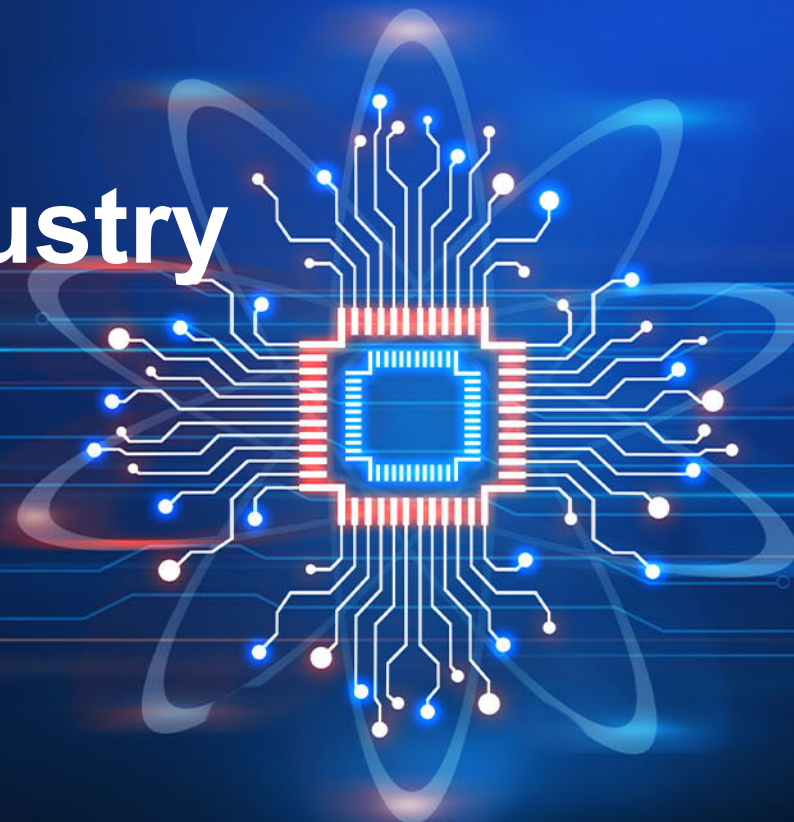


The Age of AI - AI and the Health Care Industry

Ryan P. Blaney, Partner
Co-Head of Privacy & Cybersecurity

January 30, 2024





ChatGPT's Response to Create an Agenda?


ChatGPT 3.5 ▾

You
draft an agenda for a presentation of health care AI for legal and compliance professionals

ChatGPT
Title: Exploring the Intersection of Healthcare AI: Legal and Compliance Perspectives

Agenda:

- I. Introduction
 - Welcome and Introductions
 - Purpose of the Presentation
- II. Understanding Healthcare AI
 - Definition and Scope of Healthcare AI
 - Overview of AI Applications in Healthcare
 - Importance of AI in Improving Healthcare Processes
- III. Legal and Compliance Frameworks in Healthcare AI
 - Regulatory Landscape: Overview of Relevant Laws and Regulations
 - Compliance Challenges in Implementing Healthcare AI
 - Legal Considerations for Healthcare AI Ac  on

Message ChatGPT... 

ChatGPT can make mistakes. Consider checking important information.

Agenda

Introduction

Overview of Health Care AI

- Define AI in Health Care
 - Health Care Providers, Pharma
 - Devices, IT Services
-

- Transformative Impact on Patient Care
-

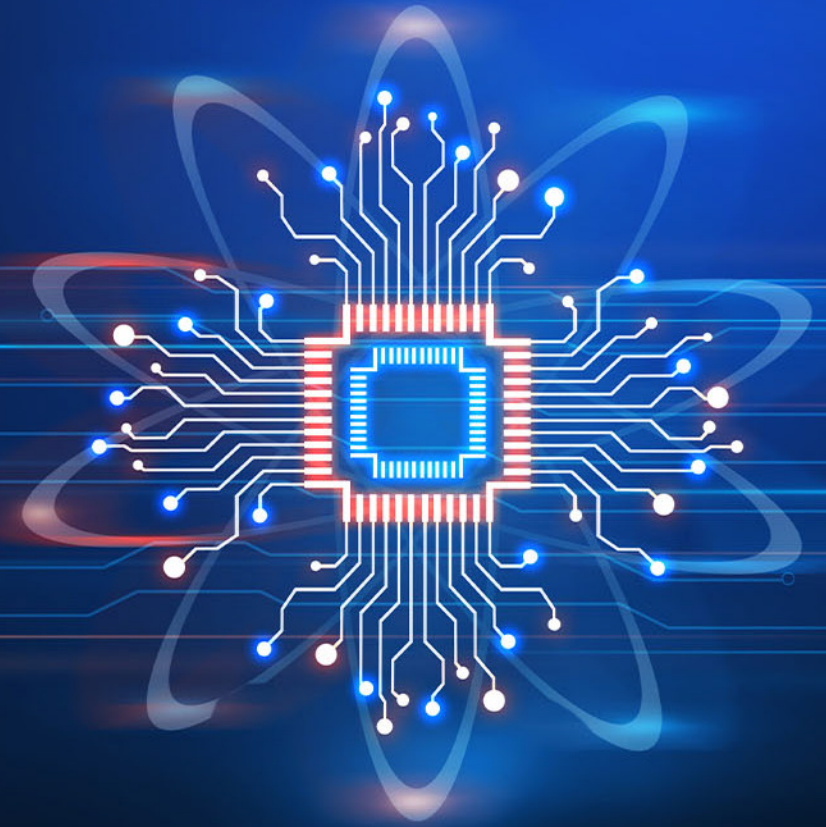
Current Legal Framework in the United States

- Federal (CMS, HHS, DOJ)
 - FTC Developments
 - State AGs
-

Legal Considerations

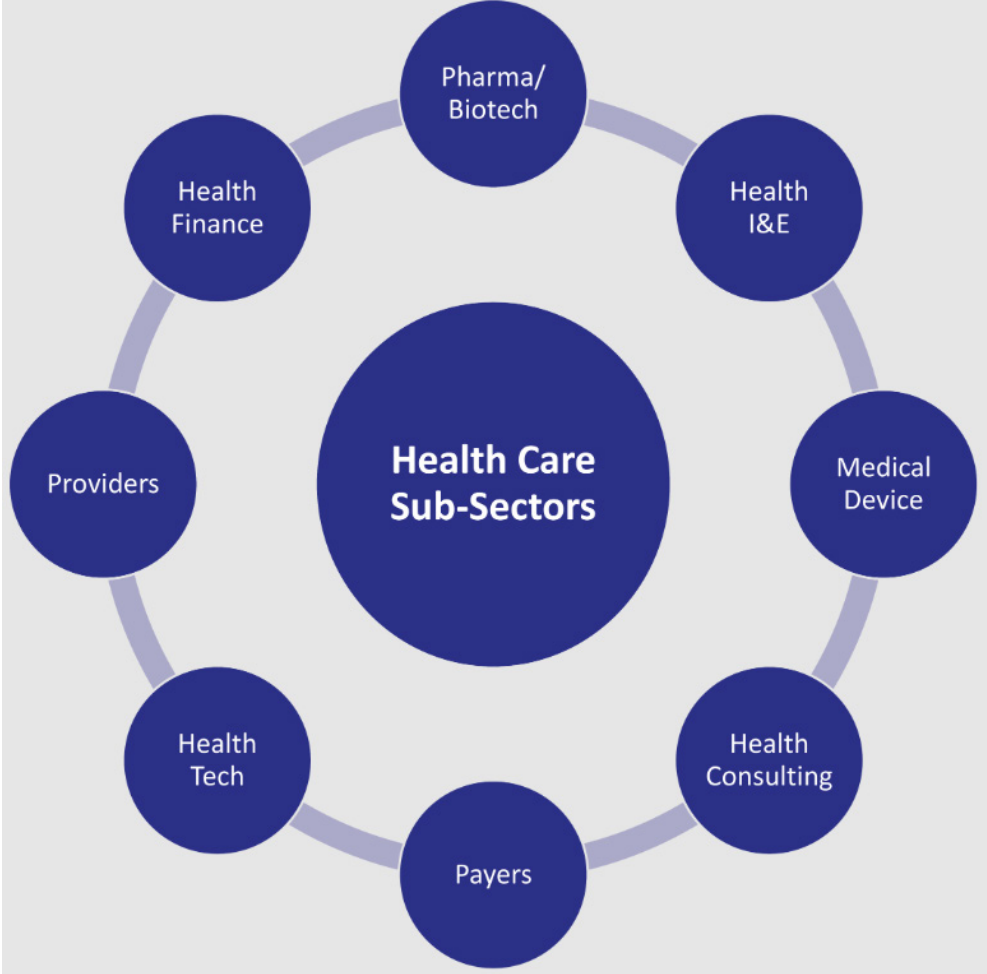
Conclusion

Overview of AI in Health Care



The Health Care Industry

- According to the American Hospital Association, health care makes up approximately one-sixth of the U.S. economy.





