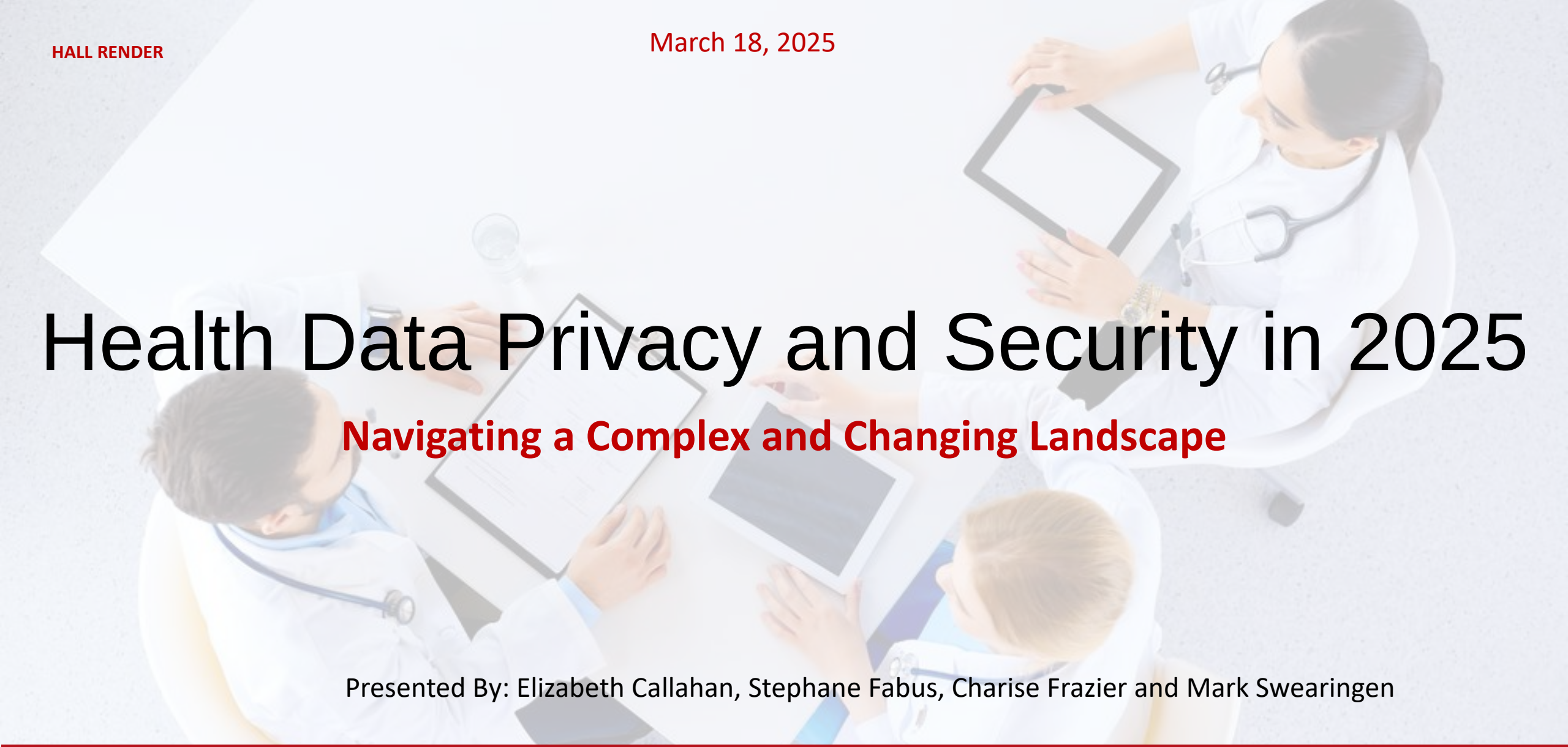
March 18, 2025



Health Data Privacy and Security in 2025

Navigating a Complex and Changing Landscape

Presented By: Elizabeth Callahan, Stephane Fabus, Charise Frazier and Mark Swearingen

Legal Disclaimer

- This presentation is for educational purposes only.
- The contents of this presentation are not to be considered legal advice.

