address privacy, bias, and ethical concerns in AI applications. While regulations continue to evolve, it is crucial for healthcare professionals and compliance officers to stay informed about new laws and best practices. Organizations should develop internal policies that align with regulatory expectations, ensuring that AI is deployed responsibly and in a manner that upholds patient safety and data integrity.

Looking ahead, collaboration between regulatory bodies, healthcare providers, and technology developers will be essential in shaping AI policies that balance innovation with ethical responsibility. By embracing a forward-thinking regulatory approach and fostering industry-wide cooperation, healthcare stakeholders can harness the full potential of AI while mitigating risks associated with its use.

References

All reference websites were accessed as of February 13, 2025.

-
- ⁱ The *Evaluation of an Effective Compliance Program* (dated September 2024), <https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl?inline=>
- ⁱⁱ *CMS Frequently Asked Questions Related to Coverage Criteria and Utilization Management Requirements in CMS Final Rule (CMS-4201-F)* (dated February 6, 2024) <https://www.aha.org/system/files/media/file/2024/02/faqs-related-to-coverage-criteria-and-utilization-management-requirements-in-cms-final-rule-cms-4201-f.pdf>
- ⁱⁱⁱ *Nondiscrimination in Health Programs and Activities*, CFR 42, CFR 45, and section 1557 of the Affordable Care Act, (dated May 6, 2024) <https://www.federalregister.gov/documents/2024/05/06/2024-08711/nondiscrimination-in-health-programs-and-activities>
- ^{iv} FDA, *Draft Guidance: Artificial Intelligence-Enabled Device Software Functions: Lifecycle Management and Marketing Submission Recommendations* (dated January 7, 2025) <https://www.fda.gov/media/184856/download>
- ^v FTC, *AI (and other) Companies: Quietly Changing Your Terms of Service Could Be Unfair or Deceptive*, (dated, February 13, 2024) <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/02/ai-other-companies-quietly-changing-your-terms-service-could-be-unfair-or-deceptive>
- ^{vi} CFPB, *Consumer Financial Protection Circular 2022-03, Adverse action notification requirements in connection with credit decisions based on complex algorithms*, (dated May 26, 2022) <https://www.consumerfinance.gov/compliance/circulars/circular-2022-03-adverse-action-notification-requirements-in-connection-with-credit-decisions-based-on-complex-algorithms/>
- ^{vii} FCC, *FCC Confirms that TCPA Applies to AI Technologies that Generate Human Voices*, (dated February 8, 2024) <https://www.fcc.gov/document/fcc-confirms-tcpa-applies-ai-technologies-generate-human-voices>
- ^{viii} AI Executive Order, *Removing Barriers to American Leadership in Artificial Intelligence*, (dated January 23, 2025) <https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/>
- ^{ix} *Joint Statement on Enforcement of Civil Rights, Fair Competition, Consumer Protection, and Equal Opportunity Laws in Automated Systems*, (dated April 4, 2024) <https://www.justice.gov/crt/media/1346821/dl?inline>

^x U.S. Department of Health and Human Services, *IRB Considerations on the Use of Artificial Intelligence in Human Subjects Research*, (dated October 1, 2022)

<https://www.hhs.gov/ohrp/sachrp-committee/recommendations/irb-considerations-use-artificial-intelligence-human-subjects-research/index.html>

^{xi} Medical Board of California, *Generative Artificial Intelligence Notification Requirements*, AB 3030, effective date January 1, 2025

<https://www.mbc.ca.gov/Resources/Medical-Resources/GenAI-Notification.aspx>

^{xii} Nevada SB 186, Imposes requirements concerning the use of artificial intelligence in healthcare. Introduced February 3, 2025.

<https://www.leg.state.nv.us/App/NELIS/REL/83rd2025/Bill/12205/Overview>

^{xiii} California AB-2013, *Generative Artificial intelligence: Training data transparency*, September 28, 2024.

https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB2013

^{xiv} California, SB-942, *California AI Transparency Act*, September 19, 2024.

https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240SB942

^{xv} Colorado, SB 24-205, *The Colorado AI Act*, May 17, 2024.

https://leg.colorado.gov/sites/default/files/2024a_205_signed.pdf

^{xvi} Utah, SB-226, *Artificial Intelligence Consumer Protection Amendments*, March 27, 2025

<https://le.utah.gov/~2025/bills/static/SB0226.html> and

<https://le.utah.gov/%7E2024/bills/static/SB0149.html>

^{xvii} Virginia, HB2250, *Artificial Intelligence Training Data Transparency Act; Transparency and Disclosure Requirements*, February 4, 2025.

<https://lis.virginia.gov/bill->

[details/20251/HB2250#:~:text=Summary%20As%20Introduced,of%20the%20consumer's%20personal%20data.](https://lis.virginia.gov/bill-details/20251/HB2250#:~:text=Summary%20As%20Introduced,of%20the%20consumer's%20personal%20data.)

^{xviii} Massachusetts, General Law – Part 1, Title II, Chapter 6, Section 220: *The Massachusetts Police Reform Law*, December, 31, 2020

[https://malegislature.gov/Laws/GeneralLaws/PartI/TitleII/Chapter6/Section220#:~:text=\(b\)%20Any%20law%20enforcement%20agency,the%20Federal%20Bureau%20of%20Investigation.](https://malegislature.gov/Laws/GeneralLaws/PartI/TitleII/Chapter6/Section220#:~:text=(b)%20Any%20law%20enforcement%20agency,the%20Federal%20Bureau%20of%20Investigation.)

^{xix} Washington, RCW, Title 43, Chapter 43.386.010 (Facial Recognition Law, effective date July 1, 2021)

<https://app.leg.wa.gov/RCW/default.aspx?cite=43.386&full=true>

^{xx} California, *Governor Newsom signs bills to crack down on sexually explicit deepfakes & require AI watermarking*, dated September 19, 2024.

<https://www.gov.ca.gov/2024/09/19/governor-newsom-signs-bills-to-crack-down-on-sexually-explicit-deepfakes-require-ai-watermarking/#:~:text=SB%20926%20by%20Dr.,that%20person%20serious%20emotional%20distr>
[ess](https://www.gov.ca.gov/2024/09/19/governor-newsom-signs-bills-to-crack-down-on-sexually-explicit-deepfakes-require-ai-watermarking/#:~:text=SB%20926%20by%20Dr.,that%20person%20serious%20emotional%20distr)

^{xxi} Texas, Tx. Pen. Code § 21.165, *Unlawful Production or Distribution of Certain Sexually Explicit Videos*, effective November 21, 2023.

<https://casetext.com/statute/texas-codes/penal-code/title-5-offenses-against-the-person/chapter-21-sexual-offenses/section-21165-unlawful-production-or-distribution-of-certain-sexually-explicit-videos>