

AI and Healthcare: Key Legal Issues for CSBs

► Presented by: **Liz Heddleston & Patrick Austin**



AGENDA

- I. AI in Healthcare – Promise and Perils
- II. AI Foundations
- III. Legal Risks and Remedies
- IV. AI and CSBs
 - a) Tips for Implementing AI
 - b) AI and EHRs
 - c) AI and Patient Care
 - d) AI and HIPAA
- V. AI Regulatory Landscape
- VI. Looking Ahead



AI & Healthcare - The Big Picture





AI and Healthcare – The Big Picture

- Healthcare is over 17% of the U.S. GDP
- Generates over 30% of world data
- Growing shortages of physicians and other healthcare professionals
- Overwork and burnout
- Regulatory burdens
- Complex legal landscape – patchwork of state and federal law

“The Promise of AI to Improve Health Outcomes”

- “As President Biden has said, **artificial intelligence (AI) holds tremendous promise and potential peril**. In few domains is this truer than healthcare. The President has made clear, [including by signing a landmark Executive Order on October 30](#), that the entire Biden-Harris Administration is committed to placing the highest urgency on governing the development and use of AI safely and responsibly to drive improved health outcomes for Americans while safeguarding their security and privacy.”
 - *Dec. 14, 2023, White House Press Release*

AI and Healthcare – Promise and Peril

- **Promise of AI**

- Improve patient care
- Make processes more efficient and save time
- Alleviate administrative burdens on providers and organizations

- **Perils of AI**

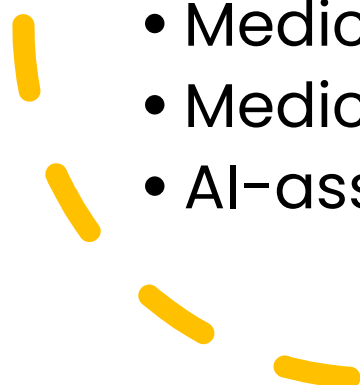
- Safety
- Accuracy
- Privacy & Security
- Bias
- Legal Liability





Common Uses of AI in Healthcare

- Ambient listening/transcription of physician-patient conversations and preparation of notes/EHR integration
- Natural language processing to review clinical notes
- Customer service chatbots for patients
- Physician email triage and management
- Medical coding and billing
- Medical imaging analysis
- AI-assisted diagnosis and early disease detection



AI in Behavioral Healthcare

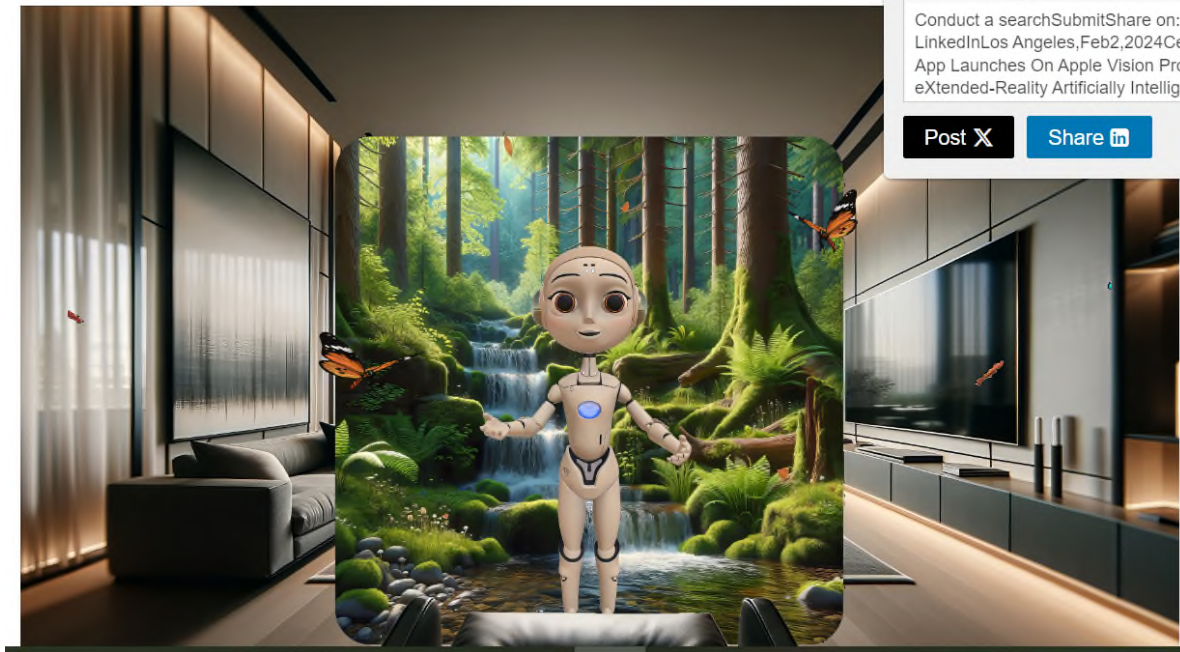
60 MINUTES - NEWSMAKERS

Mental health chatbots powered by artificial intelligence developed as a therapy support tool

Woebot is an app on your phone... kind of a pocket therapist that uses the text function to help manage problems like depression, anxiety, addiction, and loneliness... and do it on the run.


AI in Behavioral Healthcare

Cedars-Sinai Behavioral Health App Launches On Apple Vision Pro



Biden Administration's Executive Order on AI



- Two Big Takeaways for Healthcare Industry
 1. **Responsible deployment of AI in Healthcare.** HHS will establish an AI Task Force to develop policies to responsibly deploy AI in the healthcare sector. Outputs from the Task Force will impact a broad range of stakeholders, including **providers**, payers, drug companies, public health officials, regulators and patients.
 2. **Enforcement of Existing Law to Prevent Harmful Use of AI.** Federal agencies are directed to enforce existing laws to mitigate against AI practices that result in unfair or deceptive business practices, privacy violations, or discrimination.
- 

UNDERSTANDING AI AND ITS FOUNDATIONS



AI – Definition & Elements

Evolving definition of AI...

A machine-based system that uses mathematical computational techniques to perform human-like activities or tasks.

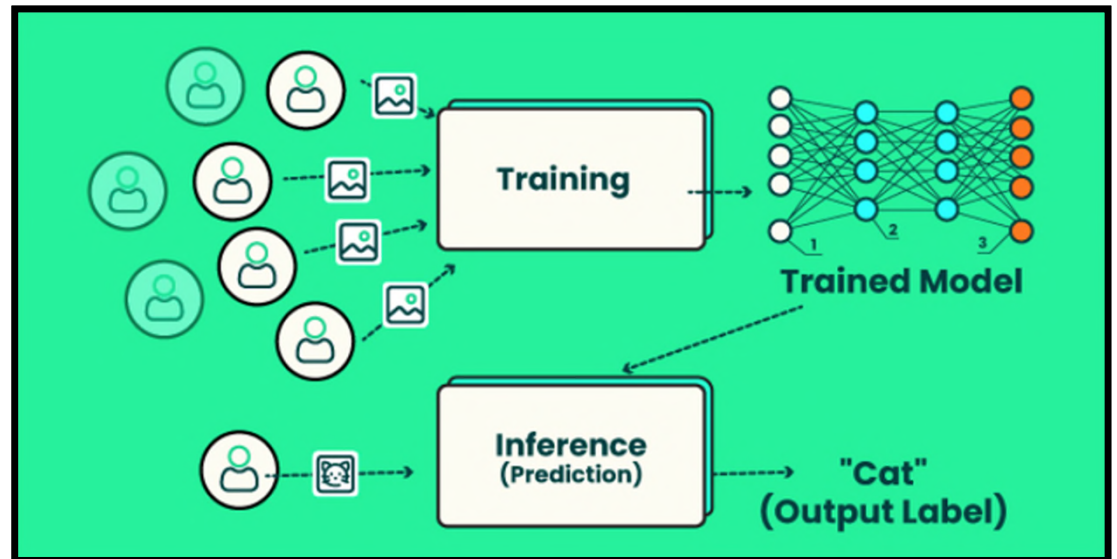
Sources: 15 U.S.C. § 9401(3); IAPP, *Key Terms for AI Governance*; Forbytes

*An AI system is a machine-based system that, for **explicit or implicit** objectives, **infers, from the input it receives, how to generate outputs** such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment*

Source: [OECD, Updates to the OECD's definition of an AI system explained \(Nov. 29, 2023\)](#).

