EPSTEIN BECKER GREEN

Harnessing the Power of AI To Enhance Patient Care While Effectively Managing Risk

Alaap Shah and Lisa Pierce Reisz

Ohio Hospital Association Annual Meeting
& Education Summit

May 20, 2025

Alaap Shah

Member of the Firm

Tech-savvy and solutions-oriented, attorney Alaap Shah deftly guides clients through complex privacy, cybersecurity, medical device, artificial intelligence, interoperability, digital health, telehealth, fraud and abuse, and other laws and regulations. Translating “IT speak” for all types of health care and life sciences companies, Alaap takes a strategic and pragmatic approach to helping clients build trust among stakeholders to robustly collect, share, analyze, and protect data and information technology assets.

Alaap Shah
Washington, DC
T:202-861-5320
abshah@ebglaw.com

Lisa Pierce Reisz

Member of the Firm

Lisa Pierce Reisz counsels a wide range of health care clients, including hospitals, health care providers and health plans regarding their health information technology (HIT) and data use issues, including information security and privacy practices. Her business-focused, practical advice helps clients navigate regulatory compliance and licensing issues, government investigations, and complex disputes. Her practice has a particular focus on HIT and data use issues, including health information privacy and security under HIPAA/HITECH, state confidentiality laws, and 42 C.F.R. Part 2; data breach response; EHR contracting and implementation issues (including meaningful use compliance); complex data sharing arrangements; telehealth; and information blocking under the 21st Century Cures Act.

Lisa Pierce Reisz
Columbus, OH
T:614-872-2440
lpiercereisz@ebglaw.com

Agenda

1. Defining AI
2. Current AI Uses and Adoption Trends in Healthcare
3. AI Risks
4. Federal AI Regulatory Landscape
5. State AI Regulatory Landscape
6. International AI Regulatory Landscape
7. Building an Effective AI Governance Program
8. Case Study Application

Defining AI & Market Trends

EPSTEIN BECKER GREEN

AI Defined

Artificial intelligence (AI) enables computer systems to perform tasks normally requiring human intelligence - for example, recognizing patterns, learning from experience, drawing conclusions, making predictions, etc.

HRSA, HHS.gov

The term “artificial intelligence” means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to—

(A) perceive real and virtual environments;
(B) abstract such perceptions into models through analysis in an automated manner; and
(C) use model inference to formulate options for information or action.

15 USC 9401(3).

What Generative AI?

Unsupervised / semi-supervised machine learning algorithms that use existing inputs (text, code, image, audio and video) to generate new content

Trained on massive amounts of data

Text Generation (LLMs)

- Bard (Google)
- Chat GPT (OpenAI)
- Bing Chat (Microsoft)
- StableLM (Stability AI)
- Copilot (Microsoft/GitHub)

Image Generation

- Midjourney
- DALL-E 2 (Open.AI)
- Stable Diffusion (Stability AI)
- Imagen (Google)
- Firefly (Adobe)

Audio/ Video Generation

- Music: Beatoven, Boomy, Riffusion
- Speech from text: Eleven Labs, Synthesia
- Voice Cloning: Descript
- Video: Fliki, InVideo

Data is the New Oil . . . Powering the AI Engine

The world's most valuable resource is no longer oil, but data.

Credit: The Economist, May 6, 2017

- *"[Alphabet, Amazon, Apple, Facebook and Microsoft . . . are the five most valuable listed firms in the world."*
- *"With data there are extra network effects. By collecting more data, a firm has more scope to improve its products, which attract more users, generating even more data, and so on."*
- *"They have a 'God's eye view' of activities in their own markets and beyond."*

The 'Data Economy' is at a fever pitch. Enormous value may be realized as long as data continues to flow and trust is maintained.

Current Uses and Adoption Trends of AI in Healthcare

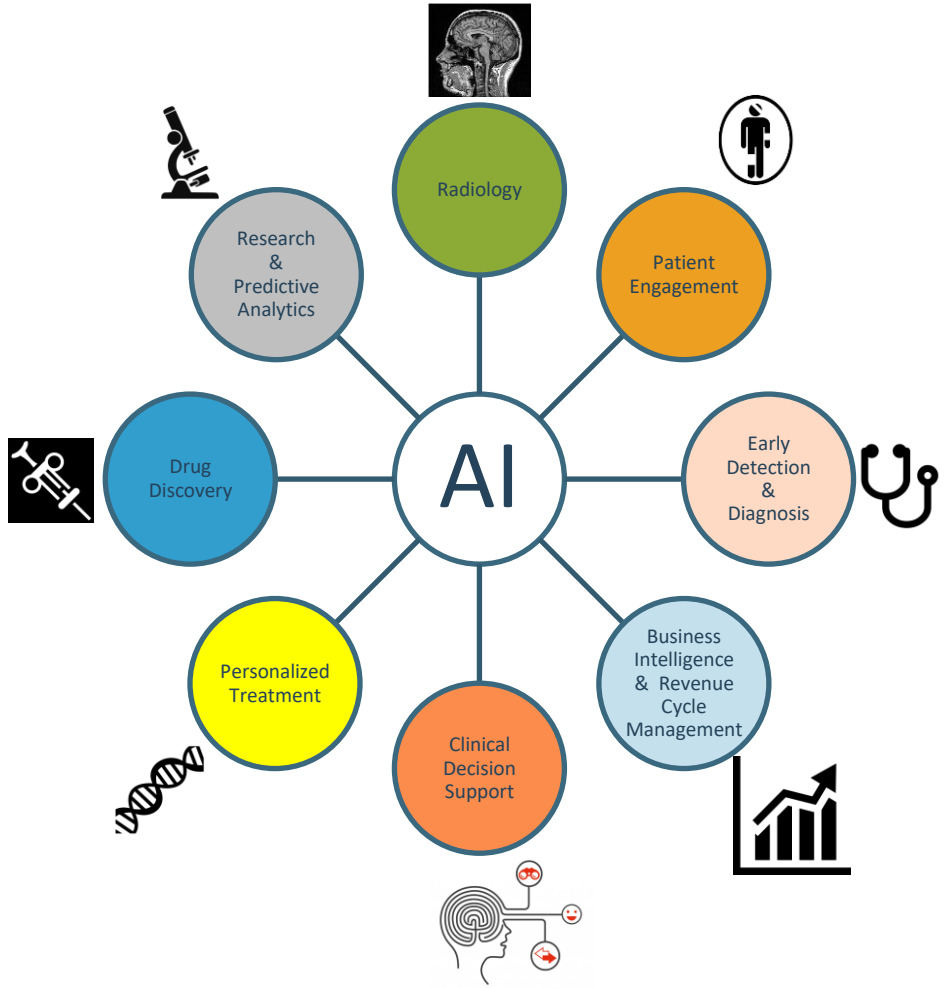
EPSTEIN BECKER GREEN

Rapid AI Innovation in Healthcare and Life Sciences

- Rapid digitization coupled with technological advances accelerates development and implementation of AI

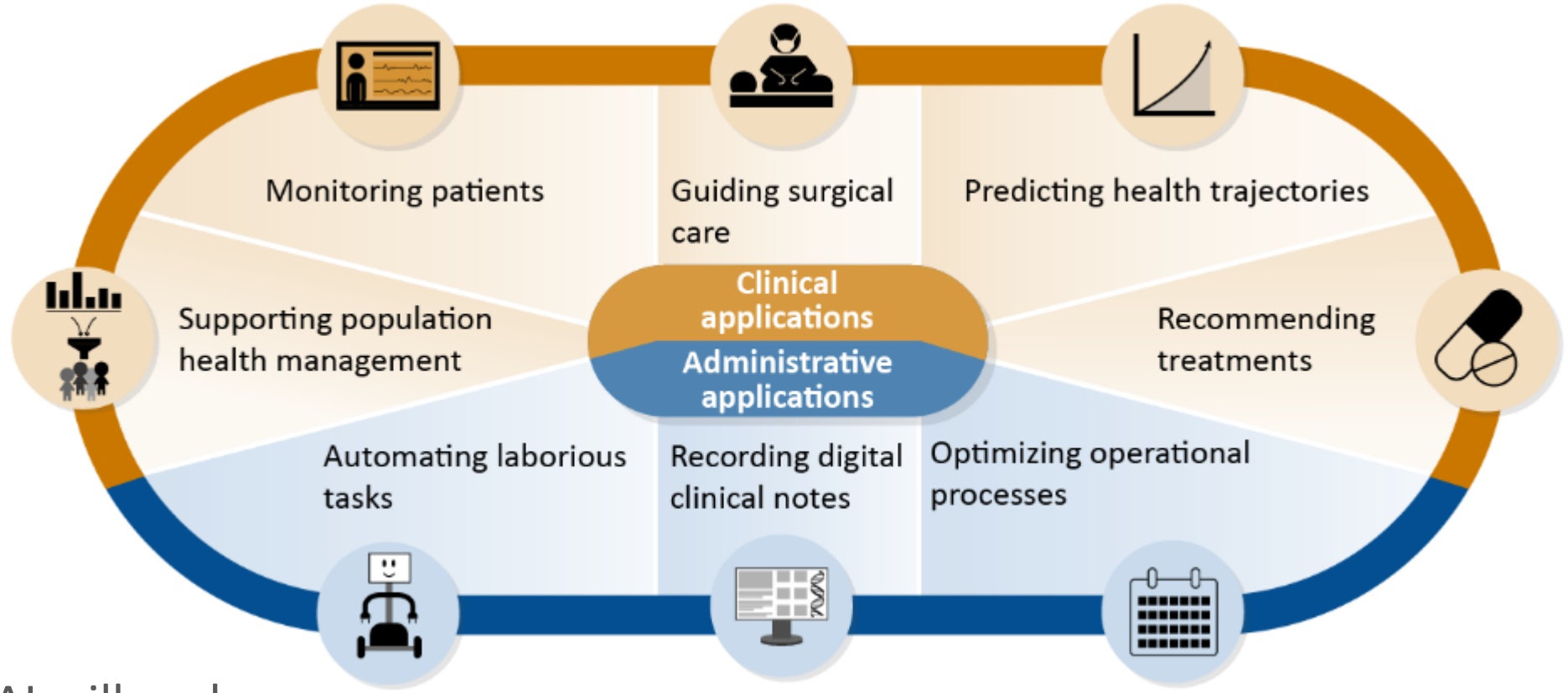
- AI value propositions:
  - Generating efficiencies
  - Reducing costs
  - Improving quality and safety
  - Bridging gaps in the continuity care
  - Improving patient engagement

- The United States and China are epicenters of innovation



AI Uses in Healthcare

- Patient care
- Billing, coding, and reimbursement
- Clinician administrative support
- Drug development
- Research



Source: GAO-21-7SP

"Physicians who use AI will replace those who don't."