Hall Render Presenters

Elizabeth Callahan

Shareholder
ecallahan@hallrender.com

Stephane Fabus

Shareholder
sfabus@hallrender.com

Charise Frazier

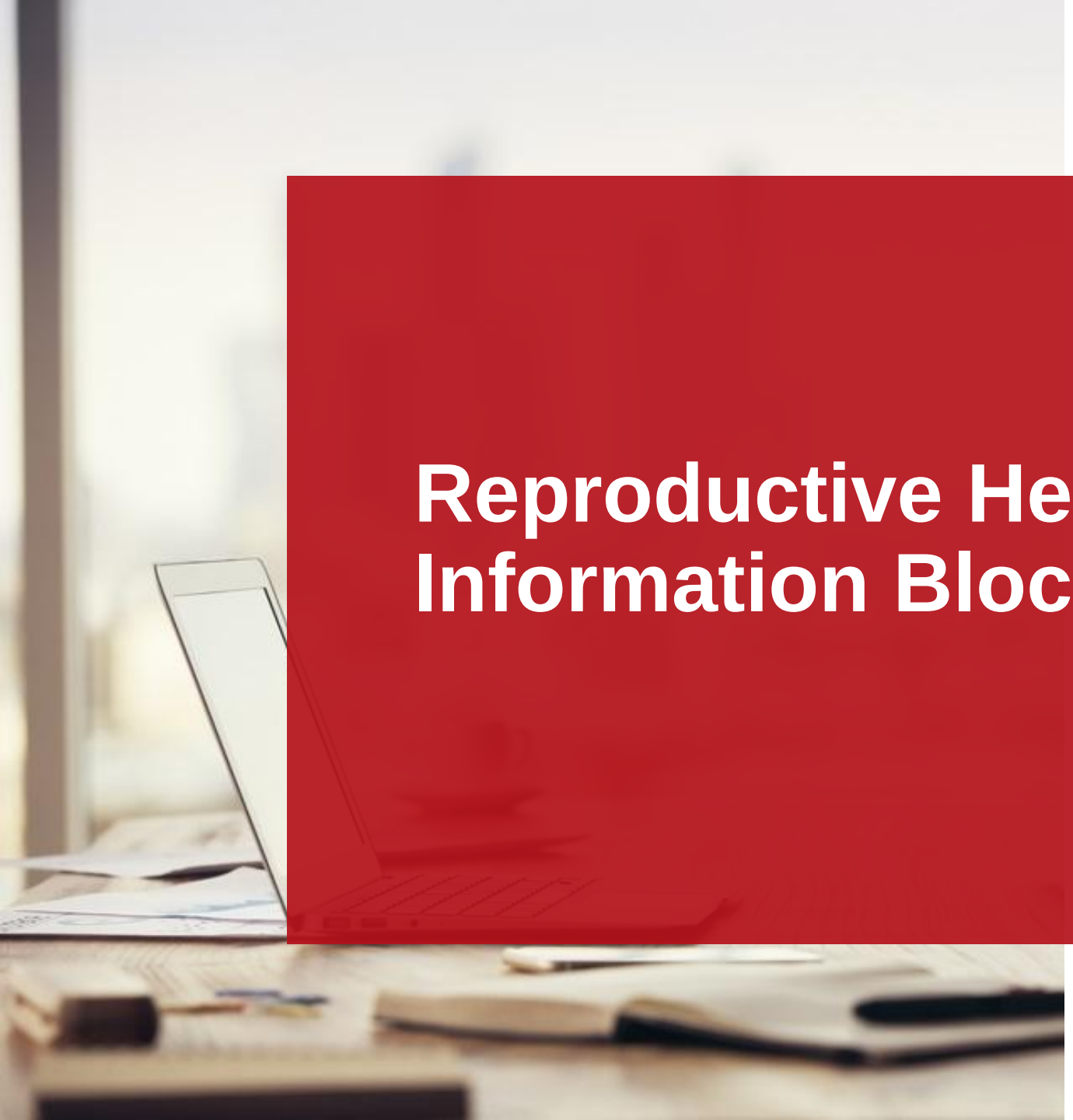
Shareholder
cfrazier@hallrender.com

Mark Swearingen

Shareholder
mswearingen@hallrender.com

Agenda

- Introduction
- Reproductive Health and Information Blocking
- Interactions with Law Enforcement
- Artificial Intelligence
- Web Tracking Technologies
- HIPAA Security Rule Proposed Changes
- Data Breach and Enforcement Update
- Questions and Closing



Reproductive Health and Information Blocking

HIPAA Final Rule on Reproductive Health

- **Published by OCR**: On April 26, 2024, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) released the HIPAA Privacy Rule to Support Reproductive Health Care Privacy ("Final Rule")
- **Executive Order Response**: Initiated in response to President Biden's directive following the Supreme Court's *Dobbs v. Jackson Women's Health* decision, which returned abortion regulation to state jurisdiction
- **Context and Purpose**: The Final Rule aims to enhance patient confidentiality for reproductive health services by limiting how Protected Health Information (PHI) related to lawful reproductive health care can be used or disclosed.

Four Major Requirements

Prohibition: Regulated entities cannot identify a person or use or disclose PHI to investigate or impose liability on any person for seeking, obtaining, providing, or facilitating lawful reproductive health care

Presumption: The reproductive health care is presumed lawful unless the regulated entity has actual knowledge that it was not lawful or received information from the requestor demonstrating a substantial factual basis that it was not lawful

Attestation: If a request for purposes of health oversight activities, judicial and administrative proceedings, law enforcement purposes, or coroner and medical examiner responsibilities and would include PHI potentially related to reproductive health care, prior to disclosure, the regulated entity must obtain a signed attestation that the use or disclosure is not for a prohibited purpose