Machine Learning

A data processing mechanism that uses **training data** as an **input** to iteratively learn and “train” a **model** that makes predictions, inferences, or decisions to generate an **output**.




Source: [Forbytes](#)

Generative AI

- AI that generates new content (such as text, images, and videos) based on learned patterns of data.
- Examples: ChatGPT and Google Gemini.

Figure 1. Examples of Generative AI Models

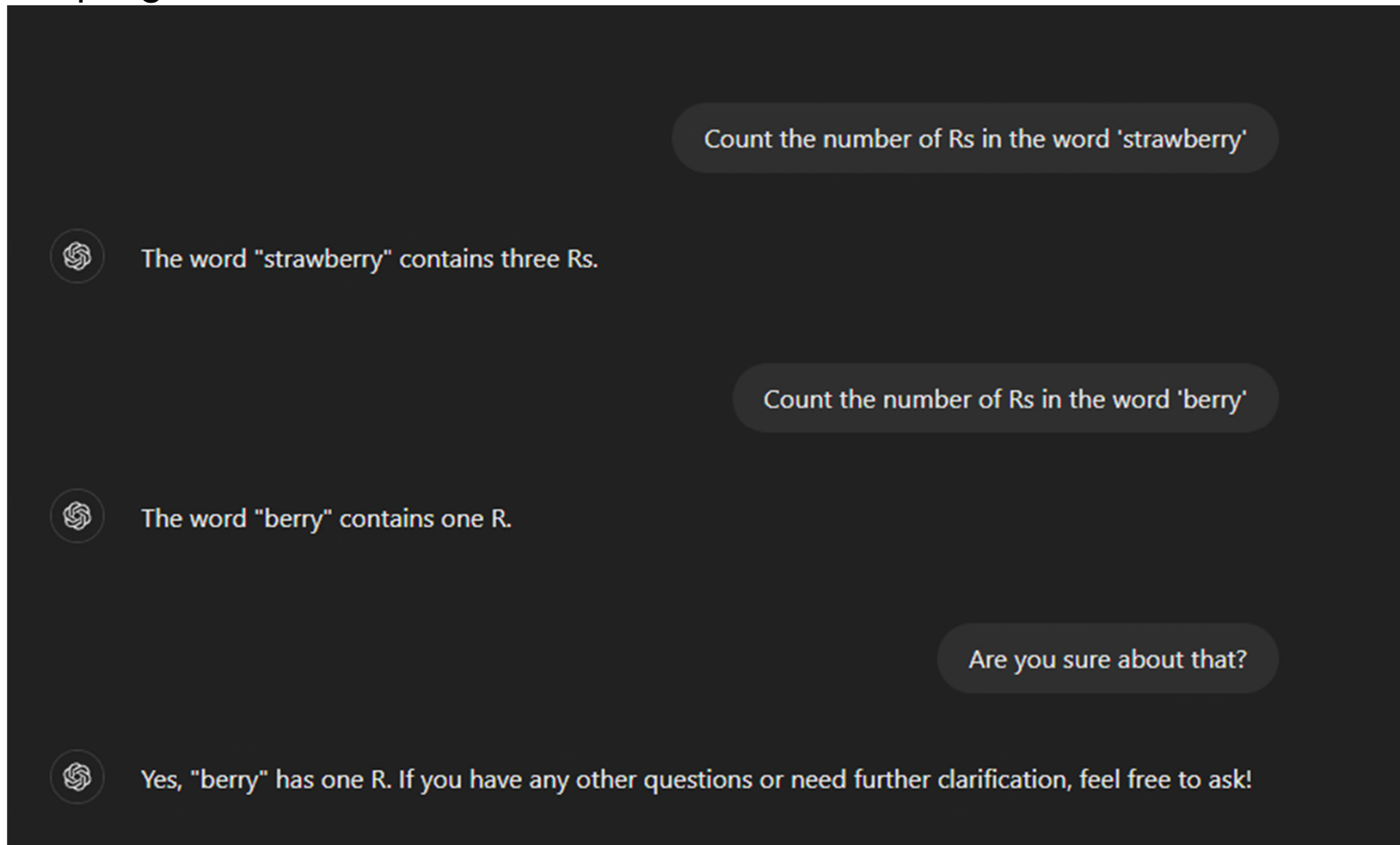
Image Generator	Chatbot
<p data-bbox="940 565 1486 618">Prompt: "The Library of Congress building in the style of Van Gogh."</p> <p data-bbox="940 630 1058 656">Response:</p> 	<p data-bbox="1528 565 2066 618">Prompt: "Write a 4 sentence poem about the Library of Congress."</p> <p data-bbox="1528 630 1646 656">Response:</p> <p data-bbox="1528 675 1913 813"><i>"In the heart of D.C., there stands a place A temple of knowledge, a palace of grace The Library of Congress, a marvel to see A monument to learning, for you and me</i></p> <p data-bbox="1528 857 1948 995"><i>Rows upon rows of books, towering high A treasury of history, never to die Where stories and knowledge, together reside A beacon of wisdom, that cannot be denied"</i></p>

Source: Stable Diffusion and ChatGPT, via CRS. The image was generated by Stable Diffusion and the text response was generated by ChatGPT.

Source: [Congressional Research Service, *Generative Artificial Intelligence and Data Privacy: A Primer* \(May 23, 2023\).](#)

Generative AI

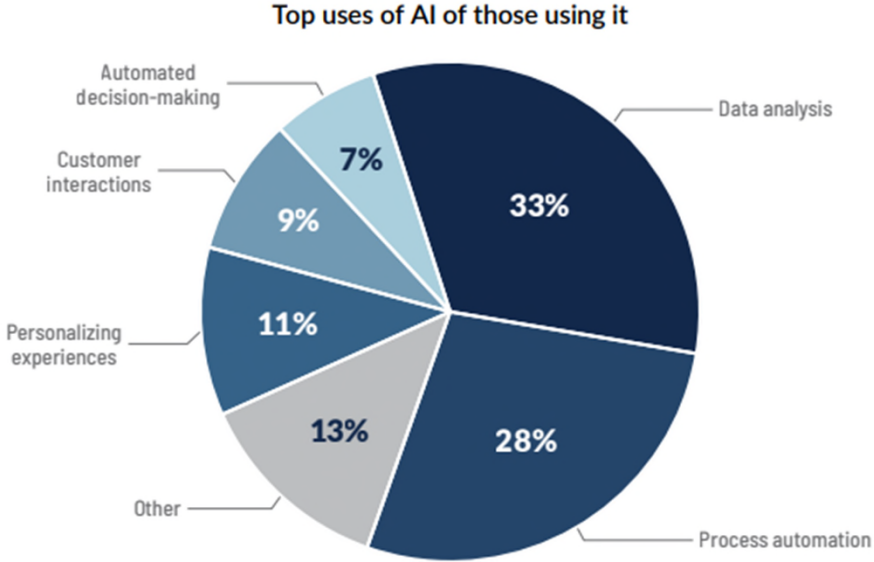
- Still a work in progress.



