HALL RENDER
KILLIAN HEATH & LYMAN
HEALTH CARE UNINTERRUPTED

Artificial Intelligence and Advanced Technologies

Understanding the risks and impact on healthcare organizations

MEDICAL STAFF SEMINAR 2025

Empowering Medical Staff. Enabling Excellence.

DECEMBER 4-5, 2025

HALL RENDER
KILLIAN HEATH & LYMAN
HEALTH CARE UNINTERRUPTED

Presenter Info

Michael Batt
Attorney, Hall Render
mbatt@hallrender.com
(317) 977-1417

Agenda

- What is new?
- What are we talking about?
- Why do we care?
- What should we be doing?

MEDICAL STAFF SEMINAR 2025

Horror stories

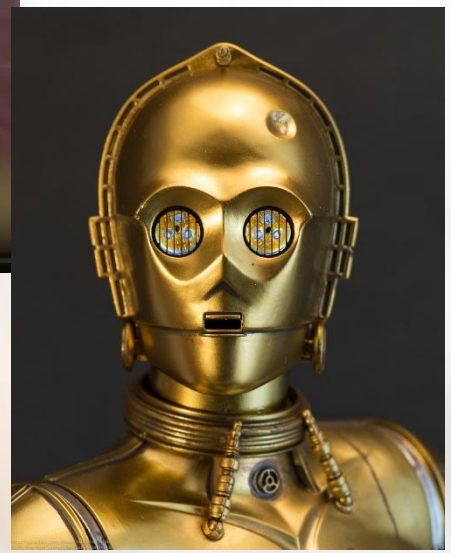
- Physician wears go-pro into surgery.

- Physicians utilizing personal devices with personal app to deliver care.

- AI powered physicians moving faster than reasonable or beyond the scope of their practice

What is new?

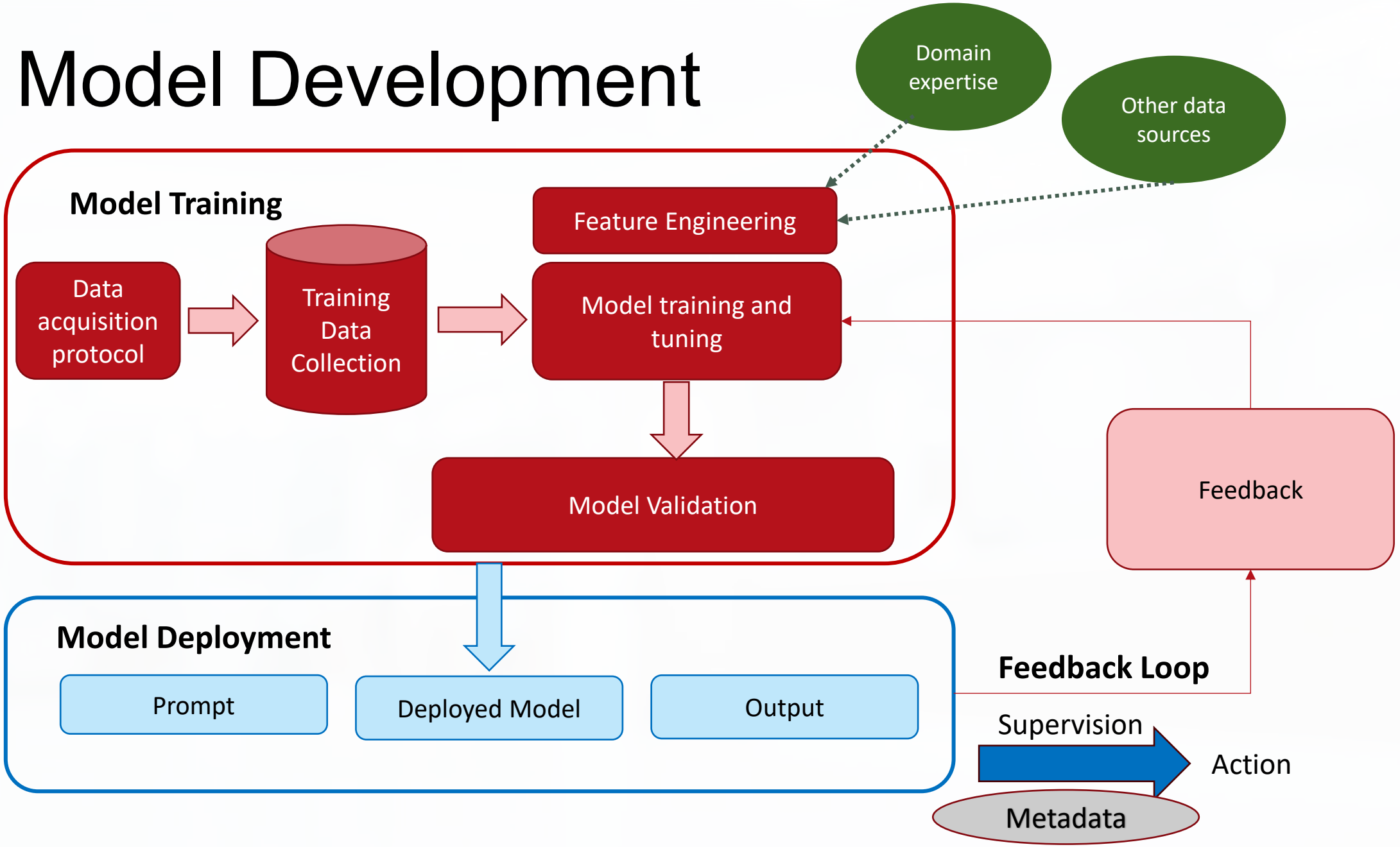
- Artificial Intelligence
  - Discriminative AI
  - Generative AI
  - Agentic AI