Notice of Privacy Practices: NPP must provide individuals with information about how their reproductive health care PHI may or may not be disclosed pursuant to the final rule, including descriptions and examples of the prohibition and attestation requirements. NPP must also include a statement explaining that PHI disclosed pursuant to the Privacy Rule may be subject to redisclosure and no longer protected.

Attestation Requirements for PHI Disclosure

- **Attestation Mandate**: Covered entities **must** obtain a signed attestation from the requesting party before disclosing PHI when the request relates to:
  - Health oversight activities;
  - Judicial and administrative proceedings;
  - Law enforcement purposes; and
  - Disclosures to coroners and medical examiners.
- **Purpose of Attestation**: Requires the requestor to attest that the requested PHI will not be used or disclosed for the prohibited purpose of investigating or imposing penalties for lawful reproductive health care. The attestation must confirm that the request is lawful and not in violation of reproductive health privacy protections. It also informs the requestor of the potential for criminal penalties
- **Key Elements**: A valid attestation must be clear, in plain language, and not contain unnecessary statements beyond HIPAA requirements. OCR provided a model form for this purpose, which can be electronically signed if it meets e-signature standards.

Implementation Steps

- **Review PHI Policies**: Identify any PHI flagged as reproductive health-related and update privacy policies accordingly.
- **Staff Training**: Train workforce on the restrictions for PHI disclosure, particularly for front-line staff and those handling law enforcement requests.
- **Business Associate Agreements**: Update agreements to include attestation requirements and ensure compliance in data exchanges.
- **Notice of Privacy Practices Update**: Ensure that the NPP reflects new requirements, including examples of prohibited disclosures and uses, as well as any attestation requirements.