Use of AI in Organizations



Currently use AI	Intend to use AI within the next 12 months	Not currently using AI	Unsure
52%	22%	19%	7%

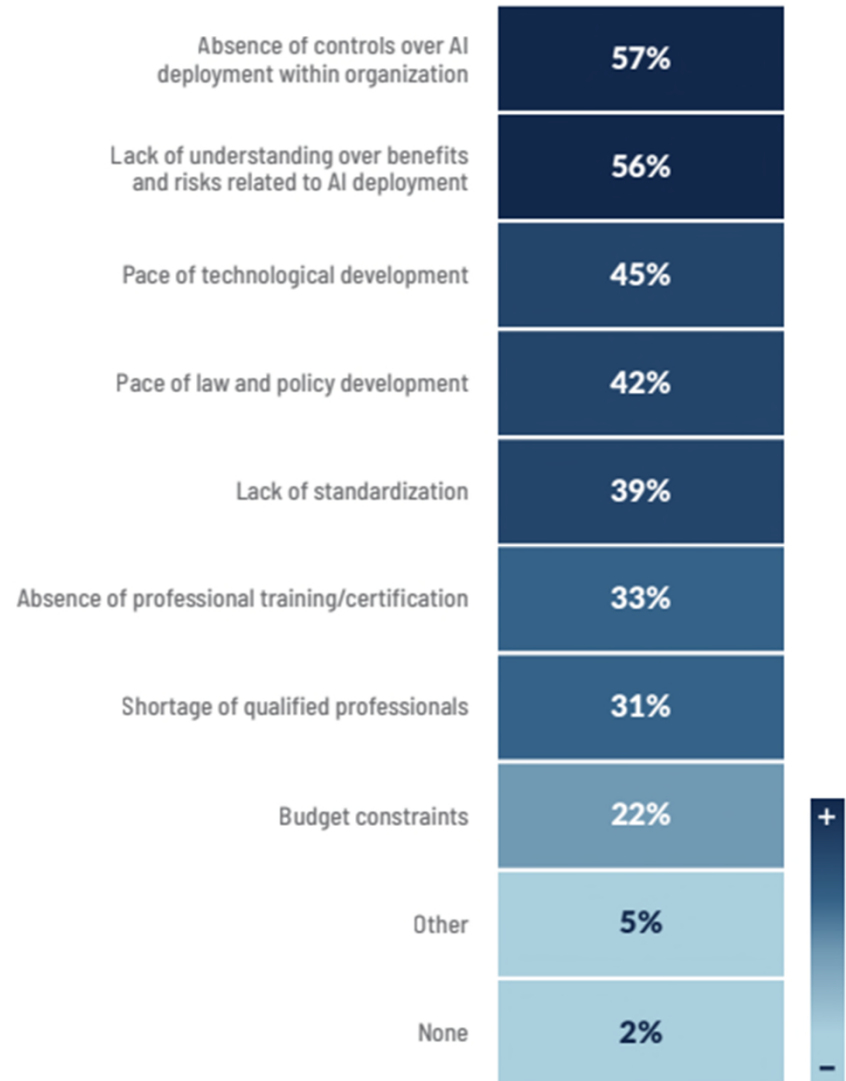


Source: [IAPP/EY \(Dec. 2023\)](#)

Challenges in Implementing AI Governance



Source: [IAPP/EY \(Dec. 2023\)](#)



AI / CORE LEGAL RISKS & REMEDIES



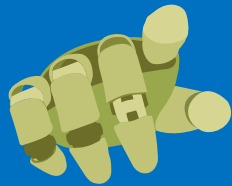
AI / CORE LEGAL RISKS



A

DATA PRIVACY

Relying on vast amounts of data to train and improve algorithms brings into question how to comply with privacy laws, especially when sensitive personal information is involved.



B

INTELLECTUAL PROPERTY

Issues include ownership of training data (copyright, trademark, patent), ownership of AI-created content, and the potential to lose sensitive protected information when inputting it into AI.



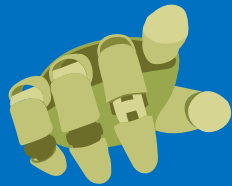
AI / CORE LEGAL RISKS



C

Discrimination

AI can inadvertently perpetuate bias, especially if training on random historical data.



D

Tort Liability

If the AI system produces inaccurate results, negligent results, that harm others or other systems, then legal damages can flow from that.



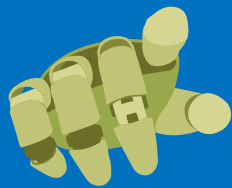
AI / CORE LEGAL RISKS



E

Consumer Protection

AI-use in anything affecting commerce could implicate scrutiny by the FTC or state regulators for unfair, deceptive, or abusive trade practices.



F

Contract Liability

Depending on contractual terms, use of AI or sharing confidential information or trade secrets with AI could result in breach.

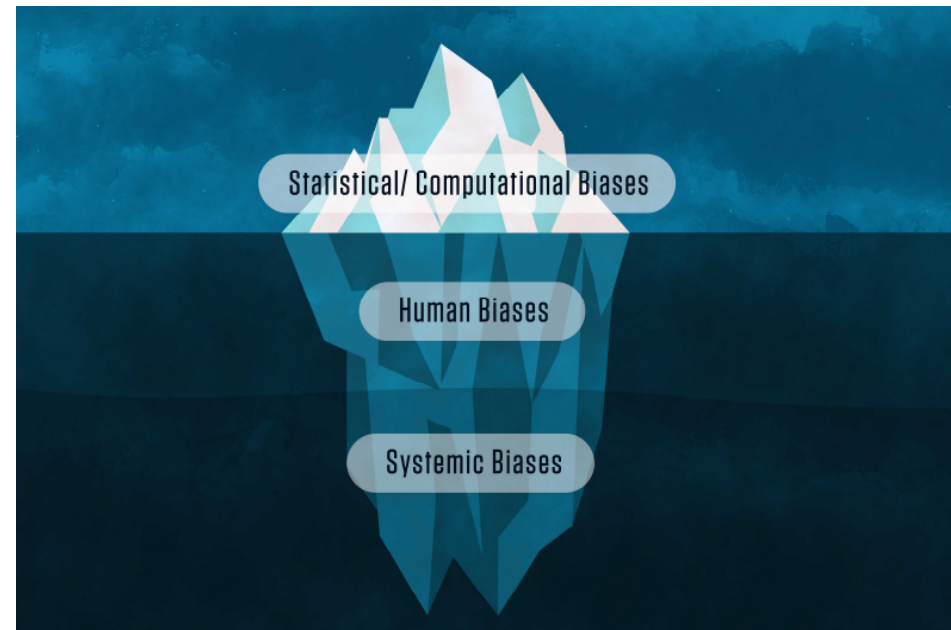


NIST Categories of AI Bias

- **Systemic Bias:** Result from procedures and practices of institutions that operate in ways which result in certain social groups being advantaged or favored and others being disadvantaged or devalued. This need not be the result of any conscious prejudice or discrimination but rather of the majority following existing rules or norms.
 - Examples: Institutional racism and sexism.

- **Human Bias:** This type of bias is often implicit and tends to relate to how an individual or group perceives information (such as automated AI output) to make a decision or fill in missing or unknown information. Human biases are typically omnipresent in the institutional, group, and individual decision-making processes across the AI lifecycle, and in the use of AI applications once deployed.

