AI: What to Know and Be Concerned About

KARQM Spring Conference

April 8, 2026

Learning Objectives

- Understand artificial intelligence (AI) terminology necessary for context of risks
- Articulate risks AI introduces for patient care, operations, and compliance/privacy/security
- Identify options to address and reduce AI-related risks

Expectations

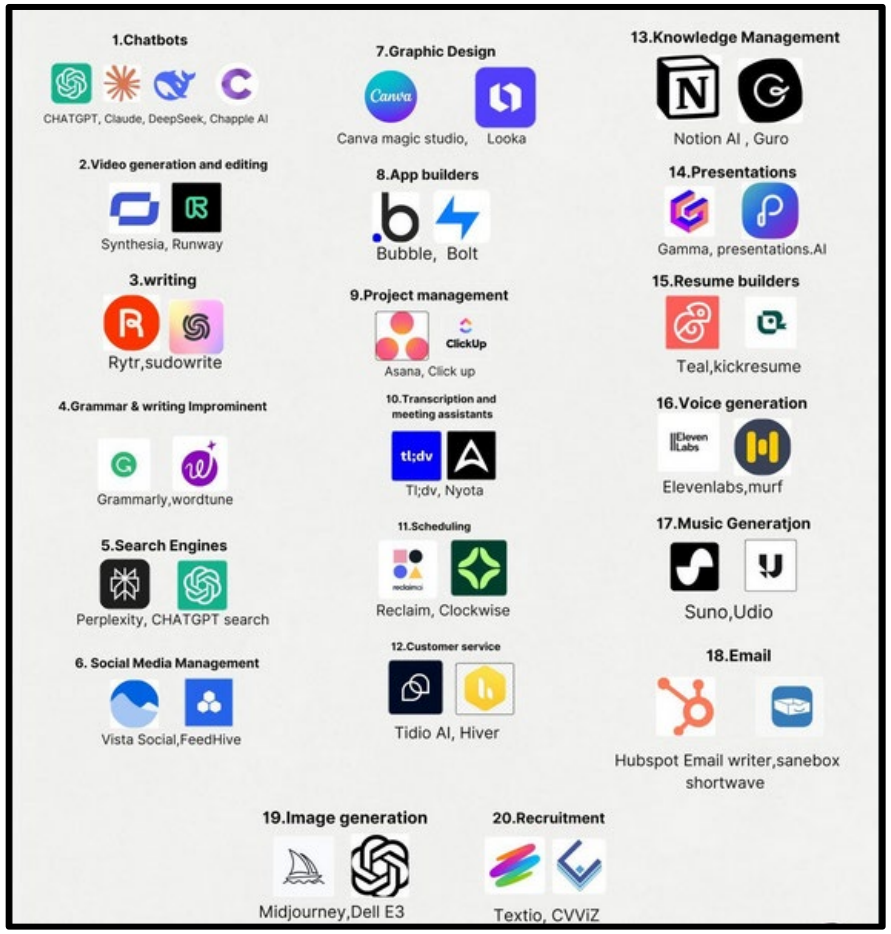
- The presentation is at a **beginner** to **intermediate** level
- **No previous experience** using AI is necessary for participation
- High-level concepts with some depth in appropriate areas
- Topics in AI have great breadth and depth technically, ethically, and philosophically; we have 50 minutes today
- Presentation intended to be thought-provoking and informative
- Intention is to **raise awareness** and **not cast doubt**

Speaker Bio

- 40 years of IT experience, 26 years in Information Security and in Healthcare industry
- Currently Co-Managing Partner at tw-Security
- Former CISO Mercy Health of Ohio and Data Security Administrator at The Cleveland Clinic

Agenda

Acknowledging the Positive - General



- Automates repetitive and mundane tasks
- Enhances decision making
- Improves workflow efficiencies and productivity
- Can improve accuracy and reduce human error
- Rapid data analysis especially on large data sets

Acknowledging the Positive - Healthcare

- Can improve diagnostic accuracy
- Early disease detection
- Predictive analytics and personalized care **improve outcomes** and **lower readmissions**
- Clinical decision-making using very large data sets and/or real-time data
- Can accelerate medical research results

Some AI Terminology

- **Artificial Intelligence:** Machines **simulating human intelligence** processes such as learning, reasoning, and self-correction
- **Machine Learning:** A subset of AI whereby **machines learn** from data, identify patterns, and **make decisions** with minimal human interaction
- **Neural Networks:** Computational models inspired by the human brain's interconnected neuron structure. It is the basis for **Deep Learning**, which enables **processing large data sets** for tasks such as image and speech recognition