ChatGPT's Response re: Healthcare AI?



You

Describe healthcare ai in 50 words



ChatGPT

Healthcare AI encompasses the use of artificial intelligence technologies in various aspects of healthcare, including diagnosis, treatment, patient care, and administrative tasks. It leverages algorithms and data analysis to improve medical outcomes, streamline processes, enhance decision-making, and ultimately transform the delivery of healthcare services for patients and providers alike.



AI and GAI

AI:

Computer systems that perform tasks requiring human-like cognition, enabling machines to autonomously learn, reason, and adapt through experience.

GAI:

A subset of AI focused on creating new, original content or data, such as images, text, or music, by autonomously learning patterns and features from existing datasets.

How the U.S. Department of Health & Human Services Defines AI?



AI Definition

To understand whether TAI principles need to be applied to a technology solution, let's first discuss what defines AI.

To help determine if a use case constitutes AI*, consider whether the solution or system...^{1, 4}

- A. *...performs tasks under varying and unpredictable circumstances without significant human oversight, or **can learn from experience and improve performance** when exposed to data sets?*
- B. *...uses computer software, physical hardware, or other technology to **solve tasks that require human-like perception**, thinking, planning, learning, communication, or physical action?*
- C. *...thinks or acts like a human, including the use of **cognitive architecture or neural networks** (e.g., developed to mimic the underlying mechanisms of the human mind)?*
- D. *...relies on a **set of techniques, including machine learning, to approximate a cognitive task?***
- E. *...is designed to act rationally by utilizing **intelligent software or an embodied robot to achieve goals** using perception, planning, reasoning, learning, communicating, decision-making, and acting?*

These considerations, while not all-encompassing, serve as a guide in determining whether a solution constitutes AI and whether TAI principles need to be applied

**Based on the National Defense Authorization Act for Fiscal Year 2019, Section 238 (g), as utilized in Executive Order (EO) 13960.*

HHS Trustworthy AI Playbook – Sample AI Methods

| | DEFINITION | SAMPLE TAI IMPLICATIONS |
|--|--|--|
| Machine Learning (ML) | <i>“A subfield of artificial intelligence that gives computers the ability to learn without explicitly being programmed” – MIT⁵ Includes probabilistic methods⁵ and can support predictive analytics⁶</i> | Machine learning should be bias-free and incorporate relevant shifts in healthcare demographics |
| Natural Language Processing (NLP) | <i>“Machines learn to understand natural language as spoken and written by humans” – MIT⁷ and includes both Natural Language Generation (NLG) and Natural Language Understanding (NLU) – IBM⁸</i> | NLP models should be understandable to users to prevent incorrect interpretations that could negatively impact affected individuals |
| Speech Recognition | <i>“Systems [that] interpret human speech and translate it into text or commands.” – Gartner⁹</i> | Voice and speech should be inclusive of a broad range of languages, dialects, and accents |
| Computer Vision | <i>“Intelligent algorithms that perform important visual perception tasks such as object recognition, scene categorization, integrative scene understanding, human motion recognition, material recognition, etc.” – Stanford¹⁰</i> | Computer vision models should be trained with data representative of the patient populations that will use them to support unbiased results |
| Intelligent Automation | <i>“The use of automation technologies – artificial intelligence (AI), business process management (BPM), and robotic process automation (RPA) – to streamline and scale decision-making across organizations– IBM¹¹</i> | Intelligent automation solutions should have a human sponsor that is responsible for ensuring protected information (e.g., patient data) is not accessible |

Artificial Intelligence

Artificial intelligence is technology that mimics human activity, decision-making, and learning

- What is Artificial Intelligence (AI)?
 - Per [John McCarthy, Stanford University](#):
 - “...the science and engineering of making intelligent machines, especially intelligent computer programs”
 - “... related to the similar task of using computers to understand human intelligence...”
 - “...AI does not have to confine itself to methods that are biologically observable”
 - Per [IBM](#):
 - “...leverages computers and machines to mimic the problem-solving and decision-making capabilities of the human mind”



Blade Runner movie poster
Image source: IMP Awards



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center

How the Office of Information Security Describes Potential Benefits:

Artificial Intelligence in Healthcare

Artificial intelligence in healthcare has the potential to revolutionize clinical research and the monitoring and delivery of care

- Benefits of AI to the health sector:

- Analysis of big data sets

- Accelerated clinical decisions

- Example: Interpretation of medical imaging

- Improved (deeper) patient insights → predictive analysis

- Connecting disparate health data (integrated electronic health records)

- New drug discovery and preventive medicine

- Medical devices (Software-as-a-Medical-Device/SaMD)

- "...software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device"

- Improved efficiency of enterprise operations/streamlined workflows

Recommended reading:

[Cloud Security Alliance: Artificial Intelligence in Healthcare](#)



Office of
Information Security
Securing One HHS



Health Sector Cybersecurity
Coordination Center

AI in Health Care – Proven Benefits:

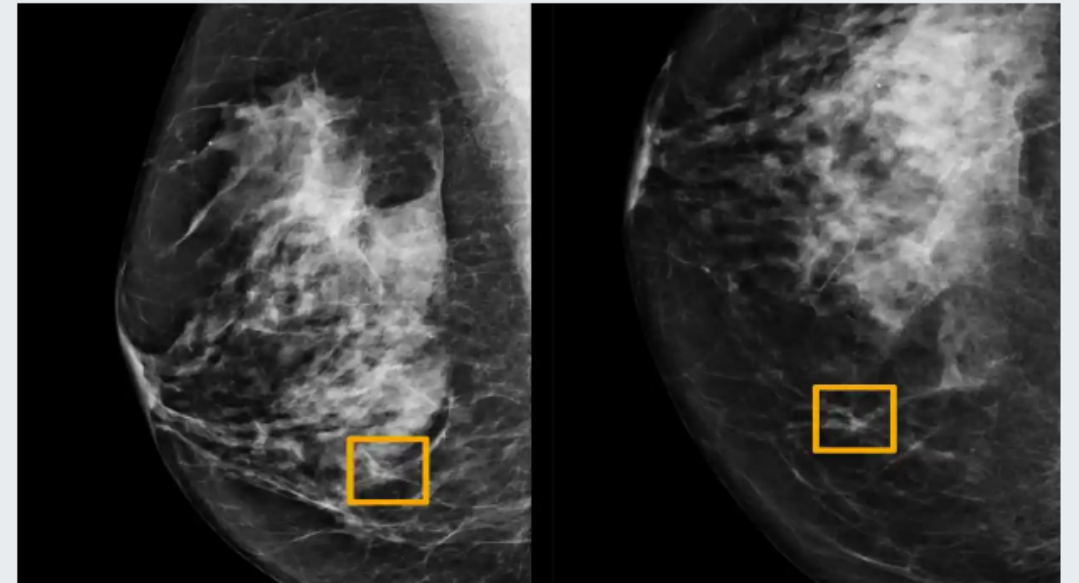
AI system outperforms experts in spotting breast cancer

An AI program developed by Google in 2020 has demonstrated the ability to spot breast cancer in mammograms better than expert radiologists

The yellow box in the images on the right indicate where an AI system identified cancer in breast tissue. Six radiologists had previously failed to identify it.

Read more:

<https://www.theguardian.com/society/2020/jan/01/ai-system-outperforms-experts-in-spotting-breast-cancer>



Medical imagery indicating cancer
Image source: The Guardian

Health Care Industry and AI – Use Cases available at:
<https://www.hhs.gov/about/agencies/asa/ocio/ai/use-cases/index.html>

Department of Health and Human Services: Artificial Intelligence Use Cases Inventory

Executive Order 13960, “Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government,” requires agencies to prepare an inventory of non-classified and non-sensitive current and planned Artificial Intelligence (AI) use cases. Agencies must share their inventories with the public and other agencies, to the extent practicable. The HHS Office of the Chief Artificial Intelligence Officer (OCAIO) has created an inventory of HHS AI use cases that not only satisfies the executive order requirements, but also increases awareness of and cross-agency collaboration on AI initiatives. Below, we highlight some AI use cases (“Example HHS Use Cases”) and provide the complete inventories.