Definitions

- Artificial Intelligence or AI: Computer systems that perform tasks mimicking human intelligence, using algorithms and data. This includes understanding language, recognizing patterns, problem-solving, and decision-making, and may involve technologies like machine learning, neural networks, and robotics.
- AI Tool: AI Tool means the technology platform performing the AI function.
- AI System: AI System is the AI Tool as used by the User in a manner consistent with the Use Case.
- Use Case: A Use Case is a specific instance where an AI Tool is used to solve a problem, improve a process, or create something new by a User.
- Hallucination: A hallucination refers to when a machine learning model, especially large language models (LLMs), generates outputs that are inaccurate, misleading, or fabricated, often presented with confidence as if they were true. Essentially, the AI "makes things up" or presents false information as fact.
- Training Data: Training data is the information used to teach machine learning models how to recognize patterns, make decisions, and learn from data. It's a collection of labeled examples, like images with labels for objects or text with tagged sentences, that helps the AI algorithm understand the relationships between input and output.

AI Model Development



Three Major Risk concerns

- Is data access, use, disclosure and retention consistent with legal and policy requirements (traditional IT concerns)?
- Is the output of the AI Tool safe with bias and harm mitigated?
- Does the use of AI create new compliance implications (does the AI function to replace human decision making in prohibited manner? Does the use of AI create new metadata concerns regarding how healthcare services are rendered)?

AI Governance a Brief History

- AI has been used in healthcare for more than a decade.
- Generative Pre-trained Transformer (GPT) in 2019.
- AI Governance prohibited use of GPT models with confidential and patient data.
- Biden 2/16/23 Executive Order on AI raise focus on bias.
- Increased focus on bias and the risks associated with historic discrimination.
- Easy access to GPT tools through mobile devices resulted in significant non-compliance and data leaks.
- AI governance was viewed as a barrier or ignored as workforce members began exploring the potential and vendors raced to the market to be first.
- The demands of clinicians for access to AI Tools created challenges in managing AI Tool access and use to existing IT security and organizational polices.
- Trump 2/20/24 Executive Order repealed Biden EO.
- At present, healthcare organizations are rapidly adopting AI Tools and Use Cases through exploratory pilots and favoring executive governance processes
- The vast majority of these Use Cases rely on a human-in-the-loop to mitigate the impact of a hallucination or error.
- The result is that organizations are now relying on “human-in-the-loop” models to mitigate risk, but may have had little opportunity to develop infrastructure, services and content to support the added responsibility of Users to validate the AI Tool output.