Pending Challenge

- On September 4, 2024, Texas Attorney General Ken Paxton sued HHS in the Easter District of Texas challenging both the 2024 Reproductive Health Privacy Final Rule and 2000 Standards for Privacy of Individually Identifiable Health Information Final Rule for interfering and limiting disclosures to state officials and law enforcement under 45 CFR 164.512(f)(1)(ii)(C)
- The arguments:
  - HIPAA statute explicitly preserves state investigative authority, and thus, the rules are contrary to the statute
  - HIPAA statute gives HHS no authority to promulgate rules limiting how regulated entities may share information with state governments
  - The rules lack statutory authority and are arbitrary and capricious
- It seeks declaratory and injunctive relief vacating and setting aside the rules and enjoining enforcement of them

Related Information Blocking Exception: Protecting Care Access Exception

- Practice **implemented to reduce potential exposure to legal action** will not be considered information blocking.
- **Four Requirements**:
  - **Belief**. The practice is undertaken based on the actor's good faith belief that: (i) Persons seeking, obtaining, providing, or facilitating reproductive health care are at risk of being potentially exposed to legal action that could arise as a consequence of particular access, exchange, or use of specific electronic health information; and (ii) Specific practices likely to interfere with such access, exchange, or use of such electronic health information could reduce that risk.
  - **Tailoring**. The practice is no broader than necessary to reduce the risk of potential exposure to legal action that the actor in good faith believes could arise from the particular access, exchange, or use of the specific electronic health information.
  - **Implementation**. The practice is implemented either consistent with an organizational policy that or pursuant to a case-by-case determination that meet certain requirements set forth in the regulations
  - **Another actor's reliance on good faith belief**. For purposes of this section, an actor who is a business associate of, or otherwise maintains EHI on behalf of, another actor may rely on the good faith belief and organizational policy or case-by-case determinations of the actor on whose behalf relevant EHI is maintained.
- Must either be:
  - Intended to reduce the ***patient's risk*** – limited to applicable information and be subject to patient nullification; or
  - Intended to reduce the ***health care provider's risk*** – limited to applicable information

Interactions with Law Enforcement

HIPAA Regulations

1. ***Pursuant to process and as otherwise required by law***
   - Required by law reporting of wounds and injuries
   - Court orders, judicial subpoenas or summons, grand jury subpoenas, or administrative requests ***for which a response is required by law***
2. ***Limited information for identification and location purposes***
   - In response to request and limited to certain information
3. ***Victims of a crime***
   - In response to a request, if the individual agrees or (if individual is incapacitated) it is in their best interests
4. ***Decedents***
   - To report a suspicious death believed to be caused by criminal conduct
5. ***Crime on premises***
   - To report a crime on the covered entity's premises
6. ***Reporting crime in emergencies***
   - To alert law enforcement to crime is responding to an off-premises medical emergency

45 C.F.R. § 164.512 (f) **Standard: Disclosures for law enforcement purposes.**

Interacting with Law Enforcement

- **Updating policies and procedures.**
  - When is disclosure permissible?
  - How will you handle law enforcement presenting on site?
  - How will you obtain required consents or attestations?
  - What is staff's role in the process?
  - What safeguards are in place to limit disclosures and ensure high quality care?
- **Assigning an individual as the designated law enforcement liaison**.
  - Coordinate with a cross-functional response team, including legal, compliance, security and senior leadership, to provide support.
  - Receive specific training and resources on compliant interactions with law enforcement.
- **Assessing data collection procedures.**
  - What data do you collect and have in your possession?
  - What options are available in HIT systems to flag, identify, suppress certain data elements?
  - Be aware of litigation holds and limitations on destruction of data.
- **Ensuring regulatory compliance.**
  - Minimum necessary requirements
  - Include in any accounting of disclosures
  - Document any interaction with law enforcement.