- [Example HHS AI Use Cases FY22 - PDF](#)
- [HHS AI Use Cases Inventory FY22 - PDF](#)
- [HHS AI Use Cases Inventory FY23 - CSV](#)

Content created by Office of the Chief Information Officer (OCIO)
Content last reviewed January 11, 2024

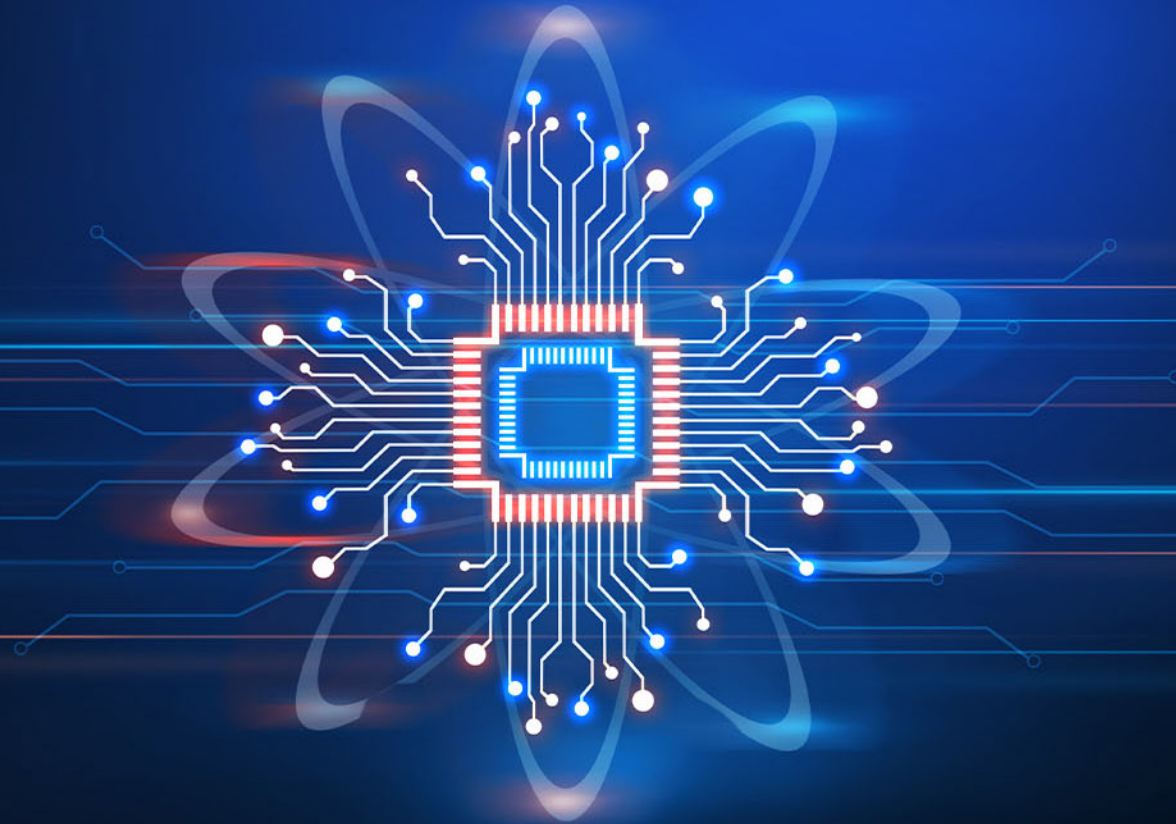
FDA's Complied list of public facing AI/ML enabled devices:

Artificial Intelligence and Machine Learning (AI/ML)-Enabled Medical Devices

[f Share](#) [X Post](#) [in LinkedIn](#) [✉ Email](#) [🖨 Print](#)

October 19, 2023 update: 171 Artificial Intelligence and Machine Learning (AI/ML)-Enabled Medical Devices were added to the list below. Of those newly added to the list, 155 are devices with final decision dates between August 1, 2022, and July 30, 2023, and 16 are devices from prior periods identified through a refinement of methods used to generate this list.

Current Legal Framework



US Developments - Legal landscape for Privacy & AI

- There is no overarching federal law governing AI.
 - Left with voluntary frameworks, executive orders against algorithmic discrimination, unfair business and anti-discrimination laws as regulated by the FTC (and other agencies), and a patchwork of state laws
- **Congress:** Efforts in Senate to establish rules on AI.
- **White House Blueprint for an AI Bill of Rights:** Outlines five principles – safe and effective systems; algorithmic discrimination protections; notice and explanation; and human alternatives to AI systems; and data
- **State laws:** Some state laws regarding use of AI in any employment decisions.
 - Other bills that seek to regulate AI and automated decision-making and require impact assessments for AI tools being debated in state legislatures (e.g., California AB-331)
- **Medical Organization:** Self regulation and industry guidelines.

Schumer calls for AI rules as ChatGPT surges in popularity

The Senate majority leader has circulated a plan to establish rules on AI to address national security concerns as ChatGPT becomes the fastest-growing consumer application in history.

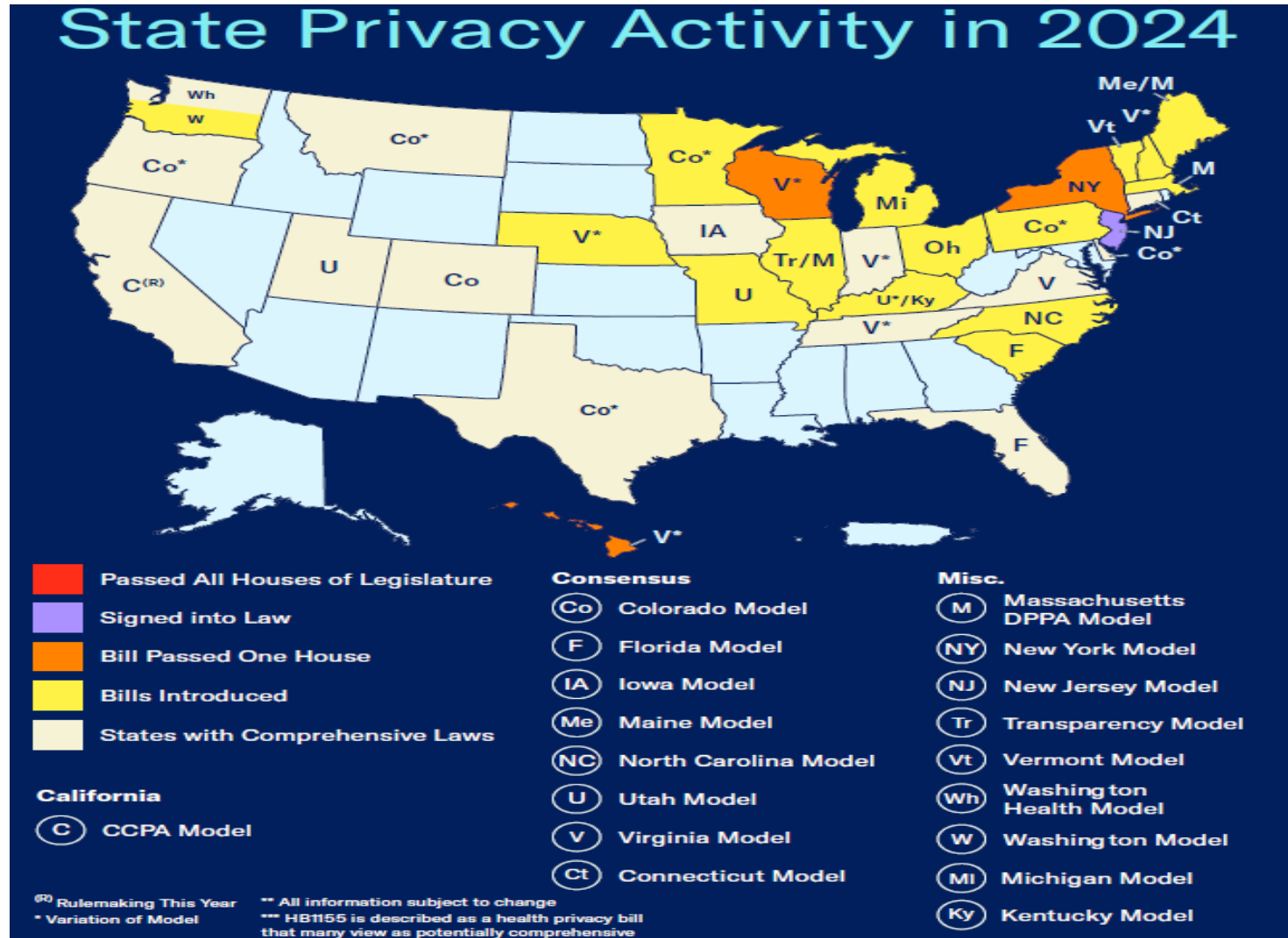


BLUEPRINT FOR AN AI BILL OF RIGHTS

MAKING AUTOMATED SYSTEMS WORK FOR THE AMERICAN PEOPLE

 OSTP

U.S. Chamber of Commerce Technology Engagement Center:



Legislative Trend: Creation of Subcategory of Personal Information

- Sensitive personal information, sometimes called SPI, is data that is subject to strict protection guidelines under laws like the GDPR and the CPRA.
 - General Data Privacy Regulation (GDPR)
 - California Privacy Rights Act (CPRA); California Consumer Protection Act (CCPA)
 - Virginia Consumer Data Protection Act (CDPA)
- If sensitive data is breached or compromised, it could lead to discrimination, harassment, identity theft, or impact the quality of the person's daily life in other harmful ways.



GDPR Definition of Sensitive Information under Article 9:

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Trend: Health-Related Data is Broader than PHI and HIPAA



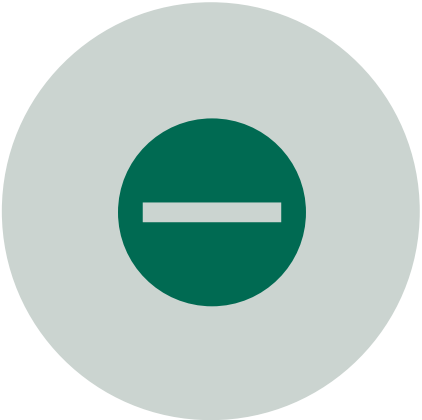
What is Health Data?



HIPAA COVERED
DATA (E/PHI)



SENSITIVE HEALTH
DATA



NON-SENSITIVE

HIPAA Covered Data?

HIPAA

“Individually identifiable health information means any information, including demographic information collected from an individual, that:

- (a) Is created or received by a health care provider, health plan, employer, or healthcare clearinghouse; and
- (b) Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and –
 - (1) Identifies the individual; or
 - (2) With respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

 Names

Dates 

 Addresses / Zip Codes / Geocodes

Phone Numbers 

 Fax Numbers

Email Addresses 

 Social Security Numbers

List of PHI

(Protected Health Information)

Medical Record Numbers 

 Health Plan Beneficiary Numbers


Account Numbers 


 AB-12 34 Certificate /License Numbers

 Device Identifiers

Vehicle Identifiers 

 URLs

IP Addresses 

 Biometric Identifiers

Facial Images 

 Any Other Unique Identifiers

What is Health Information? Washington My Health My Data Act

MHMDA

“Consumer health data means personal information that is linked or reasonably linkable to a consumer and that identifies the consumer’s past, present or future physical or mental health status.”

Includes:

- (1) Individual health conditions, treatment, diseases, or diagnosis.
- (2) Gender-affirming care information
- (3) Biometric data
- (4) Precision location information
- (5) Data that identifies a consumer seeking health care services

What is Health Information? Virginia Consumer Data Protection

Virginia CDPA

“**Personal data** means any information that is linked or reasonably linkable to an identified or identifiable natural person.”

“**Sensitive data** means a category of personal data that includes:

- (1) Mental or physical health diagnosis
- (2) Genetic or biometric data for the purpose of uniquely identifying a natural person.”

What is Health Information? FTC

FTC Consent Orders

In the Matter of Flo Health, Inc. (2023)

- “individually identifiable information from or about an individual consumer relating to health, including but not limited to information concerning fertility, menstruation, sexual activity, pregnancy, and childbirth.”

In the Matter of Health.io Inc. (2023)

- “individually identifiable information relating to the health or genetics of an individual.”

U.S. v. Easy Healthcare (2023)

- “medical records and other individually identifiable information relating to the past, present, or future physical or mental health or conditions of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of healthcare to an individual.”

FTC's Health Breach Notification Rule – 2021 Policy Statement

- Health and fitness app developers are “health care providers” for purposes of the HBNR.
- Applies to any device that is “capable of pulling health information plus any other information from multiple sources (e.g. wearables).
- Breach includes any disclosure not authorized by consumer.



Office of the Chair

UNITED STATES OF AMERICA

Federal Trade Commission

WASHINGTON, D.C. 20580

STATEMENT OF THE COMMISSION

On Breaches by Health Apps and Other Connected Devices

September 15, 2021

In recognition of the proliferation of apps and connected devices that capture sensitive health data, the Federal Trade Commission is providing this Policy Statement to offer guidance on the scope of the FTC's Health Breach Notification Rule, 16 C.F.R. Part 318 (“the Rule”).¹

Potential State Level Issues



- Original CCPA was silent on automated decision-making.
- However, the CPRA amendments, as well as other state data privacy laws (e.g., Colorado and Connecticut) gives certain rights to consumers re: automated decision-making technology.
- Notably, in March 2023, the CPPA requested pre-rulemaking comments in helping it craft regulations on automated decision-making), including questions about whether access and opt-out rights with respect to automated decision-making should depend on the industry, the technology used, and the sensitivity of the PII.
- In the Colorado privacy regs, there are rules on opt-out rights of decisions based on automated processing that produce legal or other significant effects on a consumer.

FDA, HHS and CMS Issue Guidance on AI



Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action Plan

January 2021



Trustworthy AI (TAI) Playbook
U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES

SEPTEMBER 2021

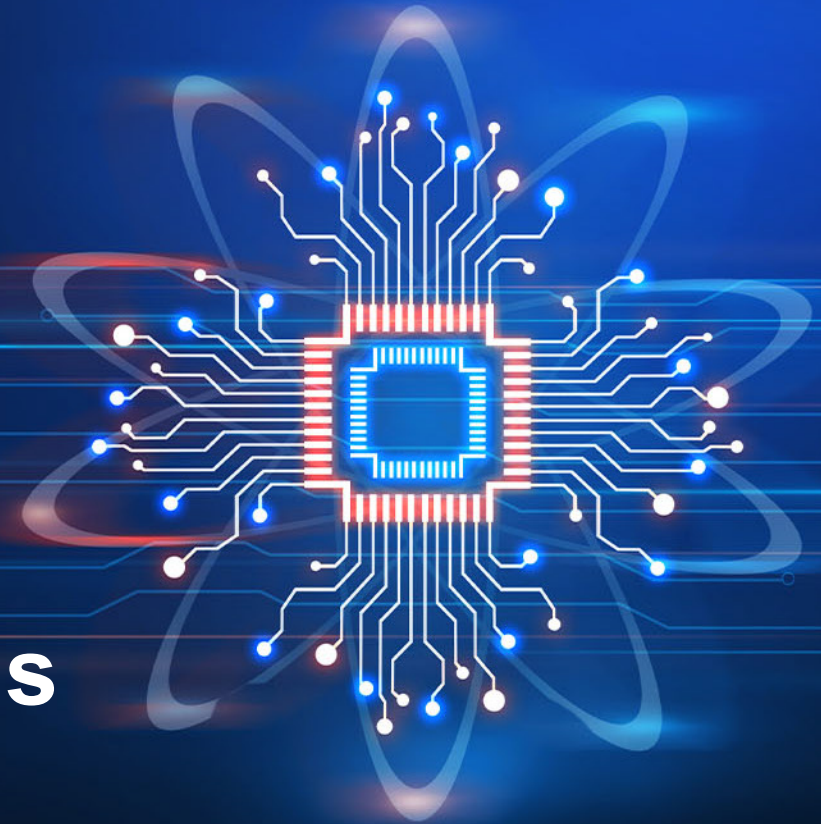
CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

CMS AI Playbook

Centers for Medicare & Medicaid Service

Version 2.0

Legal & Ethical Considerations



August 8, 2023

Mr. Sundar Pichai
Chief Executive Officer
Alphabet Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043

Dear Mr. Pichai,

I write to express my concern regarding reports that Google began providing Med-PaLM 2 to hospitals to test early this year.¹ While artificial intelligence (AI) undoubtedly holds tremendous potential to improve patient care and health outcomes, I worry that premature deployment of unproven technology could lead to the erosion of trust in our medical professionals and institutions, the exacerbation of existing racial disparities in health outcomes, and an increased risk of diagnostic and care-delivery errors.