Who is responsible when things go wrong?

- The human (clinician) in the loop.
- AI is a tool. AI does not replace or shift accountability.
- AI cannot perform tasks that require a human or professional license.

The BIG questions:

- Are we confident in the output of the AI tool?
  - Is it safe?
  - What is the consequence of a hallucination or error?
- Is our workforce well positioned to identify errors, hallucinations, or confirm the output?
  - Who is responsible for the AI tool
  - Have we effectively mitigated risks?
- Does the AI tool meet privacy, security and regulatory obligations?
  - From a technology perspective has it been vetted?

Where do we go from here?

Three steps:

- Step 1. Build a framework for engaging the right people at the right time to make informed decisions about AI and its use. The IT review is only part of the equation.
- Step 2. Engage the end user in understanding:
  - a. They are interacting with AI,
  - b. The range of appropriate use of the AI tool,
  - c. How to spot a hallucination, and
  - d. How and to whom to report a concern.
- Step 3. Manage the Metadata:
  - Maintain data only for so long as it has value
  - Ensure compliance with retention policies
  - Peer Review and PSOs when properly engaged can manage data associated with monitoring

Why do we care?

- Standard of Care – Medical Malpractice:
  - The practice of medicine is based on understanding causation. AI relies solely on correlation.
- Healthcare Provider use of Discretion
- Data breach/privacy laws
- Breach of Contract
- Scope of Insurance
- False Claims
- Consumer Protection laws
- IP ownership
- AI specific laws (employment, housing, healthcare, individual profiling)

The BIG questions:

- Are we confident in the output of the AI tool?
- Is our workforce well positioned to identify errors, hallucinations, or confirm the output?
- Does the AI tool meet privacy, security and regulatory obligations?

Now... lets build the process that leverages existing processes, is efficient, predictable and empowers the workforce to pursue innovation and brings understanding to this new tool.

Three steps:

- Step 1. Build a framework for engaging the right people at the right time to make informed decisions about AI and its use.
  - Validate safety
  - Identify risk mitigation
  - Identify accountable person
  - Define monitoring

- Step 2. Engage the end user in understanding:
  - a. They are interacting with AI,
  - b. The range of appropriate use of the AI tool,
  - c. How to spot a hallucination, and
  - d. How and to whom to report a concern.

- Step 3. Review the AI tool consistent with IT policies (Security review, Privacy Review, Technology review).

Risk Framing

- Risk is the composite measure of an event's probability of occurring and the magnitude or degree of the consequences of the corresponding event.
- Risk includes both the internal impact on the organization as well as external third parties, such as patients, employees and individuals.
- Effective risk framing involves an understanding of the risks and the implementation of strategies and frameworks to mitigate and manage these risks throughout the AI lifecycle.

NIST | NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

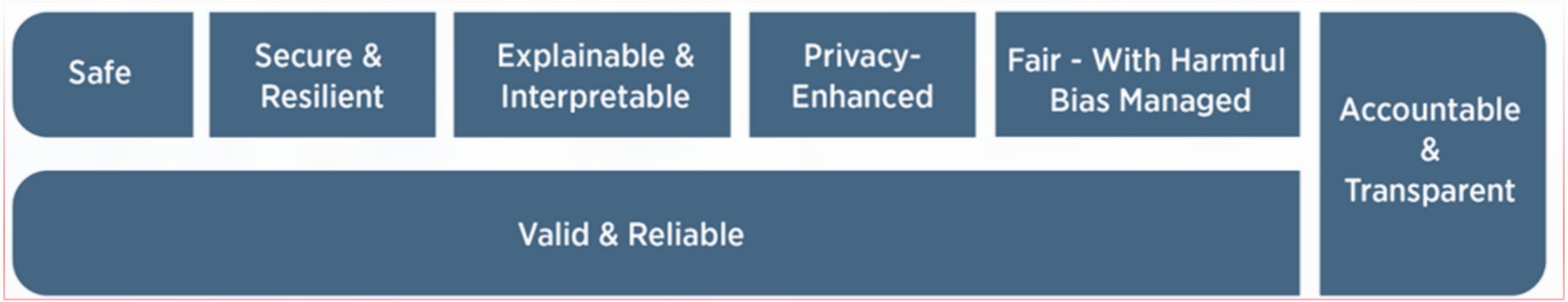
On July 26, 2024, NIST released NIST-AI-600-1, Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. The profile can help organizations identify unique risks posed by AI and proposes actions for AI risk management that best aligns with their goals and priorities.