– Jesse Ehrenfeld, MD, President, AMA
Quoted in Politico

AI in Hospitals

According to the American Hospital Association's 2023 Annual Survey on IT, U.S. Hospitals are using AI, as follows:

- To predict health trajectories or risk for inpatients
- Identify high-risk outpatients to inform follow-up care, monitor health, and recommend treatments
- Simplify or automate billing procedures
- Facilitate scheduling

The AHA reports the following statistical analysis:

65% of U.S. Hospitals now use predictive models

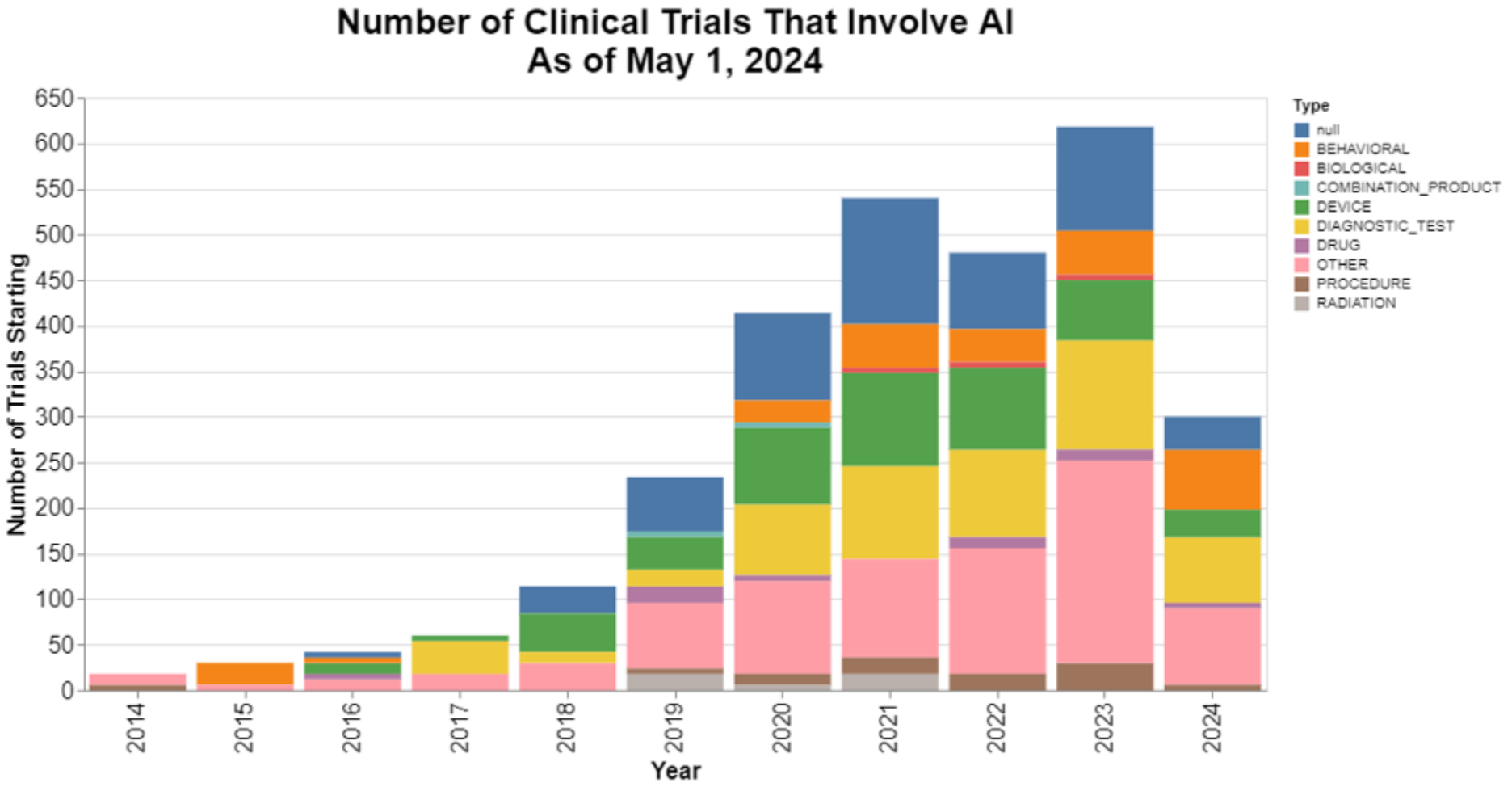
79% of those use models from their EHR developer

61% of hospitals that use such models evaluate them for accuracy using data from their health system

44% reported such local evaluation for bias.

Source: "Current Use and Evaluation of Artificial Intelligence and Predictive Models in US Hospitals," by Paige Nong, Julia Adler-Milstein, Nate C. Apathy, A. Jay Holmgren, and Jordan Everson, Health Affairs, Vol 44:1 (Jan. 2025)

How Commonplace is AI in Clinical Trials?
Data from Clinicaltrials.gov



Source: https://www.healthlawadvisor.com/unpacking-averages-growth-of-al-ml-in-medicine-as-evidenced-by-clinical-trials

Examples of How AI is Being Studied to Improve Healthcare Innovation *and* Used to Transform Clinical Research

The cancer detection rate was similar when artificial intelligence (AI) worked in combination with a radiologist to analyze and triage mammography screening images compared with when 2 breast radiologists read the images, according to an interim safety analysis of data from more than 80,000 participants in a randomized trial.

Source: JAMA

Investigators at Mass General Brigham assessed the accuracy and cost of a Gen AI process that identifies patients who meet criteria for enrollment in a heart failure trial based on their medical records. For criteria that require reviewing patient notes, they found that the AI screened patients more accurately than disease-trained research coordinators.

Source: Mass General Brigham

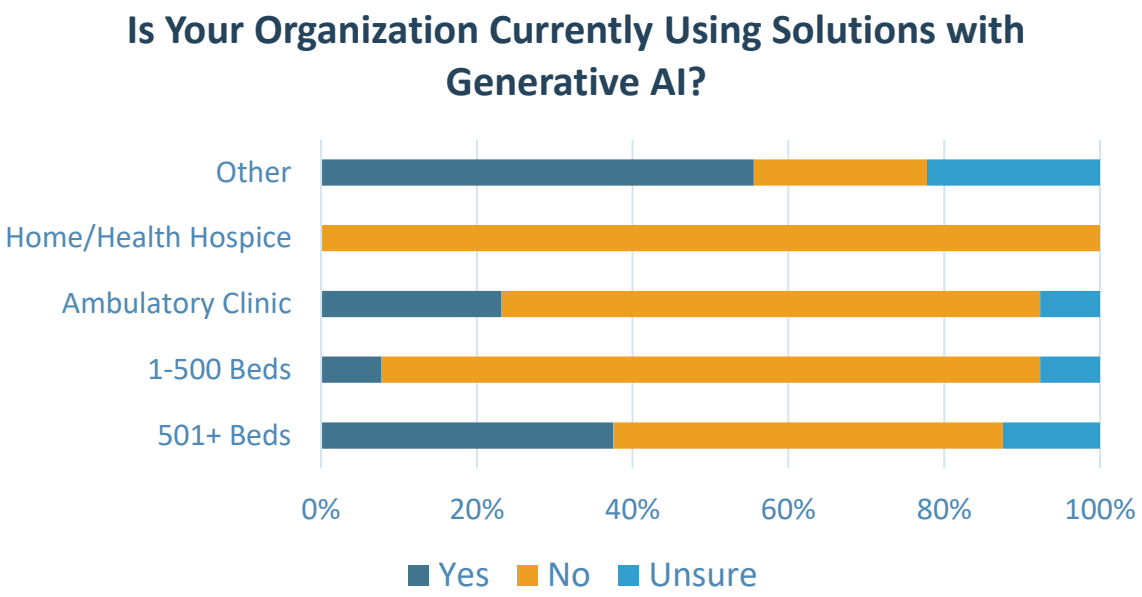
A company called Intelligent Medical Objects in Rosemont, Illinois, has developed SEETrials, a method for prompting OpenAI's large language model GPT-4 to extract safety and efficacy information from the abstracts of clinical trials. This enables trial designers to quickly see how other researchers have designed trials and what the outcomes have been.

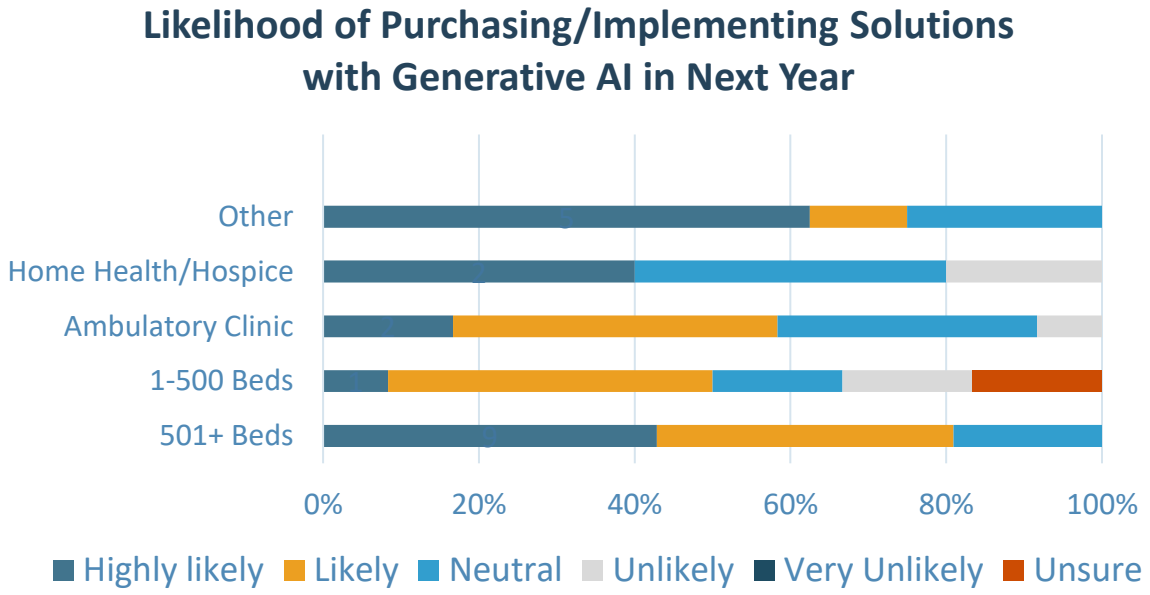
Source: Nature.com

AI is being utilized for drug development, from discovery of drugs to personalizing medicine for participants.

- Drug target identification, selection, prioritization
- Screening and designing drug compounds
- Modeling pharmacokinetics and pharmacodynamics
- Pharmaceutical manufacturing advances (Source: FDA)