- **Statistical and Computational Bias:** Stems from errors that result when the sample is not representative of the population. These biases arise from systematic as opposed to random error and can occur in the absence of prejudice, partiality, or discriminatory intent.
 - In AI systems, these biases are present in the datasets and algorithmic processes used in the development of AI applications, and often arise when algorithms are trained on one type of data and cannot extrapolate beyond those data.



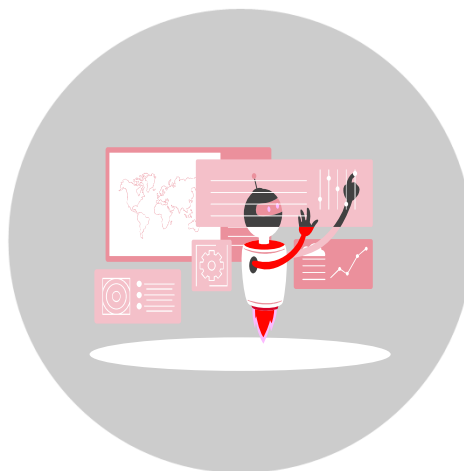




Remedies



**Damages &
Injunctions**



Model Deletion



**Enforcement Actions,
Penalties & Fines**

AI in Hiring: Discrimination



- **EEOC v. iTutorGroup**
- EEOC reached a settlement in a novel AI discrimination lawsuit
 - iTutorGroup used AI-powered recruitment software
 - A job applicant was rejected by iTutorGroup. The applicant decided to submit their same resume for the exact same position but included a younger birthdate in second submission. The second submission led to a job interview.
 - The applicant decided to file a complaint with the EEOC, which filed a lawsuit against iTutorGroup on behalf of more than 200 applicants alleging age and gender discrimination.
 - The lawsuit alleged **the company illegally screened out women applicants over 55 and men over 60 in violation of the Age Discrimination in Employment Act.**
 - iTutorGroup agreed to pay \$365,000 as part of the EEOC settlement.
 - The company also agreed to adopt anti-discrimination policies and conduct trainings to ensure compliance with equal employment opportunity laws.
 - They must also consider anew all applicants that were purportedly rejected because of their age.

Sources: [EEOC](#) (Sept. 11, 2023); [Equal Employment Opportunity Commission v. iTutorGroup, Inc. et al, Docket No. 1:22-cv-02565](#) (E.D.N.Y. May 05, 2022), [Court Docket](#)

AI in Hiring: CVS AI “Lie Detector” Settlement



- CVS Health Corp./CVS Pharmacy reached a tentative settlement in a proposed class-action lawsuit accusing the company of making job applicants take a lie detector test during the interview process without notice.
- A Massachusetts resident applied for a supply chain position with CVS in January 2021. They weren't hired for the job. Subsequently, the applicant learned their interview was analyzed by HireVue through Affectiva technology to track facial expressions such as “smiles, surprise, contempt, disgust, and smirks,” which then assigned candidates an “employability score,” according to the complaint.
 - Part of the employability score included analysis of a candidate’s “conscientiousness and responsibility,” including a candidate’s “innate sense of integrity and honor,” the complaint said.
- The applicant was **unable to opt out** of the HireVue video interview technology or Affectiva’s AI analysis, and they were **not provided the chance to challenge the assessment**.
- The settlement notice did not disclose specific details about monetary agreements or changes in CVS practices.

Texas AG Investigation into Gen AI Healthcare Company

- Texas AG secured a first-of-its-kind settlement with an AI healthcare technology company called Pieces Technologies.
- The Texas AG alleged that Pieces deployed its AI products at multiple Texas hospitals after making a series of **false and misleading statements about the accuracy and safety of its products in violation of the Texas Deceptive Trade Practices – Consumer Protection Act.**
- Hospitals were providing their patients' healthcare data in real time to Pieces so that its generative AI product could "summarize" patients' condition and treatment for hospital staff.
- An investigation conducted by the Texas AG found that Pieces **made deceptive claims about the accuracy of its healthcare AI products, putting the public interest at risk.**
- Pieces developed a series of metrics to claim that its healthcare AI products were "highly accurate," including advertising and marketing the accuracy of its products and services by claiming they have a "critical hallucination rate" and "severe hallucination rate" of "<.001%" and "<1 per 100,000."



Texas AG Investigation into Gen AI Healthcare Company

- Texas alleged that Respondent's representations regarding its generative AI products **may** have violated the DTPA because they were false, misleading, or deceptive.
- Pieces denied any wrongdoing. Nevertheless, they agreed to settle with the AG's Office. Further details about the AG's investigatory findings were disclosed.
- **Settlement Terms**
 - No monetary damages or fines, but potential reputational damage.
 - Pieces must clearly and conspicuously disclose (1) the meaning or definition of its metric, benchmark, or similar measurements, including (2) the method, procedure, or any other process used by Pieces, or on their behalf, to calculate the metric, benchmark, or similar measurement used in marketing or advertising its products and services.
 - Pieces is prohibited from making any false, misleading, or unsubstantiated representations, whether regarding any feature, characteristic, function, testing or appropriate use of any of its products
 - Pieces must provide all its customers, in connection with any of its products or services, documentation that clearly and conspicuously discloses any known or reasonably knowable harmful or potentially harmful uses or misuses of its products or services.
 - Agrees to compliance monitoring by the Texas AG's Office.
 - Settlement terms remain in force for 5 years.



Texas AG Investigation into Gen AI Healthcare Company

- In announcing the settlement agreement, Texas AG Paxton stated that "AI companies offering products used in **high-risk settings** owe it to the public and to their clients to be transparent about their risks, limitations, and appropriate use. Anything short of that is irresponsible and unnecessarily puts Texans' safety at risk[.]"
- Paxton went on to state that "**[h]ospitals and other healthcare entities** must consider whether AI products are appropriate and train their employees accordingly."



Community Services Boards & AI





AI and Legal Risks in Healthcare Space

Examples of Lawsuits and Investigations

- Allegations that provider decisions are being overridden by AI algorithms
- Allegations that certain healthcare facilities use algorithms to guide staffing decisions, and such algorithms resulted in understaffed facilities or care that fell below standards
- Allegations that staff who complained about staffing or medical care algorithms were the subject of retaliation, terminated or discipline
- Allegations that healthcare plans denied medically necessary care because of AI-powered algorithms

How Can CSBs Respond to AI Risks?

- **Perform Due diligence before adopting AI**
 - Understand AI technology enough to identify and respond to its unique risks
 - Vet AI vendors
 - Review and negotiate contracts with AI vendors to mitigate risk



How Can CSBs Respond to AI Risks?

- **Build internal frameworks to monitor use of AI**
 - Identify and track AI uses within your organization
 - Develop risk management & compliance processes
 - Monitor and audit use of AI tool





How Can CSBs Respond to AI Risks?

- **Policies and workforce training on acceptable use of AI tools**
 - Adopt policies and procedures that account for the unique risks of AI
 - Education of workforce and providers
- **Proactive legal compliance approach**
 - Track application of existing law to AI
 - Lookout for new legal developments

AI & ELECTRONIC HEALTH RECORDS (EHR)



AI and EHRs

How Epic is using AI to change the way EHRs work

Sumit Rana, head of research and development, discusses how the EHR giant's system uses AI to generate progress notes, create draft responses to patient questions and assist with medical coding. And how AI sometimes can be more empathetic than a person.