Over the past year, large technology companies, including Google, have been rushing to develop and deploy AI models and capture market share as the technology has received increased attention following OpenAI's launch of ChatGPT.² Numerous media outlets have reported that companies like Google and Microsoft have been willing to take bigger risks and release more nascent technology in an effort to gain a first mover advantage.³ In 2019, I raised concerns that Google was skirting health privacy laws through secretive partnerships with leading hospital systems, under which it trained diagnostic models on sensitive health data without patients' knowledge or consent.⁴ This race to establish market share is readily apparent and especially concerning in the health care industry, given the life-and-death consequences of mistakes in the clinical setting, declines of trust in health care institutions in recent years, and the sensitivity of health information. One need look no further than AI pioneer Joseph Weizenbaum's experiments involving chatbots in psychotherapy to see how users can put premature faith in even basic AI solutions.

According to Google, Med-PaLM 2 can answer medical questions, summarize documents, and organize health data. While AI models have previously been used in medical settings, the use of

¹ Kruppa, Miles, and Nidhi Subbaraman. "In Battle with Microsoft, Google Bets on Medical AI Program to Crack Healthcare Industry." *Wall Street Journal*, July 8, 2023. <https://www.wsj.com/articles/in-battle-with-microsoft-google-bets-on-medical-ai-program-to-crack-healthcare-industry-bb7c2db8>.

² Roose, Kevin. "How ChatGPT Kicked Off an A.I. Arms Race." *The New York Times*, February 3, 2023. <https://www.nytimes.com/2023/02/03/technology/chatgpt-opens-artificial-intelligence.html>.

³ Grant, Nico, and Karen Weise. "In A.I. Race, Microsoft and Google Choose Speed Over Caution." *The New York Times*, April 7, 2023. <https://www.nytimes.com/2023/04/07/technology/ai-chatbots-google-microsoft.html>.

⁴ Needleman, Sarah E., and Rob Copeland. "U.S. Lawmakers Scold Google's 'Project Nightingale' Over Health-Data Privacy." *Wall Street Journal*, November 12, 2019. <https://www.wsj.com/articles/senators-urge-scrutiny-of-health-data-deals-including-google-project-11573597883>.

generative AI tools presents complex new questions and risks. According to the *Wall Street Journal*, a senior research director at Google who worked on Med-PaLM 2 said, "I don't feel that this kind of technology is yet at a place where I would want it in my family's healthcare journey."⁵ Indeed, Google's own research, released in May, showed that Med-PaLM 2's answers contained more inaccurate or irrelevant information than answers provided by physicians.⁶ It is clear more work is needed to improve this technology as well as to ensure the health care community develops appropriate standards governing the deployment and use of AI.

Given these serious concerns and the fact that VHC Health, based in Arlington, Virginia, is a member of the Mayo Clinic Care Network, I request that you provide answers to the following questions.

1. Researchers have found large language models to display a phenomenon described as "sycophany," wherein the model generates responses that confirm or cater to a user's (tacit or explicit) preferred answers⁷, which could produce risks of misdiagnosis in the medical context. Have you tested Med-PaLM 2 for this failure mode?
2. Large language models frequently demonstrate the tendency to memorize contents of their training data, which can risk patient privacy in the context of models trained on sensitive health information. How has Google evaluated Med-PaLM 2 for this risk and what steps has Google taken to mitigate inadvertent privacy leaks of sensitive health information?
3. What documentation did Google provide hospitals, such as Mayo Clinic, about Med-PaLM 2? Did it share model or system cards, datasheets, data-statements, and/or test and evaluation results?
4. Google's own research acknowledges that its clinical models reflect scientific knowledge only as of the time the model is trained, necessitating "continual learning." What is the frequency with which Google fully or partially re-trains Med-PaLM 2? Does Google ensure that licensees use only the most up-to-date model version?
5. Google has not publicly provided documentation on Med-PaLM 2, including refraining from disclosing the contents of the model's training data. Does Med-PaLM 2's training corpus include protected health information?
6. Does Google ensure that patients are informed when Med-PaLM 2, or other AI models offered or licensed by, are used in their care by health care licensees? If so, how is the disclosure presented? Is it part of a longer disclosure or more clearly presented?
7. Do patients have the option to opt-out of having AI used to facilitate their care? If so, how is this option communicated to patients?

⁵ Kruppa, Miles, and Nidhi Subbaraman. "In Battle With Microsoft, Google Bets on Medical AI Program to Crack Healthcare Industry." *Wall Street Journal*, July 8, 2023. <https://www.wsj.com/articles/in-battle-with-microsoft-google-bets-on-medical-ai-program-to-crack-healthcare-industry-bb7c2db8>.

⁶ Singhal, Karan, Tao Tu, Juraj Gottweis, Rory Sayres, Ellery Wulczyn, Le Hou, Kevin Clark, et al. "Towards Expert-Level Medical Question Answering with Large Language Models." arXiv, May 16, 2023. <https://arxiv.org/pdf/2305.09617.pdf>.

⁷ Perez, Ethan, Sam Ringer, Kamile Lukosiute, Karina Nguyen, Edwin Chen, Scott Heiner, Craig Pettit, et al. "Discovering Language Model Behaviors with Model-Written Evaluations." In *Findings of the Association for Computational Linguistics: ACL 2023*, 13387-434. Toronto, Canada: Association for Computational Linguistics, 2023. <https://aclanthology.org/2023.findings-acl.847>.

8. Does Google retain prompt information from health care licensees, including protected health information contained therein? Please list each purpose Google has for retaining that information.
9. What license terms exist in any product license to use Med-PaLM 2 to protect patients, ensure ethical guardrails, and prevent misuse or inappropriate use of Med-PaLM 2? How does Google ensure compliance with those terms in the post-deployment context?
10. How many hospitals is Med-PaLM 2 currently being used at? Please provide a list of all hospitals and health care systems Google has licensed or otherwise shared Med-PaLM 2 with.
11. Does Google use protected health information from hospitals using Med-PaLM 2 to retrain or finetune Med-PaLM 2 or any other models? If so, does Google require that hospitals inform patients that their protected health information may be used in this manner?
12. In Google's own research publication announcing Med-PaLM 2, researchers cautioned about the need to adopt "guardrails to mitigate against over-reliance on the output of a medical assistant."⁸ What guardrails has Google adopted to mitigate over-reliance on the output of Med-PaLM 2 as well as when it particularly should and should not be used? What guardrails has Google incorporated through product license terms to prevent over-reliance on the output?

Sincerely,



Mark R. Warner
U.S. Senator

⁸ Singhal, Karan, Shekoofeh Azizi, Tao Tu, S. Sara Mahdavi, Jason Wei, Hyung Won Chung, Nathan Scales, et al. "Large Language Models Encode Clinical Knowledge." *Nature* 620, no. 7972 (August 2023): 172-80. <https://doi.org/10.1038/s41586-023-06291-2>.

Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility?