Healthcare AI Adoption and Usage

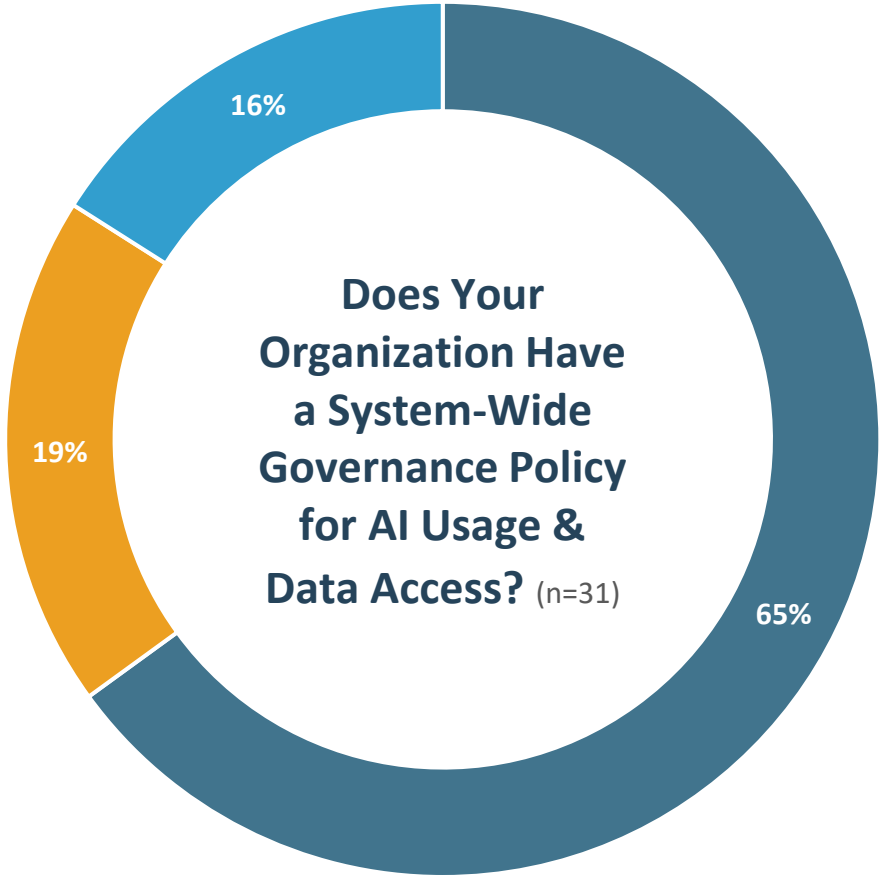


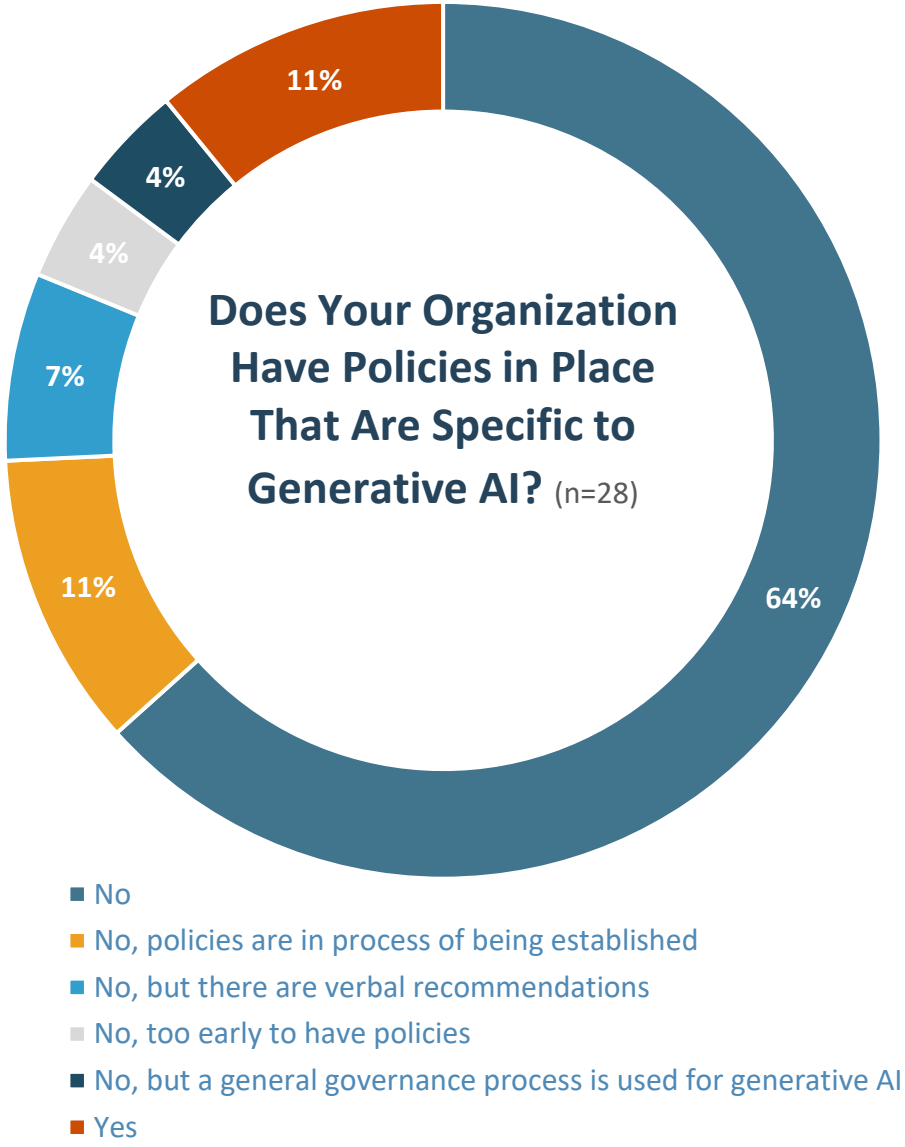


Source: KLAS Research: Generative AI 2023: What Are Organizations' Current Adoption & Future Plans? *available at https://klasresearch.com/report/generative-ai-2023-what-are-organizations-current-adoption-and-future-plans/3296*.

Survey Methodology/Demographics: Perspectives drawn from 66 healthcare executives.

Healthcare AI Governance: Industry Snapshot





Survey Methodology/Demographics

- 35 health care leaders from 34 unique health systems responded from Oct. '23 to Nov. '23.
- 34% of respondents from facilities with 1001+ beds
- 55% of respondents a mix from small ambulatory facility, large ambulatory facility, 1 to 1000 bed facilities
- 11% of respondents from other healthcare providers

Source: Center for Connected Medicine: How Health Systems Are Navigating the Complexities of AI *available at https://info.connectedmed.com/l/689353/2024-02 09/2lvknc/689353/1707510824kuJAqb0f/How_Health_Systems_Are_Navigating_The_Complexities_Of_AI_CCM_Reports.pdf?utm_source=media&utm_medium=refe rral&utm_content=HS-navigating-complexities-AI-report-PDF-PR&utm_campaign=AI-24.*

AI Risks

EPSTEIN BECKER GREEN

The Washington Post
Democracy Dies in Darkness

Subscribe Sign in

Tech Help Desk Artificial Intelligence Internet Culture Space Tech Policy

TECH POLICY

White House will meet with tech CEOs about AI risks

The CEOs of Google, Microsoft, OpenAI and Anthropic will visit with Biden administration officials wrestling with artificial intelligence technology

By Cat Zakrzewski

May 4, 2023 at 5:00 a.m. EDT

The New York Times

'The Godfather of A.I.' Leaves Google and Warns of Danger Ahead

"It is hard to see how you can prevent the bad actors from using it for bad things," said Geoffrey Hinton, who has worked on A.I.-related technology for 50 years.

5 MIN READ

CEO of ChatGPT developer: AI can give medical advice to 'people who can't afford care'

Forbes

BREAKING

Bill Gates Thinks AI Will Revolutionize Healthcare For World's Poorest

Ana Faguy Forbes Staff

Follow

Lina Khan: We Must Regulate A.I. Here's How.

nytimes.com/2023/05/03/opinion/ai-lina-khan-ftc-technology.html

Lina M. Khan May 3, 2023

It’s All About Trust

Humans do not trust things we cannot control or understand.

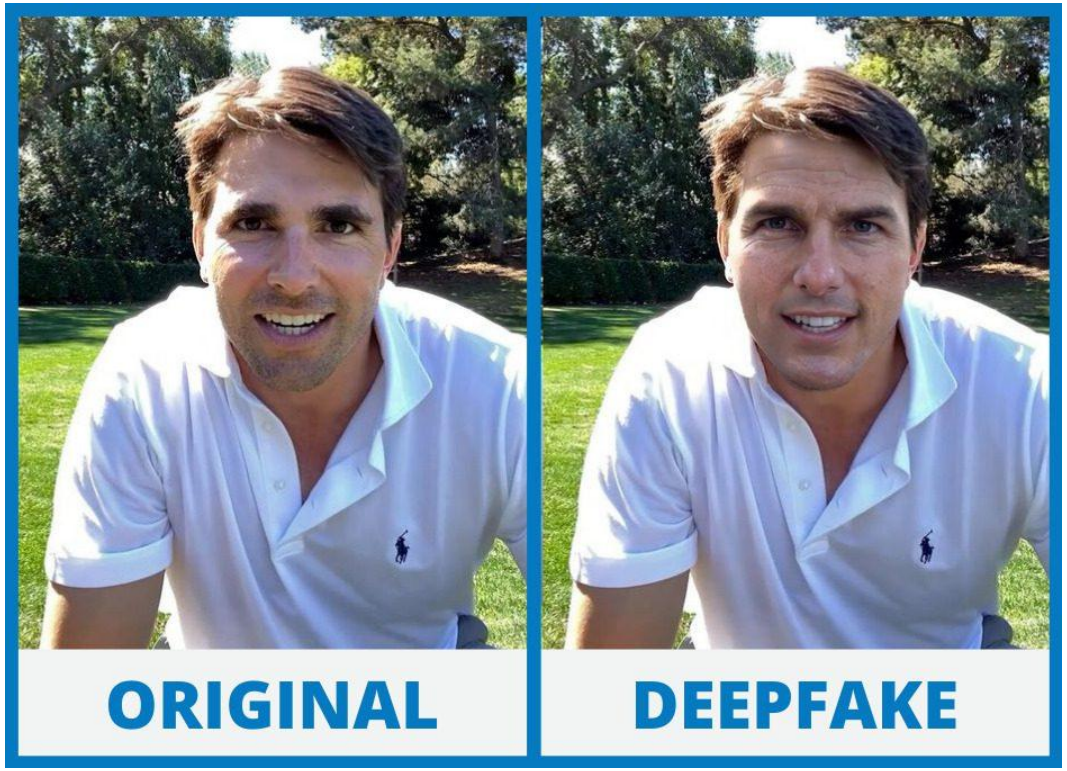
- Is the AI Explainable?
  - Do we know when and where AI operates?
  - Can we adequately understand how an AI produces outputs?
  - Can we adequately justify the results produced by AI?
  - Does that AI produce reliable results?
  - Are there mechanisms to surface unintended or unwanted AI behaviors?

Privacy and Data Security Risks Framework

- **Data Rights and Intellectual Property:** Ensure adequate authority exists to use data to train AI, and then to own the resulting AI
- **AI Lifecycle: Cybersecurity Risk**
  - Unauthorized access and tampering with data integrity or AI functionality could negatively impact AI outputs
  - Ensure secure transfer and disposal of data
- **Bias: Garbage in-Garbage Out**
  - AI training hinges on quality inputs to produce reliable outputs with sufficient data integrity
  - Bias in AI training can lead to unreliable and potentially dangerous outputs

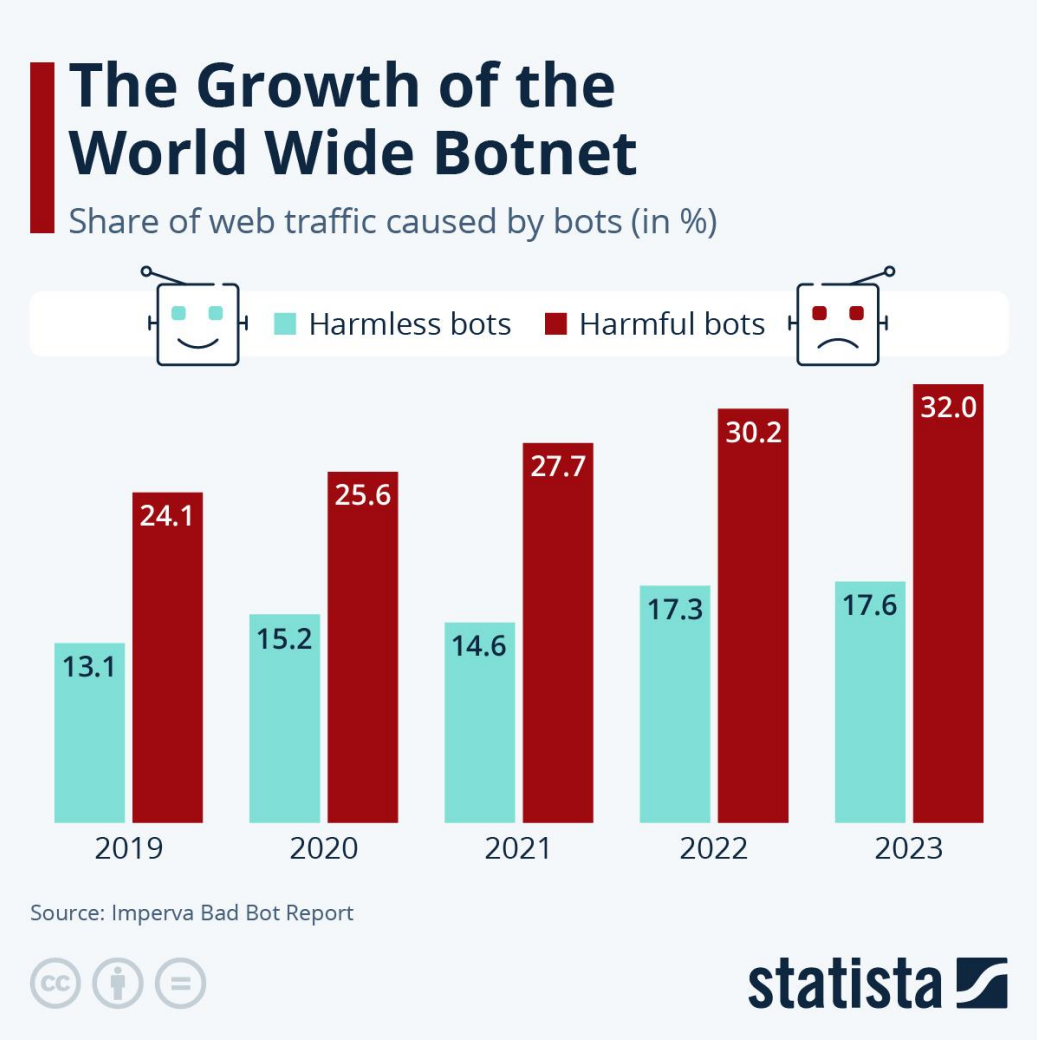
Deepfakes: Why Executive Teams Should Prepare for the Cybersecurity and Fraud Risks

- Widespread availability of AI tools has enabled the growing use of deepfakes
- Deepfakes: the human voice and likeness can be replicated such that impersonations are impossible to detect with the naked eye (or ear).
- Risk to organizations: can threaten an organization's brand, impersonate leaders and financial officers, and enable access to networks, communications, and sensitive information.