“Core” of the Framework

- Govern - Policies, processes, procedures and practices across the organization related to the mapping, measuring and managing of AI risks are in place, transparent, and implemented effectively.
- Map – Context is recognized and risks related to context are identified.
- Measure – Identified risks are assessed, analyzed and tracked
- Manage – risks are prioritized and acted upon based on projected impact

NIST AI Risks and Trustworthiness

Characteristics of trustworthy AI systems include: valid and reliable, safe, secure and resilient, accountable and transparent, explainable and interpretable, privacy-enhanced, and fair with harmful bias managed.



Saying it simply…

- AI solutions will function much like an employee with dual reporting obligations.
  - For purposes of whether the AI System is doing a good job, an accurate job, acting without discriminatory bias, the system will be governed by the management structure associated with the workforce it is augmenting.
  - For purposes of whether the AI technology is secure, whether it has appropriate controls on data access and use, etc., the technology will be within the oversight of information services.

AI Governance Model

NIST Risk framework

- Valid and Reliable
- Safe
- Explainable & Interpretable
- Fair – with harmful bias mitigated
- Accountable and Transparent

- Secure & Resilient
- Privacy Enhanced

AI Governance Committee

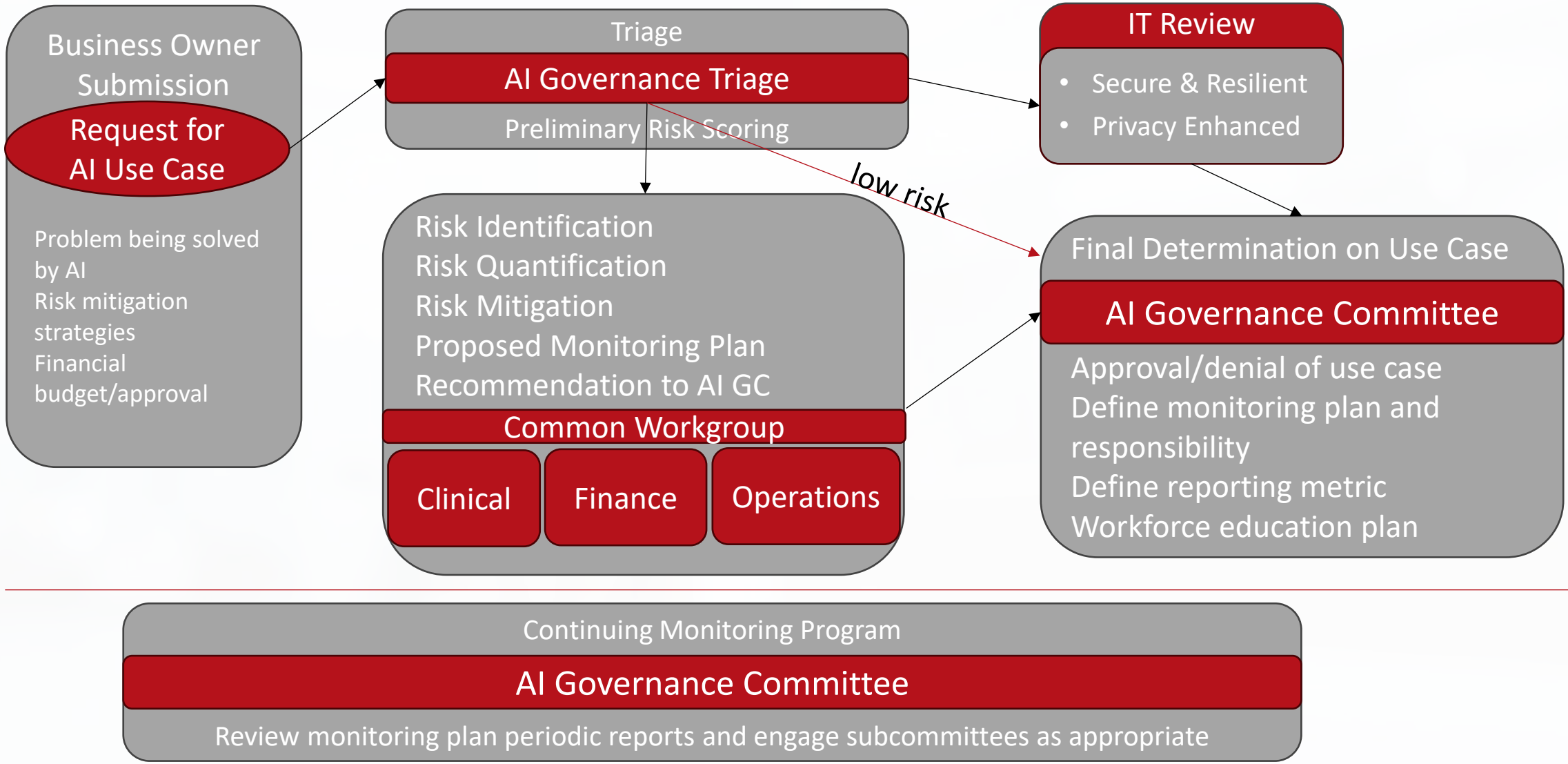
Organizational Education

- Clinical Subcommittee
- Finance Subcommittee
- Operations Subcommittee

Common working groups

- Legal/Compliance
- Medical Staff
- Peer Review/PSO
- Financial Integrity
- Procurement
- IT Review
- Security Review
- Disaster Recovery
- Privacy/ Data Management

Workflow for initial vetting of AI Use Case