ETHICAL

- Regulation
- Privacy
- Mitigation of Bias
- Transparency
- Relevance



LEGAL

- Governance
- Confidentiality
- Liability
- Accuracy
- Decision Making

HHS Trustworthy AI for Patient – Centered Outcomes Research:

| TAI Principle and Description ³ | Consequences of Nonalignment ³⁰ |
|--|--|
| <p>Fair/Impartial AI applications should include checks from internal and external stakeholders to help ensure equitable application across all participants.</p> | <p>Algorithms based on data that are inherently biased can result in research conclusions that perpetuate health inequities and that produce or reinforce negative health outcomes that disproportionately impact one group over another.</p> |
| <p>Transparent/Explainable All relevant individuals should understand how their data is being used and how AI systems make decisions; algorithms, attributes, and correlations should be open to inspection.</p> | <p>Lack of transparency can result in algorithmic systems that are hard to control, monitor, and correct (that is, the “black box” issue) and will result in lack of trust from key stakeholders and the public.</p> |
| <p>Responsible/Accountable Policies should outline governance and who is held responsible for all aspects of the AI solution (for example, initiation, development, outputs, decommissioning).</p> | <p>If responsibility for algorithmic systems is unclear, and if harm results from use of the algorithms, it will be difficult to know who to hold responsible for addressing and preventing further harm.</p> |
| <p>Robust/Reliable AI systems should have the ability to learn from humans and other systems and produce accurate and reliable outputs consistent with the original design.</p> | <p>Algorithms that are unreliable and/or inaccurate have a higher chance of producing research conclusions that are incorrect, which may harm patients and result in negative health outcomes, further eroding stakeholder and public trust.</p> |
| <p>Privacy The privacy of individuals, groups, or entities should be respected, and their data should not be used beyond its intended and stated use; data used has been approved by the data owner or steward.</p> | <p>If patients feel that their privacy was violated, they are unlikely to participate in research and may mistrust the health care system.</p> |
| <p>Safe/Secure AI systems should be protected from risks (including cyber) that may directly or indirectly cause physical and/or digital harm to any individual, group, or entity.</p> | <p>If access to protected patient information is compromised, information may be exploited by unauthorized entities; as a result, the organization using the AI system may lose credibility.</p> |

AI Needs Patient Data – How to Apply HIPAA

Under HIPAA, a business associate only may use or disclose PHI:

- As permitted or required by its business associate agreement (BAA); and
- In a manner compliant with HIPAA if done by the covered entity (two exceptions but not relevant for our analysis regarding AI).

If Permitted by the BAA, the business associate may:

- Use and disclose PHI for its proper management and administration; and/or
- Use PHI for data aggregation to support covered entities' health care operations.

A business associate may use PHI to create de-identified information (unrelated to providing the services) if expressly permitted in the BAA.

- Sometimes the BAA will permit the BA to use PHI to perform data aggregation.

HIPAA – Treatment, Payment and Healthcare Operations

| Treatment | Payment | Healthcare Operations |
|--|---|---|
| <p>AI assistance with diagnosis</p> <p>AI assistance with recording and summarizing patient encounters</p> | <p>AI assistance with medical coding for an individual</p> <p>AI assistance with processing health care claims for submission to payors</p> | <p>AI assistance with analysis of patient population for quality improvement</p> <p>AI assistance with reviewing coding errors.</p> |

HIPAA and Research in the Context of AI



Defining “Research” - be careful

—

Research means a systemic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge



HIPAA permits a business associate to use and disclose PHI for research if:

Expressly permitted by the BAA
Permitted by HIPAA for the covered entity’s purposes

- IRB or privacy board’s waiver of HIPAA authorizations

“Sale of PHI” and AI



Under HIPAA there is a general prohibition on the sale of PHI.



Sale of PHI is considered a disclosure of PHI by a covered entity or a business associate where the covered entity or BA directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI.

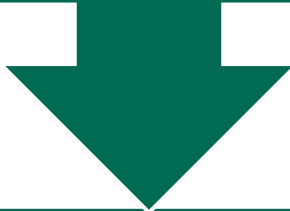
Various exceptions: If otherwise permitted under HIPAA and remuneration is limited to reasonable, cost-based fee to cover the costs to prepare and transmit the PHI.



Sale includes both financial and non-financial remuneration in exchange for access to PHI.

Sensitive PHI and Consents

There are additional restrictions under HIPAA on certain sensitive PHI.



See 42 CFR Part 2 – substance use disorder records

If the AI developer is supporting the healthcare operations of a Part 2 program

- Patient consent, or
- Qualified service organization agreement

If purpose is scientific research

- Patient consent or
- AI developer must be subject to and comply with HIPAA or HHS regulations governing human research protections.

Consents and Authorizations - Confusion

| Washington: My Health My Data | FTC Health Breach Notification Rule | Other Litigations |
|---|--|--|
| <p>Collection: Prior consent is required for specific purpose unless reasonably necessary to provide requested service.</p> <p>Sharing: Prior consent, separate from consent to collection, unless reasonably necessary to provide requested service.</p> <p>Selling: Prior Authorization required, separate from consents</p> | <p>Breach of Security: “acquisition of such information without the authorization of the individual.”</p> <p>FTC considers any unauthorized disclosure to constitute a breach of security, not just those that result from bad actors, cybersecurity incidents.</p> | <p>Potential Causes of Actions:</p> <ul style="list-style-type: none"> - State/federal wiretap laws. - HIPAA - Invasion of privacy - Breach of contract - Breach of fiduciary duty. <p>Pixel cases: allegations that pixel collected information from health care providers and hospital websites, including patient portals.</p> |

HHS's View on Privacy Considerations:

Research and Design | Privacy Principle

Objective: Understand sensitivity of the data and refine the Privacy Impact Assessment

SUPPORTING ACTIVITIES

- ◆ **Refine the Privacy Impact Assessment for Solutions Using Sensitive Data**²⁷
 - ❑ Confirm if the AI solution will use personally identifiable information (PII), protected health information (PHI), business identifiable information (BII), or other sensitive data
 - ❑ Review the preliminary Privacy Impact Assessment from Initiation & Concept to ensure it accurately reflects what information is collected, why it is collected, how it is intended to be used, and with whom it will be shared
 - ❑ Describe what opportunities individuals have to decline to provide information
 - ❑ Explain how the information will be secured, drawing on the [Data Protection and Secure Integration Plan](#)
 - ❑ Indicate whether a System of Record is being created under the Privacy Act of 1974
 - ❑ Describe what potential risks to individuals are posed by the AI solution and what mitigation strategies are in place
- ◆ **Obtain Approval for the Use of Sensitive Data**
 - ❑ Provide justification for the use of sensitive data
 - ❑ Obtain necessary approvals according to applicable Op/StaffDiv data privacy policies
- ◆ **Identify Applicable Laws and Regulations**
 - ❑ Identify and document privacy laws and regulations that would be applicable to the AI application
 - ❑ Validate that the model design is consistent with the identified laws and regulations

KEY CONCEPTS

PII³⁹
Information that can be used to distinguish an individual's identity

PHI⁴⁰
Individually identifiable information relating to the health status of an individual

BII⁴¹
Trade secrets and commercial or financial information obtained from a person that is privileged or confidential

WHY IT MATTERS: IN ACTION

In research and design for an AI solution identifying patients at high-risk for cardiovascular disease, a Privacy Impact Assessment wasn't completed. Consequently, important privacy components were missed during the subsequent development stage and **patients' sensitive privacy information was leaked.**

● Applicable to Pre-Trained Algorithms ◆ Applicable to Custom Algorithms

FTC Joint Statement on AI

FTC Chair Khan and Officials from DOJ, CFPB and EEOC Release Joint Statement on AI