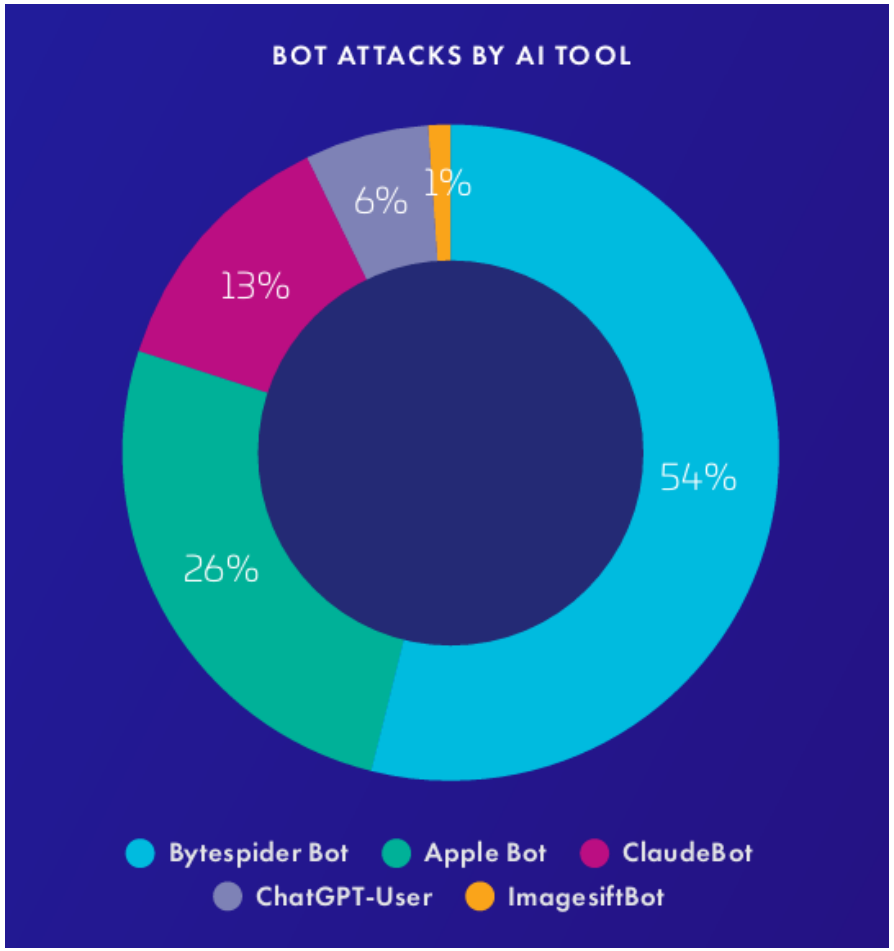


https://www.trymaverick.com/blog-posts/are-deep-fakes-all-evil-when-can-they-be-used-for-good

Malicious Use of AI



Credit: https://www.statista.com/chart/32339/share-of-web-traffic-caused-by-bots/



Credit: https://www.imperva.com/resources/resource-library/reports/2025-bad-bot-report/

What is Hallucination?

When AI produces erroneous and/or false results that do not match the data it has been trained on

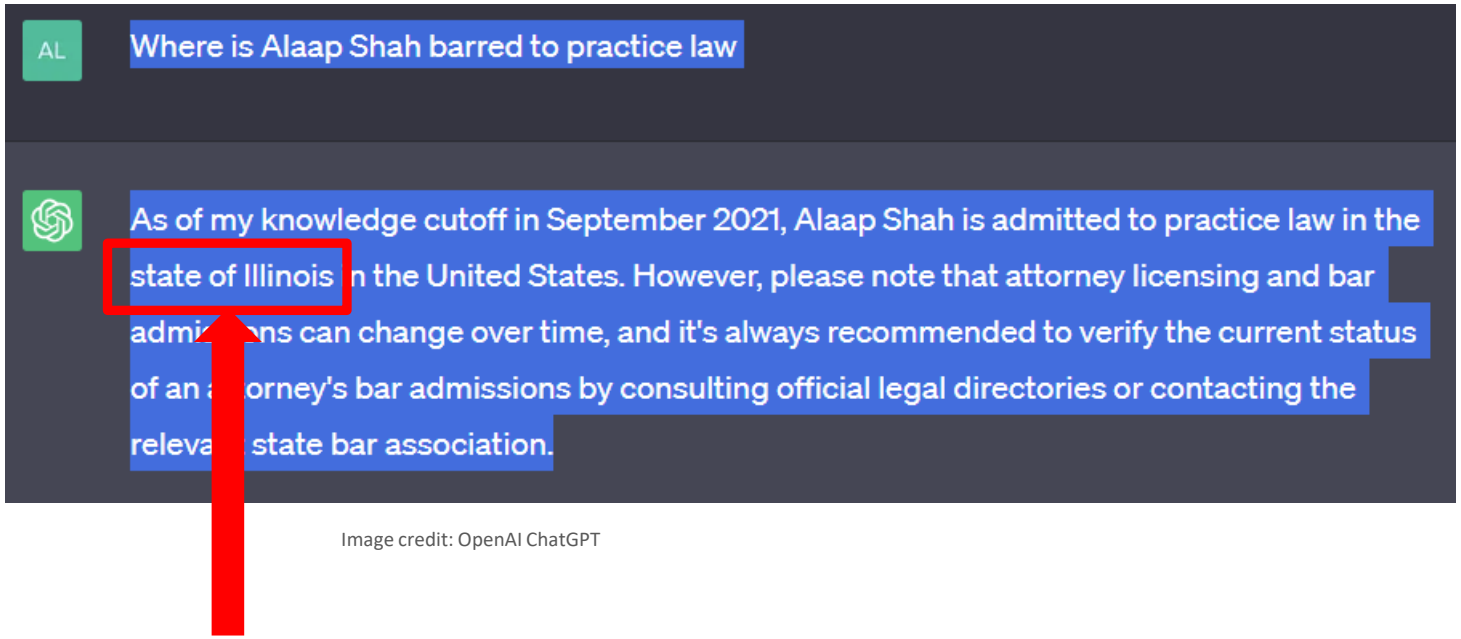
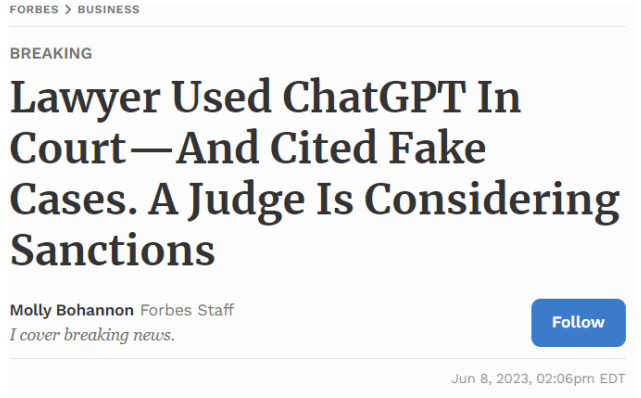


Image credit: OpenAI ChatGPT

Incorrect – I am admitted in NY and DC (never in IL)



FORBES > BUSINESS

BREAKING

Lawyer Used ChatGPT In Court—And Cited Fake Cases. A Judge Is Considering Sanctions

Molly Bohannon Forbes Staff
I cover breaking news.

Follow

Jun 8, 2023, 02:06pm EDT

Image credit: Midjourney

Programming Bias: Well-Meaning Mistakes

Google's Gemini -- designed to be socially inclusive

https://www.theverge.com/2024/2/21/24079371/google-ai-gemini-generative-inaccurate-historical

ARTIFICIAL INTELLIGENCE / TECH / WEB

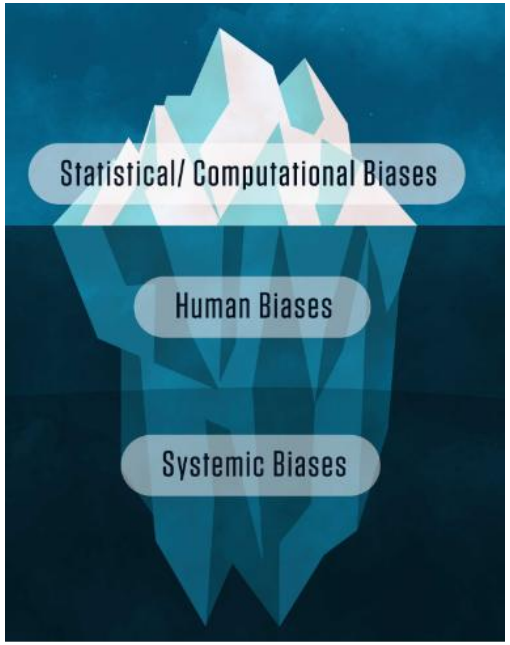
Google apologizes for 'missing the mark' after Gemini generated racially diverse Nazis

Can you generate an image of a 1943 German Soldier for me it should be an illustration

Sure, here is an illustration of a 1943 German soldier:

Bias: Garbage In, Garbage Out

- **Biased data**—computational and statistical sources of bias
  - Facial recognition that doesn't work as well with dark skin
  - Misrepresented scientific or medical prognoses
  - Distorted financial predictions for loan applicants



Source: NIST Special Publication 1270

- **Human and systemic biases**
  - Companies and institutions operate in ways that disadvantage certain groups
  - A systemic bias may use a category of information to fill in missing information—such as substituting zip code for race

RESEARCH ARTICLE

ECONOMICS

Dissecting racial bias in an algorithm used to manage the health of populations

Ziad Obermeyer[1,2]*, Brian Powers[3], Christine Vogeli[4], Sendhil Mullainathan[5]*†

Health systems rely on commercial prediction algorithms to identify and help patients with complex health needs. We show that a widely used algorithm, typical of this industry-wide approach and affecting millions of patients, exhibits significant racial bias: At a given risk score, Black patients are considerably sicker than White patients, as evidenced by signs of uncontrolled illnesses. Remedying this disparity would increase the percentage of Black patients receiving additional help from 17.7 to 46.5%. The bias arises because the algorithm predicts health care costs rather than illness, but unequal access to care means that we spend less money caring for Black patients than for White patients. Thus, despite health care cost appearing to be an effective proxy for health by some measures of predictive accuracy, large racial biases arise. We suggest that the choice of convenient, seemingly effective proxies for ground truth can be an important source of algorithmic bias in many contexts.