Navigating Immigration Enforcement in Health Care Settings

- Jan 2025 – DHS rescinds “Protected Areas” policy
- This policy previously restricted ICE and CBP from entering certain locations, including **medical facilities**, schools and places of worship

FAQs re ICE Interactions

- What areas in a hospital may ICE agents enter?
  - Public v. nonpublic areas
- What information may be disclosed?
  - Analyze warrant, subpoena, or other request
- What are best practices?
  - Designate liaison / response team
  - Review law enforcement policies and procedures
  - Conduct I-9 audits

Artificial Intelligence

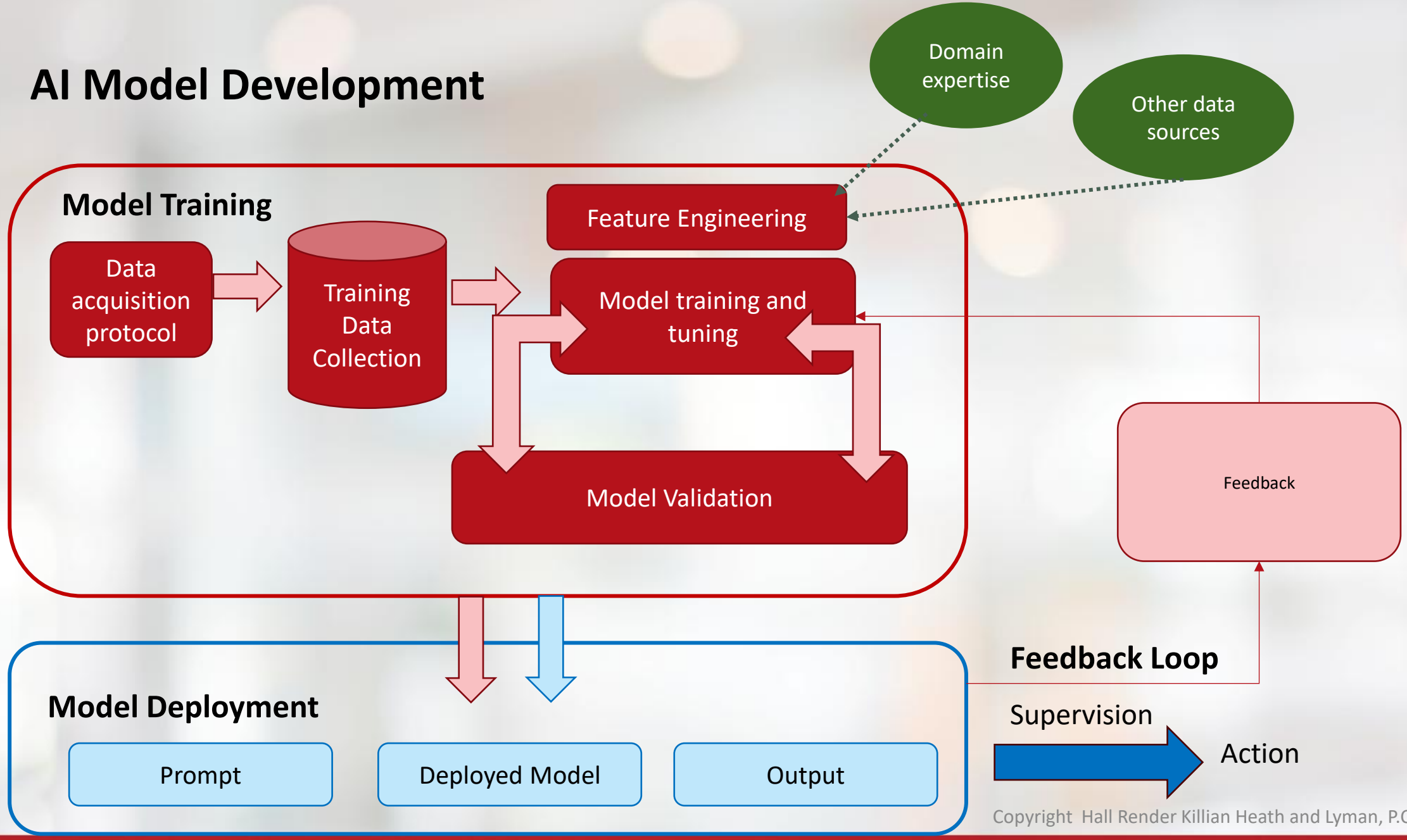
What is Artificial Intelligence?