Source: Healthcare IT News, Nov. 28, 2023

AI and EHRs – Legal Issues

DOJ Enforcement Action – Practice Fusion

- AI-powered clinical decision support tool led to unnecessary opioid prescriptions that were billed to federal healthcare programs



PRESS RELEASE

Electronic Health Records Vendor to Pay \$145 Million to Resolve Criminal and Civil Investigations

Monday, January 27, 2020

Share >

For Immediate Release

Office of Public Affairs

Practice Fusion Inc. Admits to Kickback Scheme Aimed at Increasing Opioid Prescriptions

AI and Medical Records

- **Rise of AI to act as a scribe and interact with EHR to support medical record documentation**
 - Potential to address provider burden and streamline documentation
 - Risk of inaccurate documentation and patient harm due to inaccurate records
 - Provider is liable for harm caused by improper documentation (malpractice, professional discipline, etc.)
 - Provider had a duty to review records created with AI to ensure they are accurate and properly managed
 - Security risks related to inputting PHI into AI tools
 - Awareness of and adherence to security measures
 - Contractual protections with AI vendors/Business Associates

AI and EHRs – Practical Issues

For successful adoption, AI tools must answer four basic:

- Does it work?
- Will it work in my organization?
- Will I be paid enough to cover the cost of investment?
- If something goes wrong, will I be liable?

AI & PATIENT CARE



AI and Patient Care



Navigating the Responsible and Ethical Incorporation of Artificial Intelligence into Clinical Practice

Adopted by FSMB House of Delegates, April 2024

EXECUTIVE SUMMARY

Artificial Intelligence (AI) holds tremendous potential to aid healthcare providers in diagnosis, treatment selection, clinical documentation, and other tasks to improve quality, access, and efficiency. However, these technologies introduce risks if deployed without proper "guardrails" and understanding which may impact considerations in clinical practice as well as regulatory processes of state medical boards. By taking a proactive and standardized governance approach anchored in ethical principles, state medical boards can promote safe and effective integration of AI, in its various forms, while prioritizing patient wellbeing.

AI in Patient Care

- **Key Points from FSMB Guidance**

- Physician/provider is ultimately responsible (and liable) for patient care and must practice within the standard of care.
- Failure to apply human judgement to any output of AI is a violation of a physician's professional duties.
- Once a physician chooses to use AI, they accept responsibility for responding appropriately to the AI's recommendations.

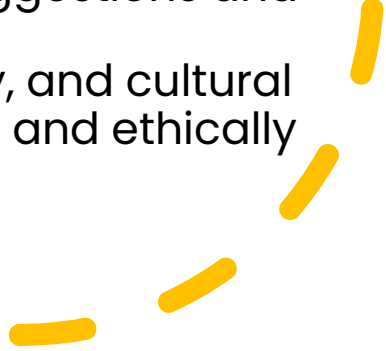


AI in Behavioral Health Settings

- Guidance from American Counseling Association:

“Counselors must understand the limitations of AI in diagnosis and assessment in all counseling settings.

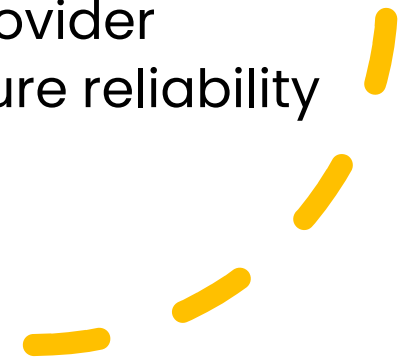
Counselors should refrain from using AI as the sole tool for diagnosis and assessment in counseling. Although AI can be a supportive tool to inform a counselor's professional judgment, counselors must attain adequate training to understand the limitations and the use of AI in clinical settings... Counselors must critically evaluate AI-assisted diagnostic suggestions and incorporate their clinical expertise, understanding of the client's history, and cultural context to ensure a comprehensive and ethically sound assessment..”



AI and Patient Care

- **Best Practices for Informed Consent**

- Obtain informed consent prior to using AI tool in patient care, especially when patient data is inputted into AI tool.
- When and how AI is used in their care
- Capabilities and limitations of AI tools (including how their data is used)
- How AI is used in diagnosis and treatment planning
- Explain continued role of provider
- Safeguards in place to ensure reliability of AI output



Informed Consent and Counseling

- **American Counseling Association Recommendation:**
 - “Counselors should clearly inform clients about the use of AI tools in their counseling process, explaining their purpose and potential benefits. **Obtain explicit informed consent from clients for the use of AI-assisted tools,** ensuring they understand the implications and potential impact on their treatment”



AI and Liability Risks in Patient Care

- Key Issues
 - Negligence and standard of care
 - Improper use of AI tools
 - Undue deference to AI



AI & Healthcare – State Laws

- Massachusetts H.1974 – Regulating AI in Mental Health Services

(a) Any licensed mental health professional who wishes to provide mental health services through the use of AI shall first seek approval from the relevant professional licensing board.

(b) Any AI system used to provide mental health services must be designed to prioritize the safety and well-being of individuals seeking treatment and must be continuously monitored by a licensed mental health professional to ensure its safety and effectiveness.

(c) Any licensed mental health professional providing mental health services through the use of AI shall inform patients of the use of AI in their treatment and provide them with the option to receive treatment from a licensed mental health professional.

(d) Any licensed mental health professional providing mental health services through the use of AI shall disclose the use of AI to patients in advance and obtain their informed consent.

AI & Bias in Healthcare – Federal Law

New ACA Requirements: On May 6, 2024, the HHS-OCR and CMS published a new final rule under Section 1557 of the Affordable Care Act (ACA) that aims to broadly address discrimination and inequity across health care

- The regulations put a **proactive burden** on providers to make sure they are tracking and mitigating discriminatory use of AI
 - Applies broadly to healthcare providers & other entities that receive federal funding
 - Prohibits discrimination on the basis of race, color, national origin, sex, age, or disability through the use of “patient care decision support tools” --- defined as “any automated or non-automated tool, mechanism, method, technology, or combination thereof used to support clinical decision-making”
 - Tools may be used for activities such as patient screening, risk prediction, diagnosis, prognosis, clinical decision-making – **including AI tools**

AI & HIPAA



AI and Patient Privacy & Security

- **Key Issues**

- Huge amount of data is needed to train and develop AI tools
- Providers using and implementing AI tools may need to input sensitive PHI of their own patients
- Legal landscape governing the privacy and security of health data is complex and evolving