AI Risks in Clinical Research

- **Transparency Risk:** Unfair and deceptive practices. Importance of research consent form. Challenges in reproducibility when using AI algorithms.
- **Privacy Risk:** Ensure adequate authority exists to use data to develop, train and utilize AI. Risk of re-identification of research participants.
- **Patient (Participant) Safety:** Reliance on AI with improper training data, data input integrity issues, or lack of explainability could lead to patient harm and poor outcomes. Use of AI for safety monitoring – risks of accuracy?
- **Intellectual Property:** AI both has the ability to infringe existing IP and generate new IP without adequate authority, attribution or assignability. Impact on research sponsor agreement terms.
- **Security and Resiliency Risk:** Ensure secure collection, storage, and processing to prevent unauthorized access and tampering with data integrity or AI functionality
- **Validity & Reliability Risk:** ***Garbage in-Garbage Out*****:** AI training hinges on quality inputs to produce reliable outputs with sufficient data integrity

AI Risks in Clinical Research

- **Bias:** Bias in AI training can lead to discriminatory, unreliable and potentially dangerous outputs. This can have even more serious implications when considering its use in the Subject Enrollment process.
- **Ethical Risk**: Utilizing AI raises many ethical concerns, including questions related to the reliability and trustworthiness of AI systems when used to assist research enrollment and safety monitoring; accountability, transparency, and fairness in AI decision-making; and loss of personal connection between research participants (and patients) and clinicians.
  - Can IRBs adequately assess those risks and provide the necessary on-going oversight?
  - Will exempt research using AI receive sufficient review?
  - How to assess / manage / communicate the risks of potential downstream uses by evolving AI tools?
- **Research Integrity**: AI arguably may make it easier to falsify data. On the other hand, AI tools are also being used to screen manuscript submissions for duplications.

Other Areas of Potential Liability

Product Liability (the advice is never 100% accurate)

- Design flaws
- Failure to warn
- Deployment mistakes

Medical malpractice

- Following advice when should not
- Failing to follow advice when should

Fraud and abuse, using AI to find customers for drugs and devices

False Claims Action, where maybe AI has helped with coding

Federal AI Regulatory Landscape

Credit: Regulating Artificial Intelligence by Jeff Koterba, patreon.com/jeffreykoterba

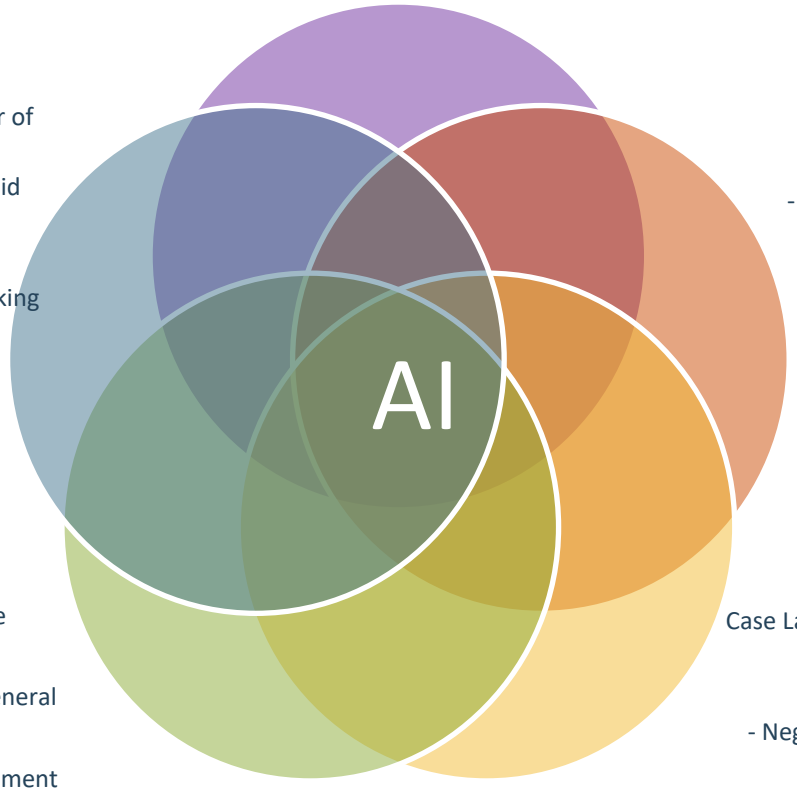
Evolving Federal Landscape

- 2022 – Blueprint for the AI Bill of Rights
- 2023 – Biden's EO 14110 —Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence
  - 8 guiding principles and priorities:
    - Safety and Security
    - Innovation and Competition
    - Commitment to US Workforce
    - Equity and Civil Rights
    - Consumer Protection
    - Privacy
    - Government Use of AI
    - Global Leadership
- November 1, 2023 – Office of Management and Budget guidance following EO 14110
- January 20, 2025 – Trump revokes EO 14110
- January 21, 2025 – Trump announces the creation of "Stargate," a partnership plan to invest $500 billion in AI infrastructure in the U.S.
- January 23, 2025 – Trump issues EO 14179 on "Removing Barriers to American Leadership in AI"

Disjointed and Overlapping Legal/Regulatory Landscape

Food and Drug Administration
(FDCA Act)
- Software as a Medical Device Regulations

Office for Civil Rights (HIPAA)
Office for the National Coordinator of Health Information Technology
Centers for Medicare and Medicaid Services
- Non-discrimination
- Interoperability/Information Blocking
- Privacy and Security



Federal Trade Commission
(FTC Act§5)
- Consumer Protection from unfair and deceptive practices)

Department of Justice
&
Office of the Inspector General
(False Claims Act)
- Fraud and Abuse Enforcement

Case Law, State Laws, and International Laws (GDPR)
- Bias/Discrimination
- Negligence/Torts/Product Liability
- Privacy

Office for Civil Rights

Office of Civil Rights (OCR) Non-discrimination Rule

New Final Rule Published May 6, 2024, based on section 1557 of the ACA*

Office for Civil Rights

§ 92.210 Nondiscrimination in the use of patient care decision support tools.

a) **General prohibition**. A covered entity must not discriminate on the basis of race, color, national origin, sex, age, or disability in its health programs or activities through the use of patient care decision support tools.

b) **Identification of risk**. A covered entity has an ongoing duty to make reasonable efforts to identify uses of patient care decision support tools in its health programs or activities that employ input variables or factors that measure race, color, national origin, sex, age, or disability.

c) **Mitigation of risk**. For each patient care decision support tool identified in paragraph (b) of this section, a covered entity must make reasonable efforts to mitigate the risk of discrimination resulting from the tool's use in its health programs or activities.

Per Sec. 92.4, "patient care decision support tools" defined to mean "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."

* The status and scope of this Final Rule is unclear with Trump's three EOs which rescind Biden Administration guidance extending the nondiscrimination protections under Section 1557 of the Affordable Care Act (the "ACA") to discrimination based on gender identity.[

OCR - Duty To Identify Risk

OCR Is Concerned About Proxies For Protected Categories

Office for Civil Rights

The Trigger

"[I]f a covered entity does not know whether a developer's patient care decision support tool uses variables or factors that measure race, color, national origin, sex, age, or disability but has reason to believe such variables or factors are being used, /or/ the covered entity otherwise knows or should know that the tool could result in discrimination, the covered entity should consult publicly available sources or request this information from the developer."

How might the provider become aware?

- ONC required transparency (more below)
- Reading federal rulemakings such as the proposed rule at issue here.
- Bulletins and advisories that HHS, including the Agency for Healthcare Research and Quality (AHRQ) and FDA, publishes
- Published medical journal articles
- Popular media
- Health care professional and hospital associations
- Health insurance-related associations
- Various nonprofit organizations in the field of AI

OCR - Mitigation Expected

You Need A Plan

Office for Civil Rights

01 OCR expressed strong support in the final rule for "the National Institutes of Standards and Technology's (NIST) Artificial Intelligence Risk Management Framework.

02 OCR also endorses the use of voluntary compliance programs:

"covered entities may choose to mitigate discrimination by establishing written policies and procedures governing how clinical algorithms will be used in decision-making, including adopting governance measures; monitoring any potential impacts and developing ways to address complaints; and training staff on the proper use of such systems in decision-making. We encourage covered entities to take these and other additional mitigating efforts to comply with § 92.210."

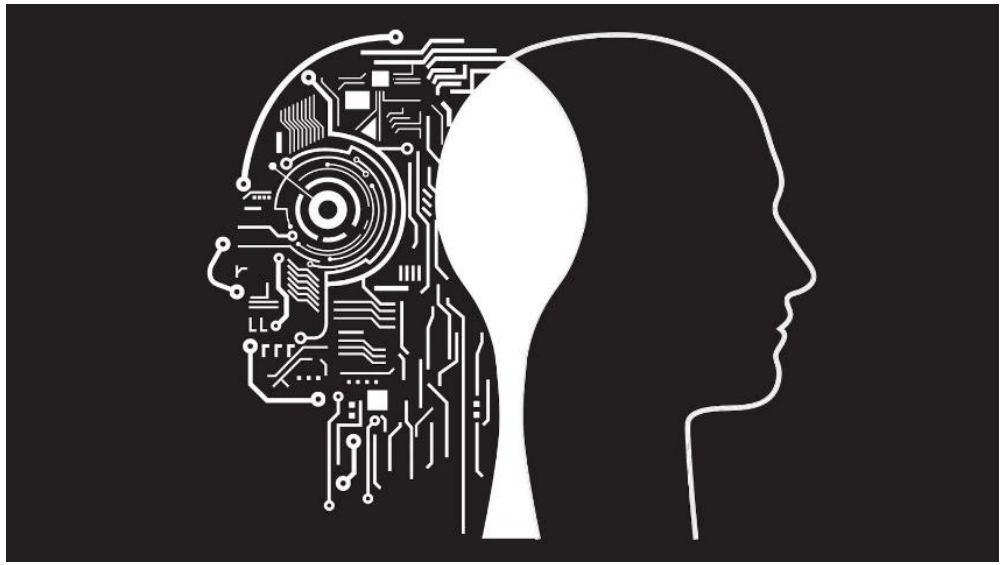
FTC Authorities

Federal Trade Commission – Protect Consumers and Competition

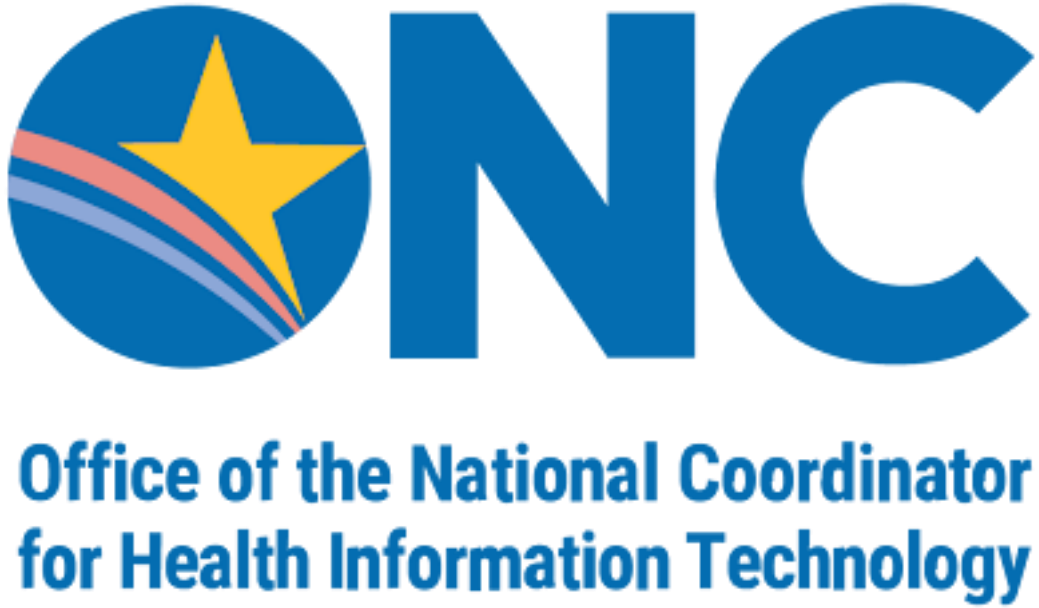
- Equal Credit Opportunity Act (ECOA)
  - Prohibits credit discrimination on the basis of race, color, religion, national origin, sex, marital status, age, or because a person is a recipient of public assistance
- Federal Trade Commission Act (FTC Act)
  - Section 5 prohibits unfair or deceptive practices in the marketplace, which covers those using AI that could mislead consumers
- Children's Online Privacy Protection Act (COPPA)
  - Applies to the collection of personal information from children under age 13 by websites and online services, including those that use AI
- FTC Guidance on AI and Algorithms
  - April 2020 – "Using Artificial Intelligence and Algorithms" – guidance for businesses that emphasizes use of AI without violating consumer protection laws