Example: Ambient listening for acute care.

[Title] identifies opportunity to reduce time spent by providers documenting patient encounter

Triage Review: CIO, Legal CMIO

Risks

- Hallucinations can impact patient care
- Direct integration to EHR
- Requires Clinical training
- Implications for recording of conversations.

Information Services Review

- Security review of AI tool
- Privacy review of use of transcripts in AI training
- Validates AI Tool is not duplicative of existing AI Tool

AI Governance Committee

- Advises PSO or Peer Review Committee re Use Case
  - identification of meta data on usage
- Defines education plan for Users
- Identifies clinician responsibility for monitoring accuracy of output.
- Defines monitoring plan and maintains records of periodic reports on monitoring.
- Collaborates with periodic security review.

Composed of representatives of Clinical, legal, Compliance, Application (IS)

Clinical Subcommittee Review

- Analysis of accuracy through review of vendor documentation, and pilot of AI tool
- Develop risk mitigation tactics for physician engagement
- (legal) Evaluation of implications for record retention and production

AI Governance Committee (AI-GC)

- The AI-GC is charged with **leading the organization** through the process of adopting AI technology safely and efficiently.
- The AI-GC should provide initial triage of proposed AI Use Case to assess risk, identify expanded use of previously approved AI Tools, and **assign to the appropriate Subcommittee.**
- The AI-GC may determine an AI Use Case presents minimal risk and **bypass** subcommittee.
- The AI-GC may review AI Use Cases that predate AI-GC.
- The AI-GC is ultimately responsible for ensuring **monitoring** plans are being performed and shall coordinate with peer review, PSO and Compliance.