April 25, 2023



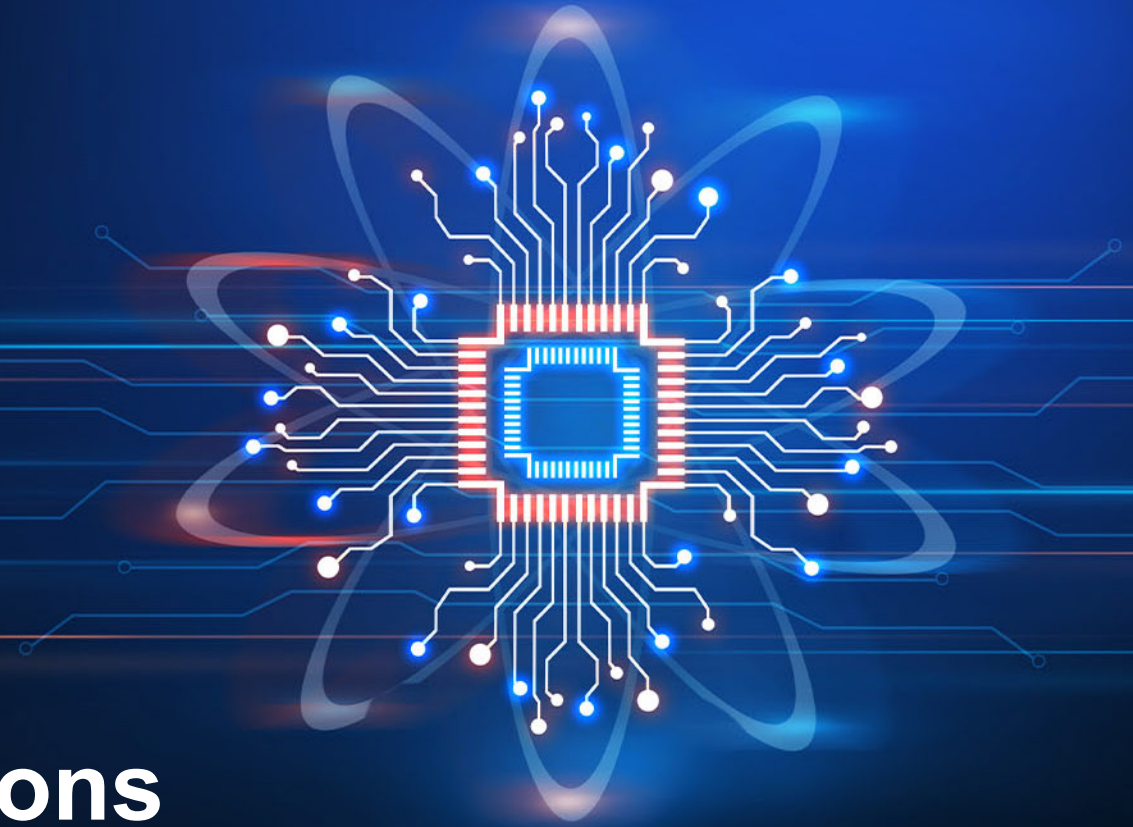
- “Existing legal authorities apply to the use of automated systems and innovative new technologies just as they apply to other practices.”
- “The FTC are among the federal agencies responsible for enforcing civil rights, non-discrimination, fair competition, consumer protection, and other vitally important legal protections.”
- “Many automated systems rely on vast amounts of data to find patterns or correlations, and then apply those patterns to new data to perform tasks or make recommendations and predictions. While these tools can be useful, they also have the potential to produce outcomes that result in **unlawful discrimination.**”
 - Potential discrimination can come from different sources.
 - Examples: Unrepresented or imbalanced datasets; “black box” and opacity issues; AI designs that do not account for private or public usage;



Prior FTC Enforcements: “Algorithmic Justice”

- *In re Kogan and Nix*, Nos. 182 3016 (Agreement Dec. 18, 2019) (former app developer that with Cambridge Analytics and its former CEO enabled app to collect Facebook data from users and friends; among other things, settlement required defendants to **delete or destroy any personal information collected from consumers via the app and any related work product that originated from the data**).
- *In re Everalbum, Inc.*, No. C-4743 (Decision and Order May 6, 2021) (photo app developer settled FTC allegations that it deceived consumers about its use of facial recognition technology and its retention of the photos and videos of users who deactivated their accounts; as part of the proposed settlement, Everalbum must, among other things, **delete models and algorithms it developed by using the photos and videos uploaded by its users**)
- *U.S. v. Kurbo Inc.*, No. 22-00946 (N.D. Cal. Stipulated Order Mar. 3, 2022) (settlement order requires WW International and Kurbo to delete personal information illegally collected from children under 13 and **destroy any algorithms derived from the data**)

AI in Health Care Cybersecurity Considerations



Surge in Hospital Hacks Endangers Patients, Cyber Official Says

Hundreds of attacks on healthcare organizations this year have breached data on over 61 million people, and forced hospitals to turn patients away

By *Kim S. Nash*

Sept. 7, 2023 5:05 pm ET | WSJ PRO

Corporate parent of two major Mass. health insurers hit by cybersecurity attack

Point32Health, the parent company of Harvard Pilgrim Health Care and Tufts Health Plan, was recently affected by a ransomware attack.

Healthcare Governance Body Warns Hospitals Face Debilitating Cyberattacks

Hospitals should prepare for downtime of a month or more, according to new cybersecurity guidelines from the Joint Commission

CommonSpirit took \$150M hit from ransomware attack

Laura Dyrda (Twitter) - Thursday, February 16th, 2023

Cybersecurity and Patient Safety

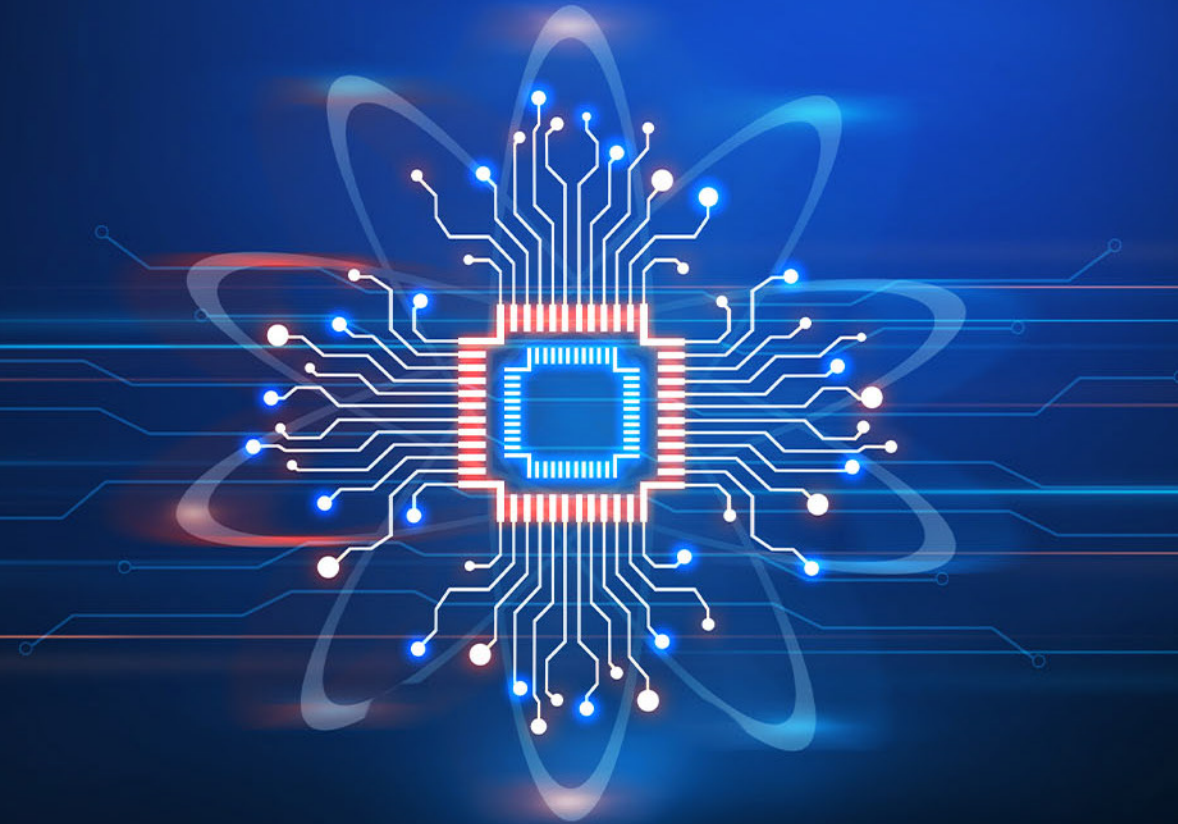


- Ransomware attacks in healthcare affect every aspect of an organization but most importantly it can impact patient safety.
- An attack can:
 - Shut down health care facilities
 - Delete and destroy patient health information and medical records
 - Disrupt a patient's continuity of care

Artificial Intelligence in Healthcare: Security Concerns

- Artificial Intelligence is not inherently insecure, but...
- Artificial Intelligence requires the gathering of very large collections of data in order to learn
 - Privacy and security concerns regarding personal health information (PHI)
 - U. California at Berkeley 2019 study: [Artificial intelligence advances threaten privacy of health data](#)
 - Therefore, data needs to be protected at rest and in motion:
 - Data repository security
 - End-to-end encryption and multi-factor authentication
- Artificial Intelligence allows for the re-identification of [de-identified data](#)
- Repurposing of research data must be done with consideration for de-identification
- Confidentiality is very important in protecting the health sector from AI technologies

Conclusion



Case Study – Generative AI & Healthcare

Generative AI potential uses in healthcare

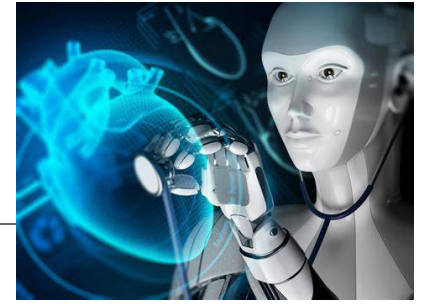
- Assistance with coding and billing and administrative tasks
- Producing routine insurance/benefits notices or forms
- Integrate generative AI into EHR software to enhance natural language queries and data analysis and spot trends in medical records (in the aggregate).