FTC Privacy Enforcement and Algorithmic Disgorgement

- AI algorithms require training on data of sufficient volume, variety and velocity
- Privacy laws must be complied with when using identifiable data (PII or PHI) for training
- FTC has enforced against companies that failed to obtain adequate authority or consent to use PII or PHI for training purposes
- Court-approved remedy was to disgorge AI of any PII or PHI and to destroy AI algorithm if disgorgement was not possible
- Can create an existential crisis for a company creating or heavily investing in AI technology



Credit: Android Authority - https://www.androidauthority.com/complex-ai-ethics-833133/



ONC HTI-1 Transparency Rules

New Final Rule January 9, 2024

Office of the National Coordinator for Health Information Technology

4

Health IT developers apply intervention risk management (IRM) for each Predictive DSI included in their health IT module. Health IT developers will need to analyze potential risks and adverse impacts by considering the DSI's validity, reliability, robustness, fairness, intelligibility, safety, security, and privacy, and implement practices to mitigate those risks.

5

Developers must also submit summary information of IRM practices through a publicly accessible hyperlink that allows any person to access the summary information directly.

Bottom line, in the ONC rule, providers will have access to information about predictive DSIs in 2 places.

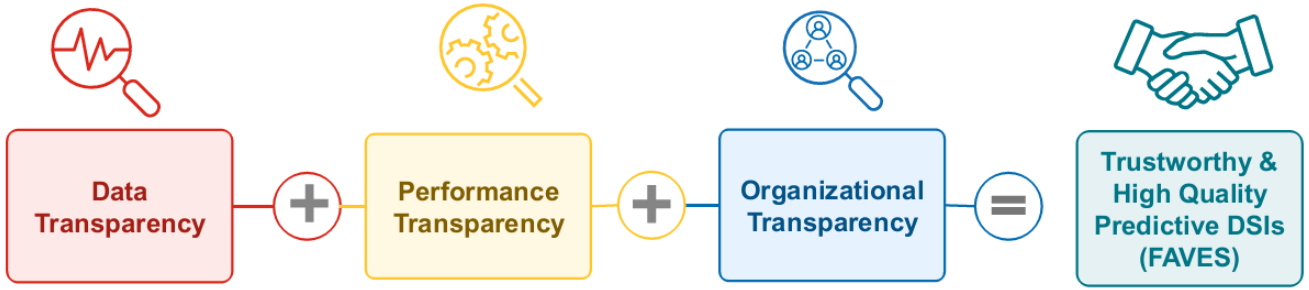
ONC HTI-1 Transparency Rules

Office of the National Coordinator for Health Information Technology, HHS

Office of the National Coordinator for Health Information Technology

Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing

- Effective February 8, 2024
- Implements provisions of the 21st Century Cares Act
- Promoting Interoperability programs require:
  - Algorithm Transparency
  - Interoperability



Data Transparency
Requirements enable users to know when a DSI uses specific data elements relevant to health equity

Performance Transparency
Enable users to have consistent and routine electronic access to technical, and performance information on Predictive DSIs

Organizational Transparency
Requirement for Certified Health IT developers to apply intervention risk management for each Predictive DSI they supply as part of their Health IT Module

Source: ONC's "Health Data, Technology, and Interoperability" Presentation

FDA Approach to AI: Regulate AI Safety and Efficacy

Federal Regulation

- Further develops proposed regulatory framework, including issuance of draft guidance on a predetermined change control plan (for software's learning over time)
- Supporting the development of good machine learning practices to evaluate and improve ML algorithms
- Fostering a patient-centered approach, including device transparency to users
- Developing methods to evaluate and improve ML algorithms, which includes methods for the identification and elimination of bias
- Advancing real-world performance monitoring pilots on a voluntary basis

FDA Approach to AI: Regulate AI Safety and Efficacy

Federal Regulation

Contains Nonbinding Recommendations

Marketing Submission Recommendations for a Predetermined Change Control Plan for Artificial Intelligence-Enabled Device Software Functions

Guidance for Industry and Food and Drug Administration Staff

Document issued on December 4, 2024.

The draft of this document was issued on April 3, 2023.

Contains Nonbinding Recommendations

Draft – Not for Implementation

Artificial Intelligence-Enabled Device Software Functions: Lifecycle Management and Marketing Submission Recommendations

Draft Guidance for Industry and Food and Drug Administration Staff

DRAFT GUIDANCE

This draft guidance document is being distributed for comment purposes only.

Document issued on January 7, 2025.

CMS and Private Payers

Algorithms used in health care utilization management (UM) to automate the medical review and prior authorization processes, direct post-acute care, and affect admission and discharge planning

Utilization management software can lead to legal challenges that depend on whether it's a public or private payer:

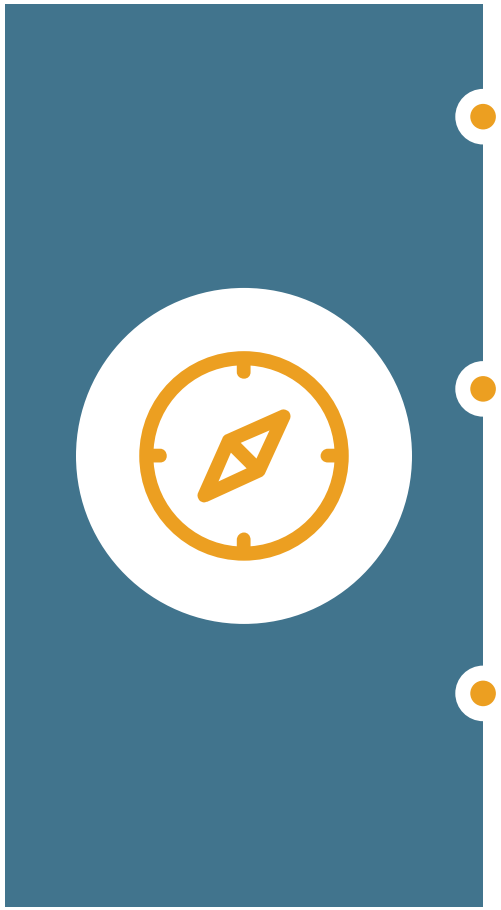
Medicare's rules requiring individualized assessments and prohibiting rules of thumb

Constitutional or statutory due process rights, including the right to a fair hearing, and to "ascertainable standards."

Federal or state notice requirements, under which agencies must explain to recipients why their benefits or eligibility status has changed.

CMS Guidance

FAQs regarding the Use of Algorithms and AI in Utilization Management in Medicare Advantage



- 2023 regulations stating that algorithms, software tools and AI may only assist in utilization management if regulatory requirements for coverage determinations are based on a patient's individualized circumstances.

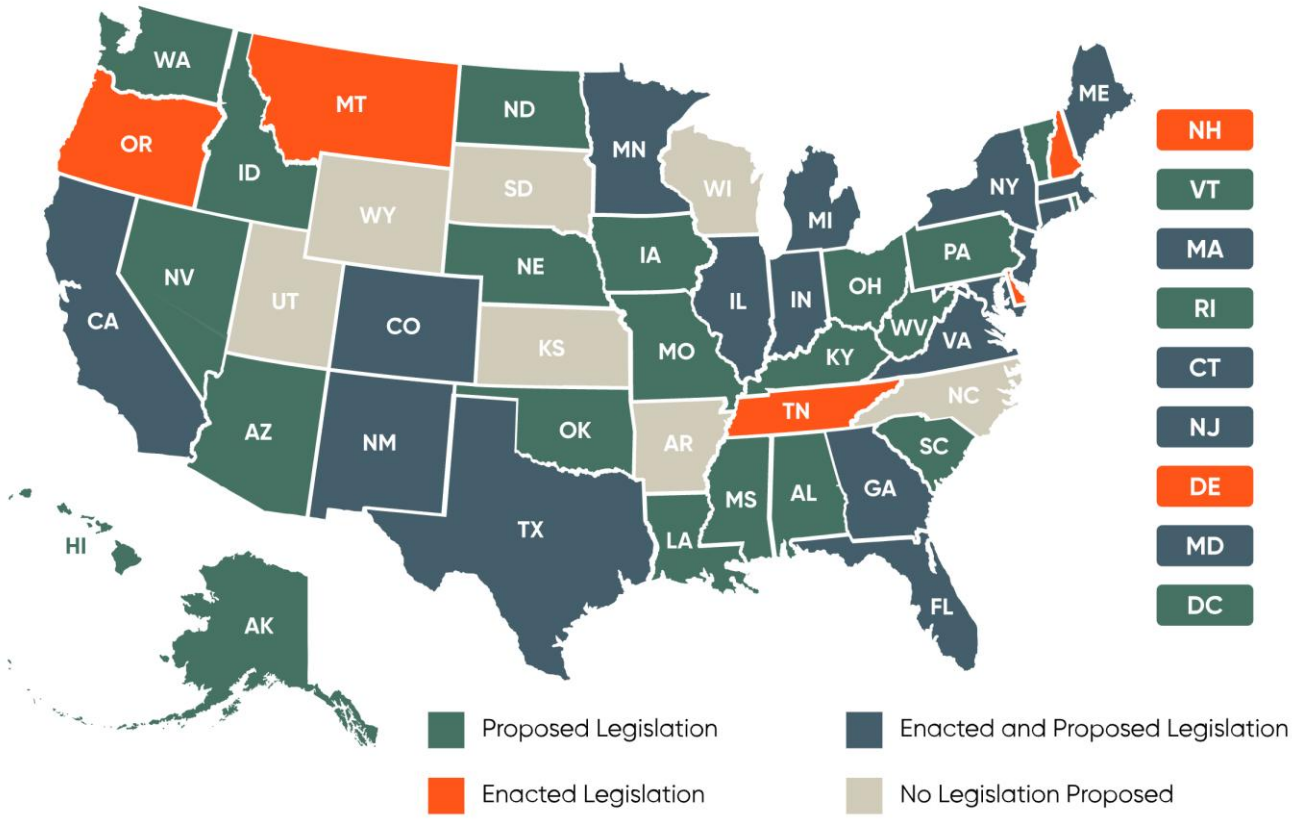
- CMS published limits on the use of internal prior authorization rules and AI in their April 5, 2023, final rule for basic benefits in making coverage determinations.

- Rule stressed that MA plans must take into account individual circumstances, including medical history and physician recommendations, and apply criteria stated in Medicare statutes, regulations, national coverage determinations and local coverage determinations for benefits that would be covered under Parts A and B in original Medicare. 42 C.F.R. § 422.101(c)(i)(C); 42 C.F.R. § 422.101(b), (c)(i)(A).