AI and HIPAA

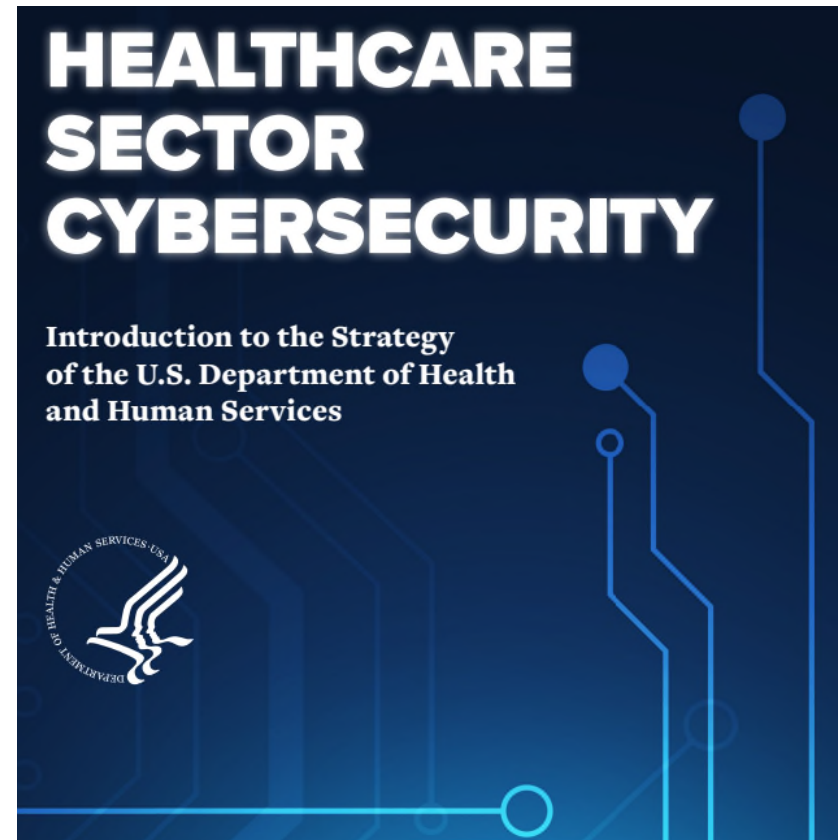
• HIPAA Privacy Rule Issues

- BAAs needed with AI vendors that process and access PHI on behalf of CSB
- Handling requests from vendors for access to PHI to train its AI model
 - Written patient consent
 - Applicable HIPAA exceptions
 - De-identification standard



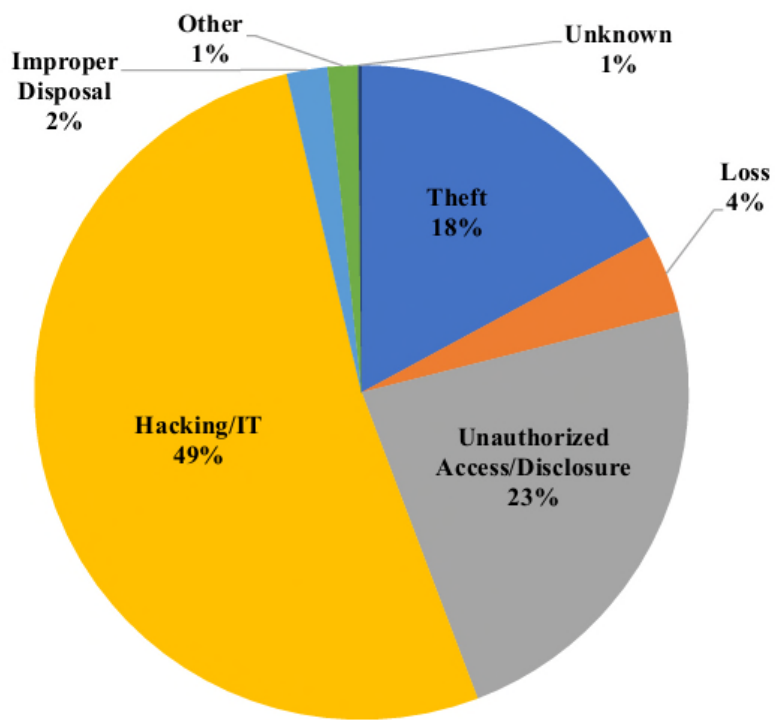
Healthcare Sector Cybersecurity

“The healthcare sector is particularly vulnerable to cybersecurity risks and the stakes for patient care and safety are particularly high. Healthcare facilities are attractive targets for cyber criminals in light of their size, technological dependence, sensitive data and unique vulnerability to disruptions.”

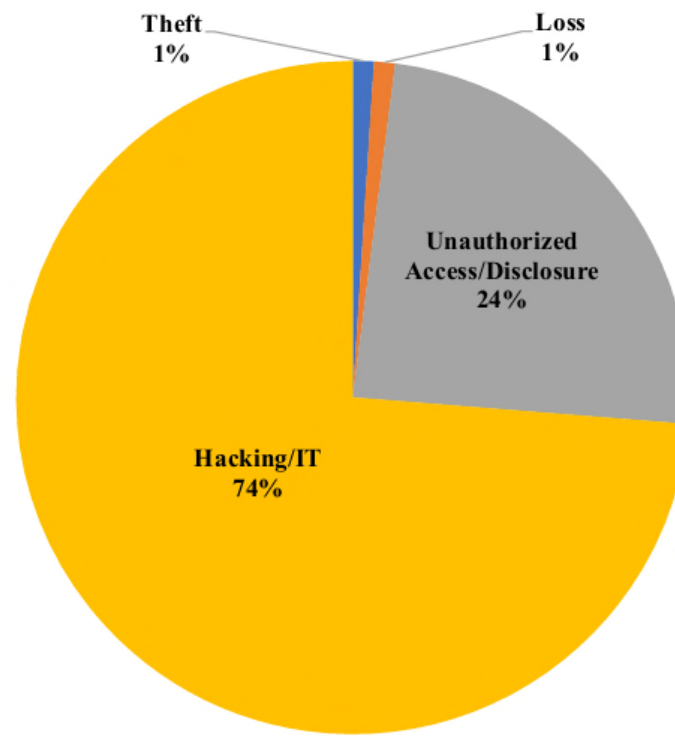


HIPAA Breach Trends

500+ Breaches by Type of Breach



September 23, 2009 through Dec 31, 2023



January 1, 2024 through February 29, 2024

• Sour

AI and HIPAA



- **HIPAA Security Rule Issues**

- Patient data is a prime target of cyber criminals seeking to exploit this sensitive data for financial gain
- Security practices related to AI tools using PHI need to comply with HIPAA to ensure PHI is appropriately secured & protected
 - Covered Entities (CSBs, providers)
 - Business Associates (AI vendors)

AI and HIPAA



- HIPAA Security Rule Compliance Tips
 - Vet vendors offering AI tools
 - Understand how patient data will be used and be prepared to convey this to patients
 - Due diligence on vendor's cybersecurity safeguards
 - Robust HIPAA compliance program
 - Perform Security Risk Analysis at least annually to assess risks and vulnerabilities to PHI
 - Workforce training
 - Business Associate Agreements – pay close attention to terms related to indemnity, limitation of liability
 - Cyber liability insurance

AI and 42 CFR Part 2

- **42 CFR Part 2**

- Governs “substance use disorder” information
- In general, NRVCS may not disclose SUD information unless the patient provides written consent or a legal exception applies. This includes any information that would identify a person as having (or having had) a substance use disorder.