- Artificial intelligence generally refers to computer technology with the ability to simulate human intelligence. AI is a category of software and not a thing.
- AI thinks in probabilities.
- AI cannot distinguish probability from causation.
- AI can only anticipate based on the known world. It cannot process in the absence of a reference point.
- Artificial intelligence can do amazing things that humans can't, but in many cases, we have no idea how AI systems make their decisions.– "black box problem" UM-Dearborn Associate Professor Samir Rawashdeh, March 6, 2023

Deep learning Generative AI

- Generative AI is a type of Artificial Intelligence that creates new content based on what it has learned from existing content
- The Process of learning from existing content is called training
- Training is the use of known data to create the ability for the machine to create new outputs that are within statistical acceptable levels without errors (hallucinations)
- When given a prompt a Generative AI model uses the statistical model to predict what is an expected response
- Results can be language, images or video

AI Model Development



The Hidden Data

- What data is used to train the AI tool?
- What data is input into the model?
- What data does the enterprise collect about how individuals are interacting with AI tools?

AI and Privacy

- The rapid growth of AI doesn't necessarily present new privacy risks
- The primary difference is the scope and scale of the risk
- AI is data-driven, so precautions must be taken to protect personal and sensitive information
- There are documented cases of regulators challenging the development of AI tools by health care organizations
- Organizations must be thorough, thoughtful, and deliberate in order to effectively protect PHI and PII in the age of fast-developing AI
- Organizations should develop an AI governance model

Web Tracking Technologies


What we see
Information sent to technology organizations

Tracking Technologies - Background

- June 2022 - Article in *The Markup* suggested that the Meta Pixel tracker was unwittingly sharing PHI with tracking technology vendors
- Over the next several months, OCR began investigations and a handful of health care organizations notified patients of breaches due to the presence of the Meta Pixel in their patient portals
- OCR issued a bulletin regarding the use of tracking technologies in December of 2022, which it updated in March of 2024.
- In late 2023, the AHA lead a group of plaintiff organizations that sued HHS to enjoin enforcement of the bulletin and seek a declaratory judgment that IP addresses are not IIHI under HIPAA.
    - OCR issued the amended guidance as a means of appeasing the plaintiffs and prompting them to dismiss the case, but the revised guidance created more questions than it answered by creating a standard that based the IIHI determination on the subjective intent of a website visitor.
    - In June of 2024, a federal court in Texas declared parts of the OCR bulletin unlawful and vacated them. The remainder of the Bulletin was left intact.

Tracking Technologies - Currently

- Federal and state regulators still have open investigations, but activity has waned
- FTC enforcement actions - 2023
  - Prescription savings services - $1.5M settlement
  - Online mental health and counseling - $7.8M and $1.5M
  - Fertility app - $200K settlement
- NY AG - 2023
  - Health system - $300K settlement
- Current emphasis on deregulation at the federal level and in some states adds to the uncertainty

Tracking Technologies - Currently

- Class action lawsuits are where the action is
- There are innumerable class actions across the country against health care organizations alleging the improper use of tracking technologies
  - Those cases currently are in a variety of procedural stages, and none have yet gone to trial on the merits
  - There have been a few public settlements to date:
    - A Wisconsin health system settled for $2M in July of 2023.
    - An Illinois health system settled for $12.25M in August of 2023.
    - A North Carolina health system settled for $6.6M in January of 2024.
  - Based on the current environment, there likely will be more public settlement in the months and years ahead.