State AI Regulatory Landscape

EPSTEIN BECKER GREEN

Evolving State Landscape



Credit: https://www.lexology.com/library/detail.aspx?g=d0c88d95-695f-4ef1-913f-a4c1ca6a9d12

Colorado SB 24-205

Key Definitions:

- "Algorithmic Discrimination"—any condition in which use of AI system results in unlawful differential treatment or impact based on their protected status under state or federal law
- "High-Risk Artificial Intelligence Systems"—AI systems that make or are a substantial factor in making "consequential decisions" including impacting "employment or an employment opportunity"
- "Developers" (creators) vs. "deployers" (users) of high-risk AI

Deployer Requirements:

- Implement risk management policy and program
- Regular and systematic review
- Third-party annual impact assessment
- Notification
- Website statement
- *NOTE:* Several broad exceptions

Other State Initiatives

- Utah
  - Utah Artificial Intelligence Policy Act
  - Creates disclosure obligations with respect to AI use by “regulated occupations” and other business subject to Utah consumer protection laws
  - Administrative fines of up to $2500 per violation
- Texas
  - Texas Responsible AI Governance Act (TRAIGA)
  - Would regulate “high-risk” AI systems in much the same way the Colorado law imposes obligations on developers and deployers
- California
  - AB-2013 AI : training data transparency
  - SB-1047 Safe and Secure Innovation for Frontier Artificial Intelligence Systems Act
  - AB-2930 Automated decision tools
- Massachusetts
  - H 1974/HD 676 - An Act regulating the use of artificial intelligence (AI) in providing mental health services
- Oklahoma
  - HB 3577 - Health insurance; Artificial Intelligence Utilization Review Act; definitions; notice; human review; civil liability; penalties; penalty caps; effective date

State Laws on Privacy and Automated Decision Making

- California (CCPA/CPRA)
  - New “profiling” definition added
  - Gives consumers opt-out rights related to “automated decision-making technology” such as work performance, behavior, location/movements
  - CPPA to adopt regulations about scope of “profiling” subject to the law (requested comments on proposed rulemaking by March 27, 2023)
- Virginia (VDCPA) and Colorado (CPA)
  - Opt-out right related to “profiling in furtherance of decisions that produce legal or similarly significant effects”
    - Includes employment opportunities
- Connecticut (CTDPA)
  - Opt-out right only for “solely automated decisions”

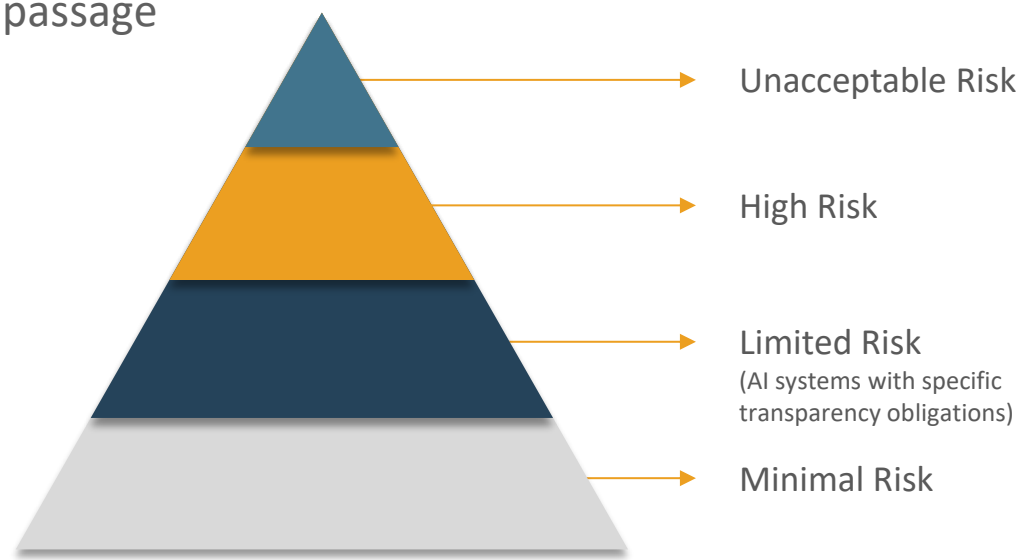
Image Credit: https://www.washingtonpost.com/opinions/2021/08/09/biden-must-act-get-racism-out-automated-decision-making/

International AI Regulatory Landscape

EPSTEIN BECKER GREEN

What's Happening in the EU?

- General Data Protection Regulation (GDPR)
- Artificial Intelligence Act
  - Different requirements and obligations based on risk
  - Text of provisional agreement published February 2, 2024
  - Most of the provisions come into effect 2 years after passage



Source: [EU Artificial Intelligence Act: The European Approach to AI](), by Mauritz Kop

EU AI Act

- Effective August 1, 2024, with compliance dates as follows:
  - Feb. 2, 2025 – Prohibitions on unacceptable risk AI
  - Aug. 2, 2025 – Obligations for general-purpose AI governance apply
  - Aug. 2, 2026 – All EU AI Act rules apply, including certain rules for high-risk systems
  - Aug. 2, 2027 – All rules for all high-risk systems become available

- EU AI Act applies to providers, deployers, product manufacturers, importers, distributors and authorized representatives, of AI systems or general-purpose AI models that are placed on the EU market, put into service or used in the EU, even if they were established in a third country.

- AI Definition: A machine-based system designed to operate with varying levels of autonomy that may exhibit adaptiveness after deployment and 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.

EU AI Act – Tiered Risk Approach

Prohibited AI Practices	High-risk AI Systems	General-purpose AI Models	General-purpose AI Models with Systemic Risks	Transparency Rules
Prohibited Systems include: ✓ Social behavioral scoring systems ✓ Emotion-recognition systems ✓ AI to exploit people's vulnerabilities, such as ages or disabilities ✓ Behavioral manipulation ✓ Untargeted scraping for facial recognition ✓ Biometric categorization systems that use certain sensitive characteristics ✓ Specific predictive policing applications ✓ Law enforcement use of real-time biometric identification in public, apart from in limited, authorized situations	**Pose a significant risk to health, safety or fundamental rights and require:** ✓ Risk management ✓ Data quality and governance ✓ Documentation and traceability ✓ Transparency ✓ Human oversight ✓ Accuracy, cybersecurity and robustness ✓ Demonstrated compliance via conformity assessment ✓ If deployed by public institution, registration in EU Database	**AI models that display significant generality, are capable of competently performing a wide range of distinct tasks, regardless of how they are placed on the market, and can be integrated into a variety of downstream systems or applications, which require:** ✓ Perform FRIAs and conformity assessments ✓ Implement risk and quality management systems ✓ Inform users about AI interaction ✓ Test and monitory for Accuracy, cybersecurity and robustness ✓ AI with systemic risks subject to higher standards	**General-purpose AI models that have "high-impact capabilities" that match or exceed the capabilities recorded in the most advanced general-purpose AI models, which require:** ✓ Model evaluation and adversarial testing ✓ Assessment and mitigation of systemic risks ✓ Documentation of serious incidents and corrections ✓ Adequate cybersecurity and physical infrastructure ✓ Adherence to codes of practice ✓ Compliance with Article 78 confidentiality, as applicable	**Specific transparency obligations are imposed on providers and deployers of certain AI systems, which include:** ✓ Make users aware of AI interaction ✓ GenAI outputs must be marked in a machine-readable format and detectable as AI generated or manipulated ✓ Emotion recognition or biometric categorization AI must inform users about the systems' operations ✓ AI creating deepfakes and manipulated text mean to inform on matters of public interest must abide by strict disclosure requirements

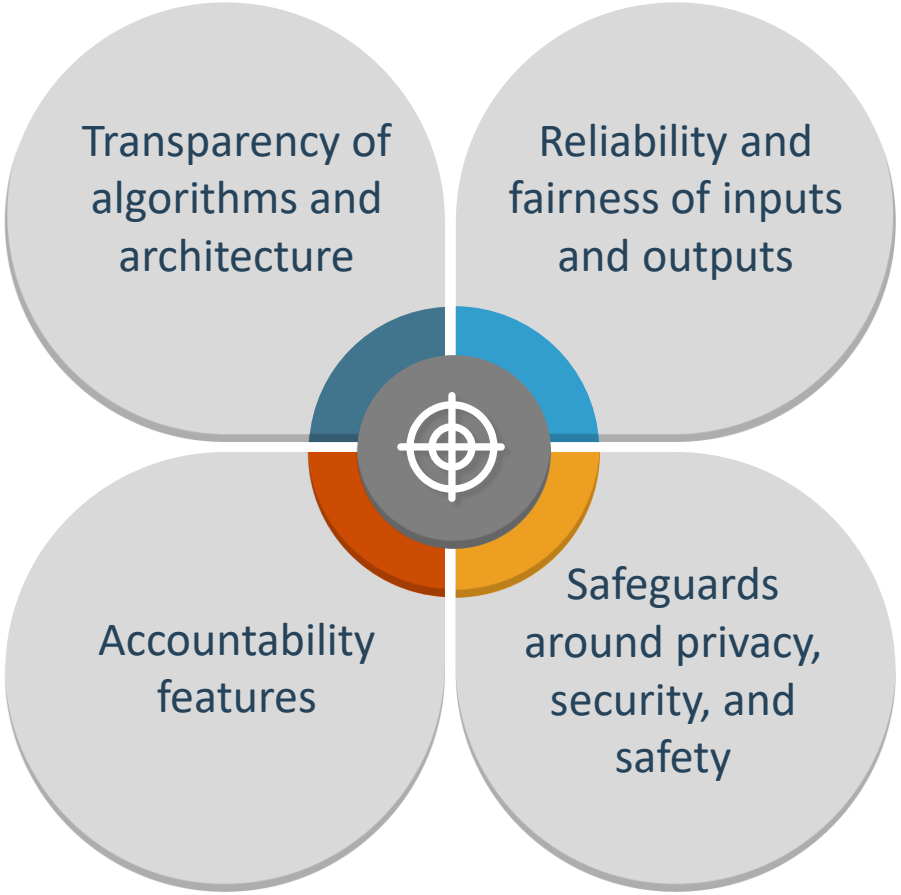
Building an Effective AI Governance Program

EPSTEIN BECKER GREEN

Ethical Dimensions for Managing Risk

Building TRUST by Opening the AI 'Black Box'

Image credit: Shutterstock



Guiding Principles

Promote health and healthcare equity during all healthcare algorithm life cycle phases.

Ensure healthcare algorithms and their use are transparent and explainable.

Authentically engage patients and communities during all healthcare algorithm life cycle phases and earn trustworthiness.

Explicitly identify healthcare algorithmic fairness issues and tradeoffs.

Establish accountability for equity and fairness in outcomes from healthcare algorithms.

Source: U.S. Department of Health and Human Services (https://www.hhs.gov/about/news/2023/12/15/guiding-principles-help-healthcare-community-address-potential-bias-resulting-from-algorithms.html)

Building Trust with AI Governance

Key Governance Steps

- Board commitment to AI Governance
- C-Suite leaders must understand and commit to AI Governance principles
- Appoint individuals to oversee the AI Governance program including data stewards
- Develop policies and protocols to oversee AI Governance program
- Establish review and approval process to identify and manage risk related to AI deployment by the organization

Principles of Data Stewardship

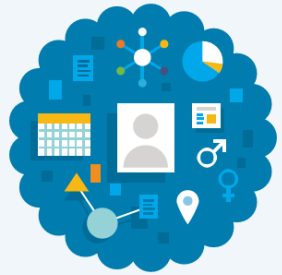
- Transparency
- Individual Participation
- Purpose Specification
- Data Minimization
- Use Limitation
- Data Quality & Integrity
- Security
- Accountability and Auditing

De-identification / Pseudonymization / Anonymization Strategy

A VISUAL GUIDE TO PRACTICAL DATA DE-IDENTIFICATION

Produced by FUTURE OF PRIVACY FORUM FPF.org

What do scientists, regulators and lawyers mean when they talk about de-identification? How does anonymous data differ from pseudonymous or de-identified information? Data identifiability is not binary. Data lies on a spectrum with multiple shades of identifiability.