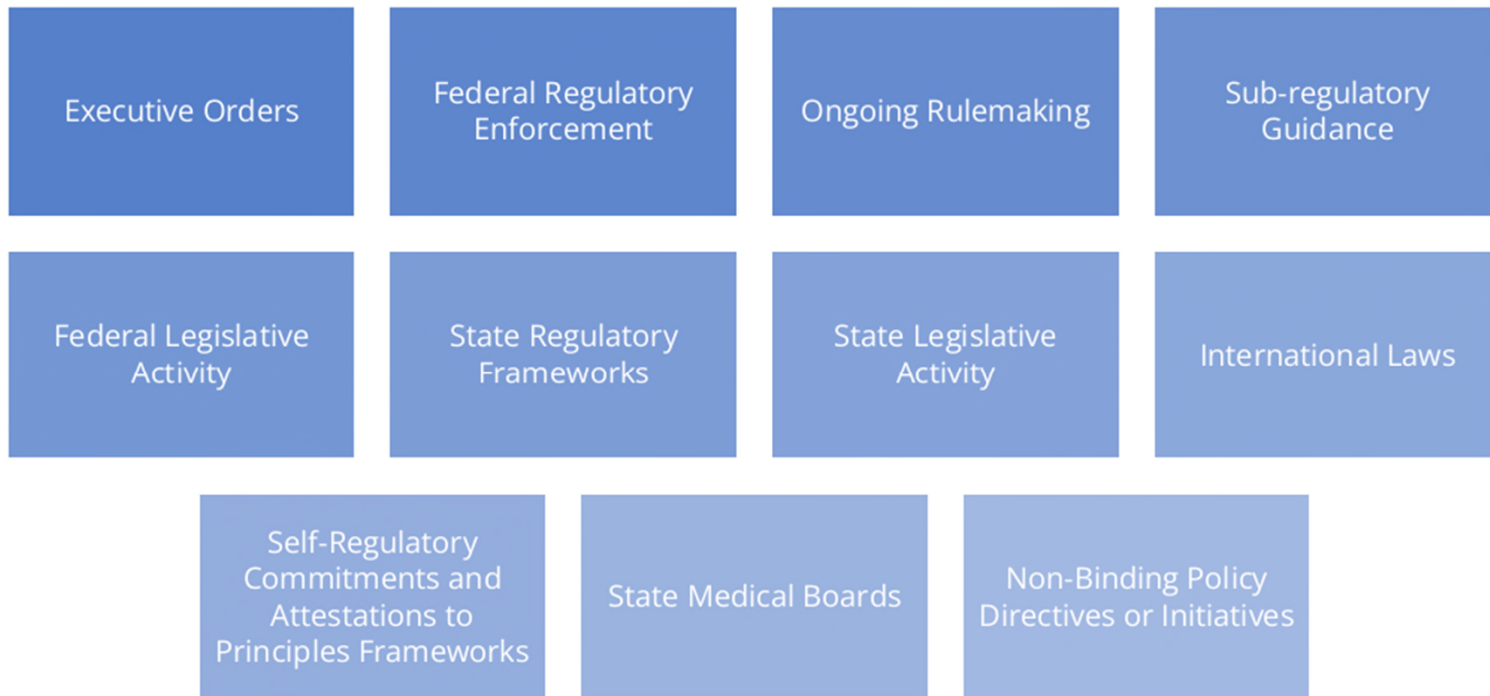
AI and 42 CFR Part 2

- **Recent Amendments to Part 2** – Effective on April 16, 2024; Compliance deadline February 16, 2026
- **Patient Consent**
 - Allows a single consent for all future uses and disclosures for treatment, payment, and health care operations.
 - Allows HIPAA covered entities and business associates that receive records under this consent to redisclose the records in accordance with the HIPAA regulations
- **Penalties:** Aligns Part 2 penalties with HIPAA by replacing criminal penalties currently in Part 2 with civil and criminal enforcement authorities that also apply to HIPAA violations.²
- **Breach Notification:** Applies the same requirements of the HIPAA Breach Notification Rule³ to breaches of records under Part 2.

AI Regulatory Landscape



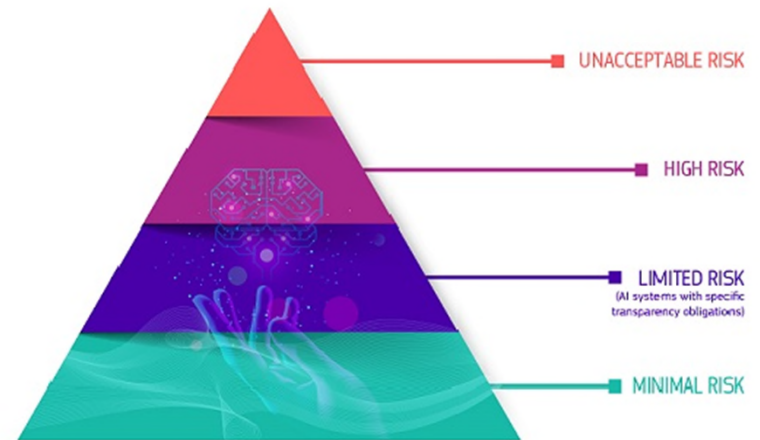
THE RACE TO REGULATE AI



E.U. AI Act

- The European Parliament adopted the Artificial Intelligence Act (AI Act) on March 14, 2024.
- Entered into force across all 27 EU Member States on August 1, 2024. Though, **enforcement of most provisions will not commence until August 2, 2026.**
- Considered to be the world's first comprehensive horizontal legal framework for AI.
- **Applies to “providers” and “deployers” of AI systems.**
 - Providers: Companies that develop AI systems with a view to placing them on the market or putting them into service under their own name or trademark, whether for payment or free of charge).
 - Includes importers and distributors of AI systems in the EU.
 - Deployers: Natural or legal persons using AI under their authority in the course of their **professional** activities.

The Regulatory Framework defines 4 levels of risk in AI:



Source: [European Commission](#)



EXECUTIVE ORDER 14110

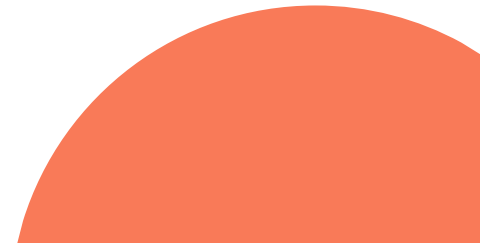
- “Whole of government” approach to AI oversight
- The Biden Administrations’ EO established new standards for AI safety and security, including the **required sharing of safety test results** and other critical information with the U.S. government.
- Directs Department of Commerce will develop guidance for content authentication and watermarking to clearly label AI-generated content
- Directs the Department of Health and Human Services (HHS) to **establish a safety program to receive reports of—and act to remedy – harms or unsafe healthcare practices involving AI.**
- Establishment of an **HHS AI Task Force** to “develop a strategic plan” that includes policies and frameworks on the responsible deployment of AI and AI-enabled technologies in the health and human services sector (including research and discovery, drug and device safety, healthcare delivery and financing, and public health).
- **Provide guidance to landlords, Federal benefits programs, and federal contractors to keep AI algorithms from being used in a discriminatory manner.**



OCTOBER 30, 2023

Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

 BRIEFING ROOM  PRESIDENTIAL ACTIONS



STATE-LEVEL

Comprehensive AI Legislation

- Colorado

vs.

Targeted AI Legislation

- Disclose Use of AI in Employment Decisions:
 - Illinois
 - New York City
- AI “Deepfake” Media in Political Ads:
 - Wisconsin
 - Michigan
 - New Mexico
 - Oregon
- AI “Deepfake” Adult Content Laws:
 - California
 - Virginia
 - Georgia
 - Illinois
 - South Dakota

VIRGINIA AI EXECUTIVE ORDERS

- Five key directives:
 1. Enactment of AI Policy Standards published by the Virginia Information Technologies Agency (VITA), including:
 - **Approval Process for AI Tools:** Before a public agency can deploy an AI tool or application, disclosures must be made to VITA such as an identification and description of the AI tool/application at the model-level (e.g., model inputs, output data type and structure, model algorithms, and data sets)
 - **Mandatory Disclaimers:** When AI capabilities are used to process or produce any decision or output regarding citizens or businesses, **a disclaimer must be used explaining the degree of AI involvement in the decision or output.**
 2. Enactment of AI Information Technology Standards, also published by VITA
 - The AI IT Standards call for the development of specific requirements for how new and existing AI systems are integrated into enterprise architecture.
 - VITA guidance details the technical standard for the management, development, purchase, and use of AI in the Commonwealth, aimed to promote AI safety, privacy, transparency, accountability, and sustainability.
 3. Enactment of AI Education Guidelines applicable to K-12 schools, community colleges, and universities
 4. Directive to establish AI standards for executive branch law enforcement and model standards for local law enforcement by **October 2024.**
 5. Establishment of an AI Task Force, which will produce a report on the use of AI by the end of 2024.