Tracking Technologies – Next Steps

- Take Inventory, assess risk, and implement appropriate governance
- Establish a cross-functional team responsible for collecting an inventory of web tracking tools AND the data that is collected by each tool
- Develop a process to audit/monitor web presences on an ongoing basis
- Incorporate web tracking into your regular HIPAA Security Risk Analysis
- Enter into BAAs with all tracking technology vendors who will receive PHI
- Ensure website privacy policies are consistent with reality
- Be mindful of tracking technology use by vendors that offer browser-based solutions

HIPAA Security Rule Proposed Changes

HIPAA Security Rule NPRM

- Near the end of December, HHS issued an NPRM regarding potential changes to the HIPAA Security Rule
- The status of the rule is unknown given the freeze that the Trump administration put on any proposed rules from the Biden administration
- The proposed changes would be significant. Notable changes include:
  - Remove the distinction between “required” and “addressable” standards
  - Require a technology asset inventory and network map showing the movement of PHI throughout a regulated entity’s electronic systems that is updated every 12 months.
  - More specific requirements for conducting a risk analysis

HIPAA Security Rule NPRM

- Notable changes (cont.):
  - Strengthen requirements for contingency planning and incident response, including timelines and prioritization for restoration and periodic testing
  - Require regulated entities to conduct a compliance audit every 12 months
  - Require business associates to verify for covered entities (and subcontractors for business associates) at least every 12 months that they have deployed technical safeguards
    - written analysis and certification of the business associate's relevant information systems by a subject matter expert
  - require encryption and multi-factor authentication
  - require network segmentation
  - require vulnerability scanning every 6 months and penetration testing every 12 months

Data Breach and Enforcement Update

Data Breach Developments

- Health care organizations are still popular targets for cyber criminals
- Recently leaked communications from health care cyber attacks have shown some hesitancy to impact patient care but no material decrease has occurred to date
  - Threat actors often do not understand the complexities and interrelationships of the health care system
- The Change Healthcare incident is still playing out
  - Change sent an initial round of notices to approximately 100 million individuals late last year that didn't identify any covered entities
  - Change is now reaching out to covered entities and offering to send letters to additional individuals that identify the covered entity involved
  - Carefully review this information and consider the proper approach for your organization
- Vendor breach incidents are continuing to occur with regularity

HIPAA Enforcement Update

- OCR was very active at the end of the Biden administration, issuing 13 enforcement actions in the last 3 months alone
- Wide variety of cases and penalty amounts
  - Entity types included hospitals, physician practices, a medical equipment supplier, a business associates, and even a health care clearinghouse.
  - Focus on right of access cases over the past several years (53)
  - Perhaps shifting more toward security risk analysis initiative and ransomware investigations
  - Resolution/penalty amounts ranging from $10,000 to $3,000,000
- Failure to conduct an enterprise-wide risk analysis is still the most commonly cited deficiency in cases involving the Security Rule
- The pace and focus for OCR enforcement is uncertain under Trump

Questions?

Please visit the Hall Render Blog at https://www.hallrender.com/resources/blog/ for more information on topics related to health care law.

Stephane P. Fabus

Hall, Render, Killian, Heath & Lyman, P.C.
330 E. Kilbourn Ave., Suite 1250
Milwaukee, WI 53202
sfabus@hallrender.com

Charise Frazier

Hall, Render, Killian, Heath & Lyman, P.C.
500 N. Meridian Street
Suite 400
Indianapolis, IN 46204-1293
cfrazier@hallrender.com

Mark J. Swearingen

Hall, Render, Killian, Heath & Lyman, P.C.
500 N. Meridian Street
Suite 400
Indianapolis, IN 46204-1293
mswearingen@hallrender.com

Elizabeth Callahan

Hall, Render, Killian, Heath & Lyman, P.C.
101 W. Big Beaver Road,
Suite 745, Columbia Center
Troy, MI 48084
ecallahan@hallrender.com