This is a primer on how to distinguish different categories of data.

DEGREES OF IDENTIFIABILITY
Information containing direct and indirect identifiers.

PSEUDONYMOUS DATA
Information from which direct identifiers have been eliminated or transformed, but indirect identifiers remain intact.

DE-IDENTIFIED DATA
Direct and known indirect identifiers have been removed or manipulated to break the linkage to real world identities.

ANONYMOUS DATA
Direct and indirect identifiers have been removed or manipulated together with mathematical and technical guarantees to prevent re-identification.

	EXPLICITLY PERSONAL	POTENTIALLY IDENTIFIABLE	NOT READILY IDENTIFIABLE	KEY CODED	PSEUDONYMOUS	PROTECTED PSEUDONYMOUS	DE-IDENTIFIED	PROTECTED DE-IDENTIFIED	ANONYMOUS	AGGREGATED ANONYMOUS
DIRECT IDENTIFIERS Data that identifies a person without additional information or by linking to information in the public domain (e.g., name, SSN)	INTACT	PARTIALLY MASKED	PARTIALLY MASKED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED
INDIRECT IDENTIFIERS Data that identifies an individual indirectly. Helps connect pieces of information until an individual can be singled out (e.g., DOB, gender)	INTACT	INTACT	INTACT	INTACT	INTACT	INTACT	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED
SAFEGUARDS and CONTROLS Technical, organizational and legal controls preventing employees, researchers or other third parties from re-identifying individuals	NOT RELEVANT due to nature of data	LIMITED or NONE IN PLACE	CONTROLS IN PLACE	CONTROLS IN PLACE	LIMITED or NONE IN PLACE	CONTROLS IN PLACE	LIMITED or NONE IN PLACE	CONTROLS IN PLACE	NOT RELEVANT due to nature of data	NOT RELEVANT due to high degree of data aggregation
SELECTED EXAMPLES	Name, address, phone number, SSN, government-issued ID (e.g., Jane Smith, 123 Main Street, 555-555-5555)	Unique device ID, license plate, medical record number, cookie, IP address (e.g., MAC address 68:A8:6D:35:65:03)	Same as Potentially Identifiable except data are also protected by safeguards and controls (e.g., hashed MAC addresses & legal representations)	Clinical or research datasets where only curator retains key (e.g., Jane Smith, diabetes, HgB 15.1 g/dl = Csrk123)	Unique, artificial pseudonyms replace direct identifiers (e.g., HIPAA Limited Datasets, John Doe = 5L7T LX619Z) (unique sequence not used anywhere else)	Same as Pseudonymous, except data are also protected by safeguards and controls	Data are suppressed, generalized, perturbed, swapped, etc. (e.g., GPA: 3.2 = 3.0-3.5, gender: female = gender: male)	Same as De-Identified, except data are also protected by safeguards and controls	For example, noise is calibrated to a data set to hide whether an individual is present or not (differential privacy)	Very highly aggregated data (e.g., statistical data, census data, or population data that 52.6% of Washington, DC residents are women)

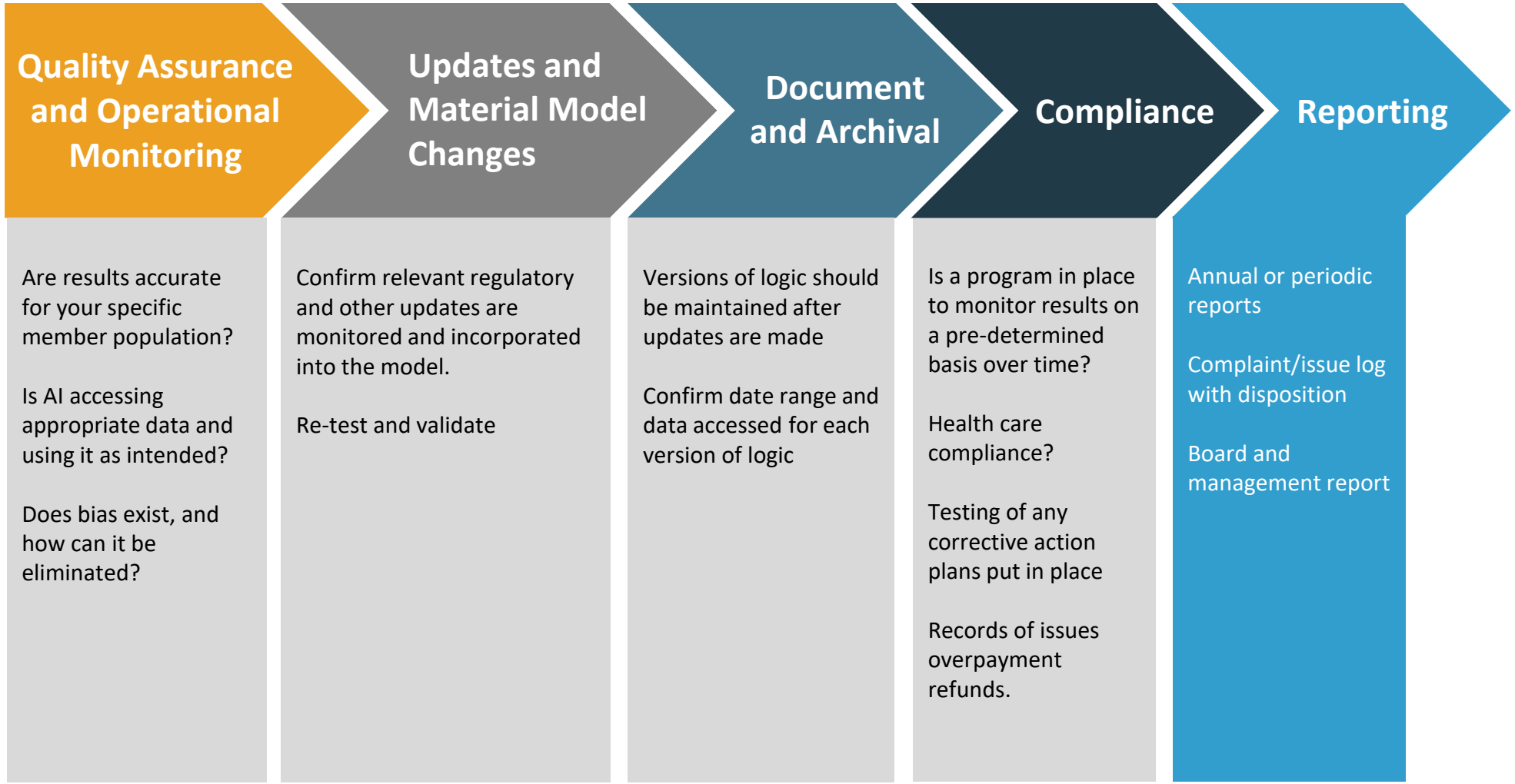
AI Due Diligence Prior to Deployment

- Who is responsible at the organization? AI Oversight Team?
- What is the scope of intended use?
- How to investigate and diligence?
  - Vendor (and software manufacturer where applicable)
  - Technology
  - Enforcement risks
- Engagement Hurdles and Challenges?
  - Legal Contract Review
  - Business Contract Review
  - Allocation of Risk, Liability and Indemnities
- What is the timeline and implementation plan?
- How to conduct pre-deployment testing and ensure validation prior to approval?

AI Contracting

- Establishing clarity on expectation of services
- Intellectual property protection
- Representations and Warranties
- Disclaimers of Warranties
- Allocation of Risk
  - Indemnification
  - Limitations on liability
- Insurance Requirements
- Changes in Law

Ongoing Activities After AI is Implemented



Adapting the 7 Elements of the OIG's Compliance Program Guidance for the Creation and Use of AI Tools

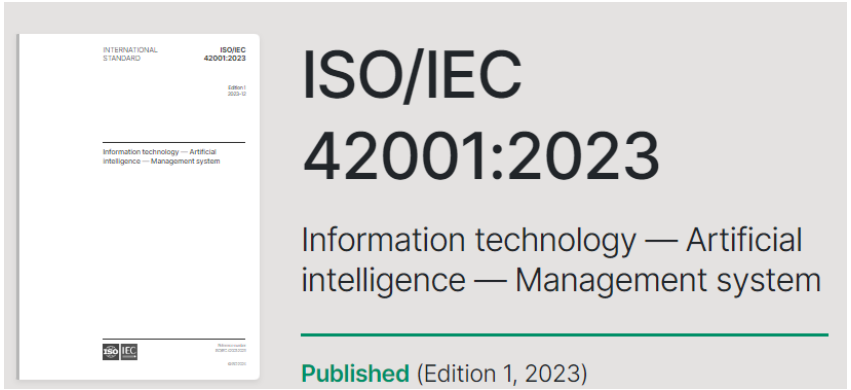
- Implement written policies, procedures and standards of conduct.
- Designate a compliance officer and compliance committee.
  - Designation of ownership of the AI risks.
  - Consider creating a committee charter.
- Conduct effective training and education.
- Develop effective lines of communication.
  - Reporting mechanism for concerns about AI tools.

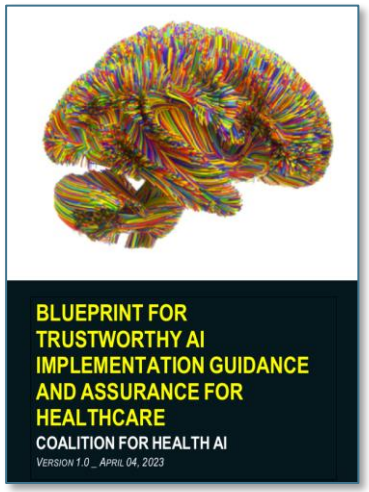
- Conduct internal and external monitoring and auditing.
  - A risk assessment identifies high and moderate risk areas, which should be the focus on auditing and monitoring programs.
- Enforce standards through well-publicized disciplinary guidelines for failure to comply.
- Respond promptly to detected offenses and undertaking corrective action.

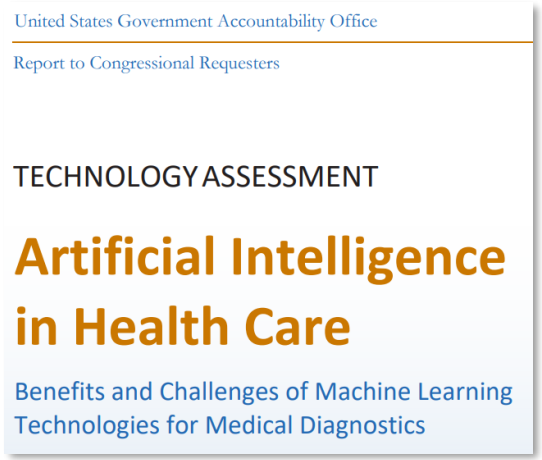
Risk Assessment: Creation and Use of AI Tools

(-) Impact →	1	2	3	4	5
Probability ↓	Negligible	Minor	Moderate	Significant	Severe
(81-100)%					AI clinical decision support tool for reading MRIs
(61-80)%				Cognitive assessment	
(41-60)%			Resume screener		
(21-40)%		Predictive orthopedic implant			
(1-20)%	Chatbot interview scheduling				AI analysis of EHR to propose billing codes

Leverage Emerging Guidance







EPSTEIN
BECKER
GREEN

Questions?

EPSTEIN BECKER GREEN

Thank you!