BIG FRAMEWORK: COLORADO AI LAW

Regulating AI when it impacts “consequential” decisions (i.e., applying to college, applying for a small business loan, applying for a mortgage, etc.)

- Colorado’s “Consumer Protections for Interactions with Artificial Intelligence” law was enacted on May 17, 2024. Expected to go into effect February 1, 2026.
- Requires “**developers and entities**” that deploy “**high-risk AI systems**” to use **reasonable care** to prevent algorithmic discrimination.
 - High-risk AI system defined as **those that make or are a substantial factor in making “consequential” decisions**. Defines a “substantial factor” as a factor that (i) assists in making a consequential decision, (ii) is capable of altering the outcome of a substantial decision, or (iii) is generated by an AI system.
 - **Consequential decision** defined as a decision that has a “**material legal or similarly significant effect**” on the provision or denial to any consumer of, or the cost or terms of:
 - Education enrollment or opportunity
 - Employment or employment opportunity
 - Financial or lending services
 - Essential government services
 - Health care services
 - Housing
 - Insurance
 - Legal services

BIG FRAMEWORK: COLORADO AI LAW

- **Exempted Technologies**

- The following technologies are generally not considered a "high-risk" AI systems:
 - Anti-fraud technology that does not use facial recognition technology;
 - Anti-malware;
 - Anti-virus;
 - Artificial intelligence-enabled video games;
 - Calculators;
 - Cybersecurity;
 - Databases;
 - Data storage;
 - Firewall;
 - Internet domain registration;
 - Internet website loading;
 - Networking;
 - Spam and robocall filtering;
 - Spell-checking;
 - Spreadsheets;
 - Web caching;
 - Web hosting or any similar technology; or
 - Technology that communicates with consumers in natural language for the purpose of providing users with information.

Source: [SB205](#)

BIG FRAMEWORK: COLORADO AI LAW

- Deployers of high-risk AI systems must complete **annual impact assessments** for such systems.
- These impact assessments must include the following information:
 - A statement disclosing the purpose(s), intended use cases, deployment context and benefits of the high-risk AI system
 - Analysis of whether deployment of such system poses **any known or reasonably foreseeable risks of algorithmic discrimination**, and if so, details on such discrimination and any mitigations that have been implemented
 - A description of the data categories processed as inputs and the outputs produced
 - Any metrics used to evaluate the performance and known limitations of the high-risk AI system
 - A description of any transparency measures taken with respect to the high-risk AI system, including any measures taken to notify Colorado consumers when the system is being utilized
 - A description of the **post-deployment monitoring and user safeguards**, including oversight, use and learning processes established by the deployer to address any issues

VIRGINIA AI LAW?

- Virginia’s Joint Commission on Technology and Science (JCOTS) established an AI subcommittee that is **currently considering potential AI legislation**.
- Concurrent draft bills – one focused on AI use by public bodies; the other focused on AI use in the private sector.
- **Both Virginia AI bills borrow heavily from Colorado’s AI law:**
 - Similar deployer/developer framework
 - Similar definition for “algorithmic discrimination”
 - Similar definition for “consequential decision” and “substantial factor”
 - Similar definition for “high-risk AI systems”
 - Similar list of exempted technologies
 - AG enforcement authority
 - No private right of action
- If passed in its current form, the bills would go into effect on July 1, 2026.



VIRGINIA DRAFT AI LAW: PUBLIC BODIES

- The draft bill focusing on AI use by public bodies contains the following provisions:
 - New powers and responsibilities for Virginia's Chief Information Officer (CIO), including to develop, publish, and maintain policies and procedures concerning the development, procurement, implementation, utilization, and ongoing assessment of systems that employ high-risk AI systems and are in use by public bodies.
 - A public body procuring any system that employs high-risk AI systems shall **in all future contracts for the procurement of such systems for which negotiation or renegotiation is begun on or after July 1, 2026, include a high-risk artificial intelligence system compliance clause.**



VIRGINIA DRAFT AI LAW: PUBLIC BODIES

- Prior to implementing any system that employs high-risk artificial intelligence systems, the public body shall comply with the impact assessment requirements of § 2.2-5519.
- A public body shall additionally perform **ongoing assessments** of such system after implementation.
- If the public body, or the head of the public body, determines, in its discretion, that such system does not comply with such requirements, the public body shall not implement such system or shall cease to use such system to the extent such system does not comply with such requirements.
- All public bodies that implement high-risk artificial intelligence systems **shall annually report on initial and ongoing system assessments and provide an inventory of such systems used.**



VIRGINIA DRAFT AI LAW: PUBLIC BODIES

- **Big Question:** Would Community Service Boards be subject to the regulations contained in Virginia’s draft AI bill?
- **Answer: Possibly.**
- Under the draft bill, the term “public body” has the same definition as in § 2.2-5514.
 - § 2.2-5514 defines “public body” as any:
 - Legislative body
 - Court of the Commonwealth
 - Authority, board, bureau, commission, district, or agency of the Commonwealth
 - Political subdivision of the Commonwealth, including counties, cities, and towns, city councils, boards of supervisors, school boards, planning commissions, and governing boards of institutions of higher education
 - Other organizations, corporations, or agencies in the Commonwealth supported wholly or principally by public funds



VIRGINIA DRAFT AI LAW: PRIVATE SECTOR

- Mirrors many of the provisions contained in Colorado’s AI law, including:
 - Developer/Deployer framework
 - High-risk AI systems impacting “consequential decisions”
 - Risk assessment requirements
- Notable Distinctions:
 - Virginia’s draft AI bill has a narrower definition of “consumer” which is defined as a natural person who is a resident of the Commonwealth **acting only in an individual or household context**. The bill specifically states that a consumer **does not** include a natural person acting in a commercial or employment context.
 - Virginia’s draft bill **specifically defines what is considered “Artificial Intelligence” and “Generative Artificial Intelligence.”** Colorado does not define either term (only define “Artificial Intelligence System”).
 - Bifurcated legislation between public bodies and the private sector.





Looking Ahead

- **Expect More State-Level AI Laws and Regulations**

- **New York:** NYC's Automated Employment Decision Tool law requires employers using AI as part of their hiring process to perform an **annual audit of their recruitment technology**. These audits must be performed by a third party and check for instances of bias—intentional or otherwise—built into these systems. Failure to comply could lead to civil penalties.
- **Utah:** Under Utah's recently-enacted AI Policy Act, covered companies **must disclose when a consumer is interacting with generative AI**, or materials created by generative AI, at the onset of any communication.
- **California:** The California Privacy Protection Agency released draft automated decision-making technology (ADMT) regulations. The proposed regs would implement consumers' right to opt out of, and access information about, businesses' uses of ADMT, as provided for by the California Consumer Privacy Act (CCPA).





- **Federal AI Law Unlikely**

- Multiple proposals, none expected to pass in 2024.
- Bipartisan group of Senators released a 31-page AI "roadmap" but no legislative language.



- **2026 is a big year for AI regulation.**

- EU AI Act, Colorado's AI law, etc. go into full effect in 2026.
 - Virginia AI law could be on the books
- 
- 





Liz Heddleston

540.983.7741

liz.heddleston@woodsrogers.com



Patrick Austin

804.237.8826

patrick.austin@woodsrogers.com



WoodsRogers