Could cancer be diagnosed from the sound of a voice?



A \$14 million research project is getting underway in the US to

Case Study – Generative AI & Healthcare



Potential Risks

- Automation bias and potential discrimination against patients based on race, gender, etc.
- Producing misleading, inaccurate or correct-sounding (but incorrect) output
- Not yet suitable for diagnostic or medical treatment suggestions
- Data security: Concern over additional sensitive medical records and possible sharing/transmittal of patient data or data being used to train AI system
- Privacy: Concern about how new AI-powered systems will use patient data

Some Final Questions to Consider



- How transparent does a company have to be regarding its use of generative AI applications when it comes to processing consumer data?
- Are there more privacy compliance concerns re: AI automated decision-making in products or services?
- Should every company that intends to use generative AI and related technologies update an existing privacy program to meet the privacy questions of AI?
- Should a company monitor internal use of generative AI (mapping its uses and cataloguing them) to prepare for privacy issues or potential compliance issues in the future (e.g., knowing the extent and types of business uses)?

Ryan P. Blaney

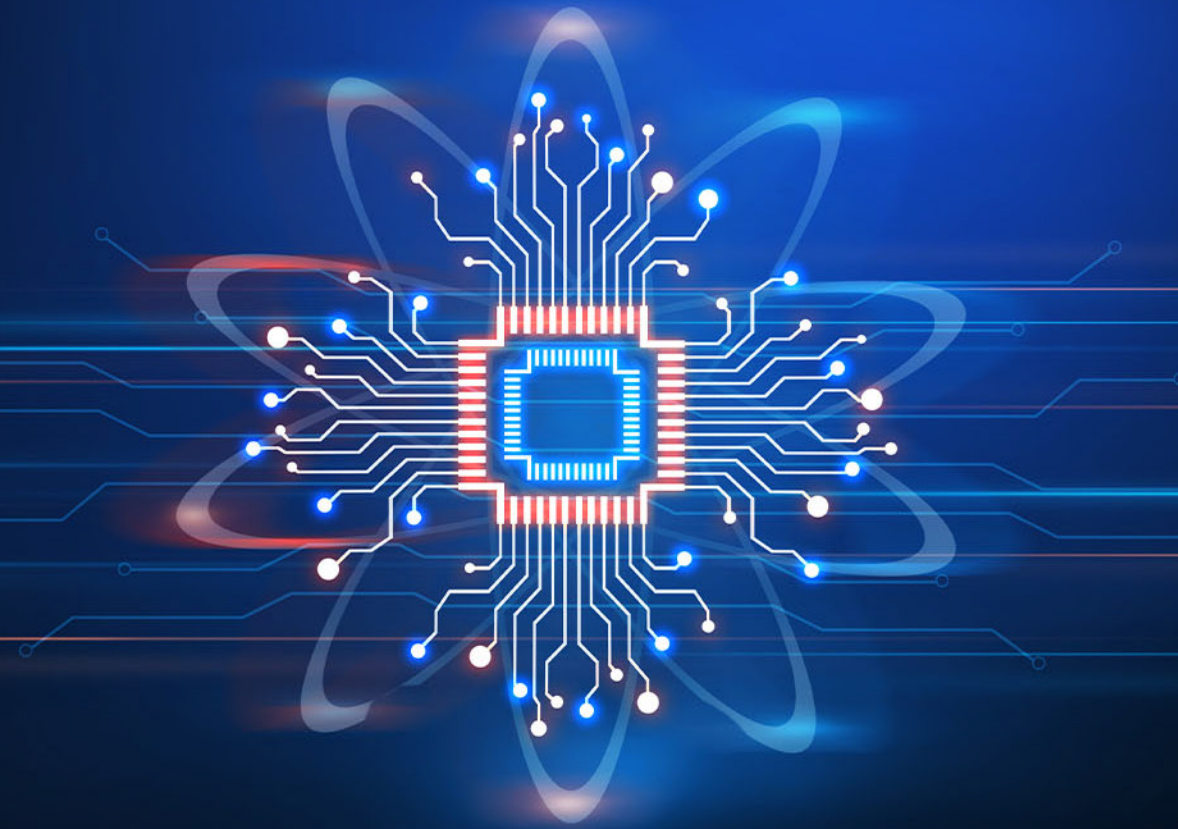
Partner, Co-Head of Privacy & Cybersecurity

Proskauer Rose LLP

rblaney@proskauer.com

Office: 202-416-6815

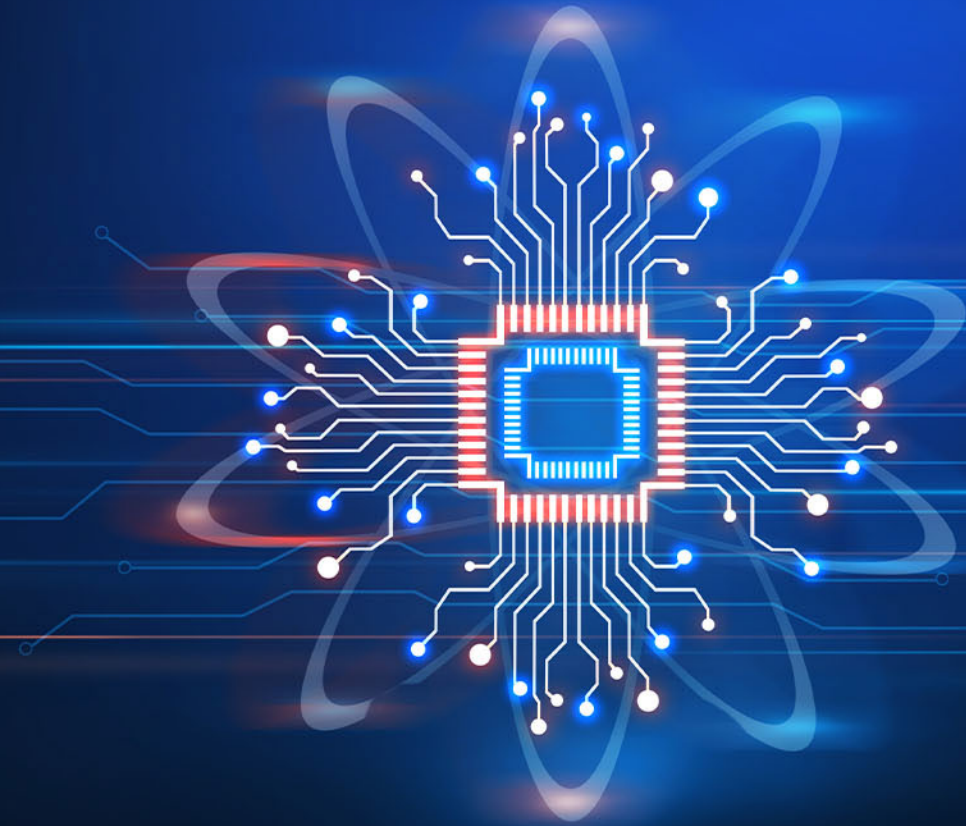
Mobile: 732-604-2028



Thank You

Department of Homeland Security Resources and Other Helpful Links

- <https://www.cisa.gov>
- <https://www.us-cert.gov/Ransomware>
- https://www.us-cert.gov/sites/default/files/2019-08/CISA_Insights-Ransomware_Outbreak_S508C.pdf
- <https://www.cisa.gov/cyber-essentials>
- <https://www.us-cert.gov/report>
- <https://www.dhs.gov/be-cyber-smart>
- <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8963864/>
- <https://www.hhs.gov/about/agencies/asa/ocio/ai/use-cases/index.html>



Proskauer»

The information provided in this slide presentation is not intended to be, and shall not be construed to be, either the provision of legal advice or an offer to provide legal services, nor does it necessarily reflect the opinions of the firm, our lawyers or our clients. No client-lawyer relationship between you and the firm is or may be created by your access to or use of this presentation or any information contained on them. Rather, the content is intended as a general overview of the subject matter covered. Proskauer Rose LLP (Proskauer) is not obligated to provide updates on the information presented herein. Those viewing this presentation are encouraged to seek direct counsel on legal questions. © Proskauer Rose LLP. All Rights Reserved.