Subcommittee Structure

- The AI Subcommittee structure is used to place the decisions about whether an AI Use Case is safe, reliable and explainable with those most capable of knowing or overseeing a similarly qualified human performing such function (Subject Matter Experts).
- Each Subcommittee is to focus diligence as appropriate based on use case, as examples:
  - Clinical may focus on mapping training data to patient population,
  - Finance may utilize AI testing processes for Coding accuracy, and
  - Operations may heavily scrutinize use cases for bias and compliance with accessibility requirements.

Information Services Review

The Information Services review of an AI Use Case should include an evaluation of the underlying technology consistent with the organizational process for ensuring the integrity, security and efficiency of technology by the organization. The AI technology should, like any other application, be subject to ongoing security monitoring. Information Services may also provide a supporting role to Subcommittees to assist them in understanding the proposed AI Use Case and reporting capabilities in support of ongoing monitoring activities.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

The following slides provide greater explanation of the risk factors identified in the NIST framework

AI Risks and Trustworthiness

- Valid and Reliable
  - *Valid* - confirmation, through objective evidence, that the requirements for the intended use have been fulfilled.
  - *Reliable* – ability of an item to perform as required without failure for a given time interval, under given conditions.
  - *Accuracy* – closeness of the results to the value accepted as being true
  - *Robustness* – ability of the system to maintain its level of performance under a variety of circumstances

- Safe – AI should not be deployed in a manner that endangers human life, health, property or the environment is endangered and should take cues from efforts and guidelines for safety in fields such as transportation and healthcare, and align with existing sector- or application-specific guidelines or standards.

AI Risks and Trustworthiness (Cont.)

- Secure and Resilient –
  - *Resilient* – ability to withstand unexpected adverse events or unexpected changes in its environment or use and degrade safely and gracefully when necessary.
  - *Security* – includes resilience but also encompasses protocols to avoid, protect against, respond to and ability to return to normal function after unexpected adverse event.

- Accountable and Transparent –
  - *Transparency* - reflects the extent to which information about an AI system and its outputs is available to individuals interacting with such a system – regardless of whether they are even aware that they are doing so. This characteristic's scope spans from design decisions and training data to model training, the structure of the model, its intended use cases, and how and when deployment, post-deployment, or end user decisions were made and by whom.
  - *Accountability* – is the allocation of responsibility between the AI developer, the entity making the AI available for use (AI deployer) and the user of the AI.

AI Risks and Trustworthiness (Cont.)

- Explainable and Interpretable –
  - *Explainability* – refers to a representation of the mechanisms underlying the AI systems operations
  - *Interpretability* – refers to the meaning of AI systems' output in the context of their designed functional purposes.

- Privacy – Enhanced: refers generally to the norms and practices that help to safeguard human autonomy, identity, and dignity. These norms and practices typically address freedom from intrusion, limiting observation, or individuals' agency to consent to disclosure or control of facets of their identities. Because AI has the ability to digest and analyze large datasets, privacy considerations include an analysis of what information is relevant to the model output.

AI Risks and Trustworthiness (Cont.)

- Fair – with Harmful Bias Managed:
  - *Fairness* - in AI includes concerns for equality and equity by addressing issues such as harmful bias and discrimination
  - *Bias* - NIST has identified three major categories of AI bias to be considered and managed: systemic, computational and statistical, and human-cognitive. While bias is not always a negative phenomenon, AI systems can potentially increase the speed and scale of biases and perpetuate and amplify harms to individuals, groups, communities, organizations, and society

Key takeaways.

1. AI is subject to existing data privacy and security rules, regulations and policies.
2. An effective human in the loop requires understanding.
3. Metadata must be managed.
4. Peer Review plays an increasing role in ensuring the safe use of AI

MEDICAL STAFF SEMINAR 2025

Questions?

Contact Us

For more information on these topics visit hallrender.com.

Michael Batt

mbatt@hallrender.com

HALL RENDER
KILLIAN HEATH & LYMAN
HEALTH CARE UNINTERRUPTED

This presentation is solely for educational purposes and the matters presented herein do not constitute legal advice with respect to your particular situation.