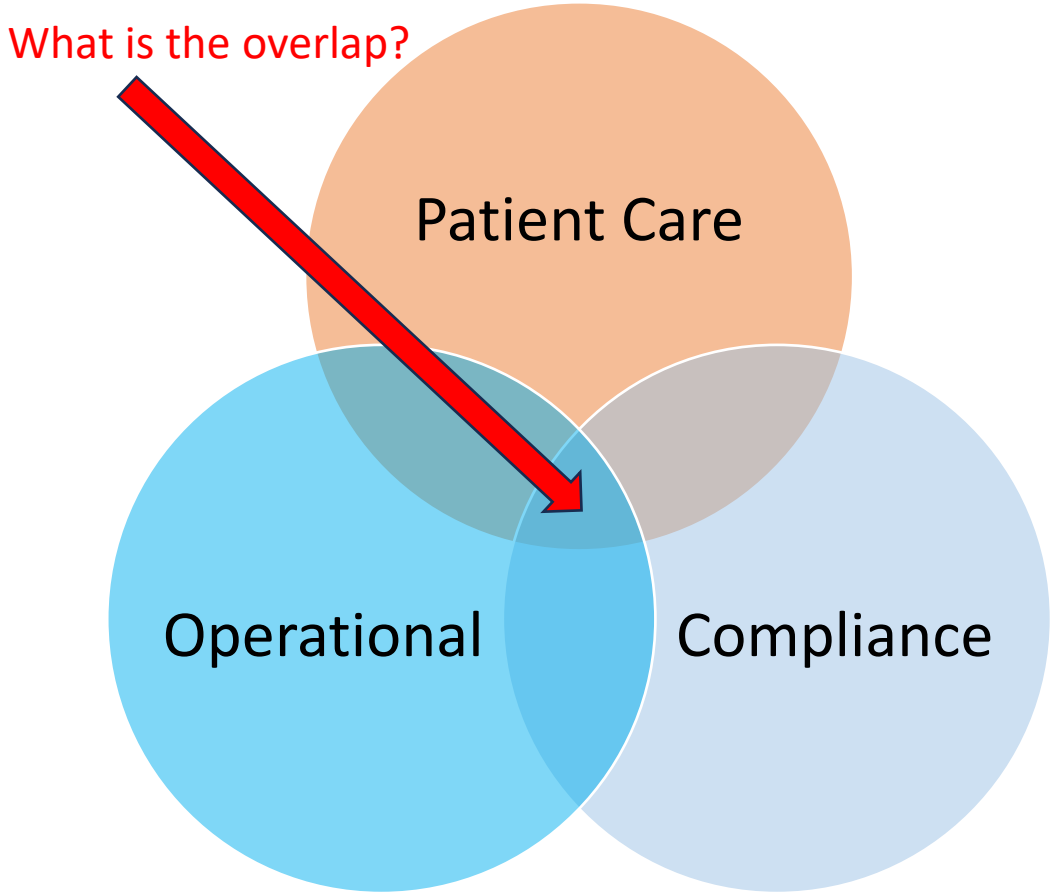
Some AI Terminology

- **Traditional AI:** Artificial Intelligence **designed** to focus on **analyzing** data or making **predictions**
- **Generative AI:** A category of AI systems designed to **create new**, **original content** (e.g., text, images, audio, video) by learning patterns and structures from existing data
- **Large Language Model:** A machine learning model designed to **understand** and **generate human language** using deep learning
- **Model Cards:** **Documentation** on the design, capabilities, and constraints of an AI system, to foster understanding and trust

Some AI Terminology

- **Risk Cards:** Supplemental **documentation** to Model Cards that openly address **potential negative consequences**, encouraging proactive approaches to harm prevention
- **Agent-based AI:** **Autonomous** entities within AI capable of perceiving their environment, making decisions, and execute actions to achieve objectives, adapting dynamically **without human intervention**
- **Hallucinations:** **Incorrect**, **misleading**, or entirely **fabricated** AI output presented as factual

AI Risks



Significant AI Risk – Lack of Governance

- Adoption of AI in business has been ~~Crawl~~, ~~Walk~~, Run
- Little or **no policy on AI use**
- Lack of use case definition
  - Who
  - What purpose
  - How
- Absence of **selection criteria** and vetting

AI Risks – Patient Care

- Misdiagnosis
  - Insufficient training of Large Language Models (LLMs)
  - Biased, polluted, poor-quality data
  - Hallucinations
- Overreliance on recommendations
- Technical issues / malfunctions
- Lack of governance / oversight
- Agents take action without human scrutiny

AI Risks – Patient Care

- Organizational Outcomes and Expectations for Performance, Quality, and Precision not clearly articulated
- Accountability of Outcomes Undefined
- Transparency for AI/ML may be Missing
- Dubious Quality of Source Data
- Absence of Comprehensive Regulatory Oversight

Source: *healthsectorcouncil.org*

AI Risks – Patient Care

- Lack of Business Leader Knowledge
- Unintended Consequences – Change Management
- Adversarial Data Input Poisoning
- Inversion, Inference, and Model Extraction Attacks

Source: *healthsectorcouncil.org*

AI Risks - Operational

- Does the **vendor** have internal AI **governance** established?
  - Addressing products, services, roadmaps, and ethics
- Is there an additional **E**nd **U**ser **L**icense **A**greement?
- What rights does the vendor have to use customer data for model training?
- Must the vendor disclose when it changes models?
- Does the solution use **R**etrieval **A**ugmented **G**eneration? **E**xplainable **A**rtificial **I**ntelligence?

AI Risks - Operational

- Do we know if the vendor **outsources** its AI **platform**?
- Do we know if the product or solution **remains functional** if the AI platform is **down**?
- Do we understand how AI is used in **non-clinical contexts** (such as financial analyses) and what risks/impacts exist for errors/hallucinations, etc.?
- Is the vendor willing to discuss methods used for training the models?
- Does the vendor **outsource** its **implementation team**?

AI Risks - Operational

- Who is responsible for:
  - **Training** the system
  - **Administering** the system
  - **Customizing** the system
- How **specialized/complicated** is the training to use the solution?
- How many **FTEs** are required to maintain the AI platform?
- Does the platform have the means to detect **hallucinations**?
- How easy is it to **scale** the platform as usage and demands are placed on it?

AI Risks - Compliance

- Has a **risk analysis** been performed on the platform, especially if it stores, processes, or transmits PHI?
- Can the system **generate** PHI / PII?
- Is the AI platform **located overseas**? (Think DeepSeek)
- Does the solution make calls to another vendor's AI platform?
- Is there a disaster **recovery plan** for the AI platform?
- Does the solution host the engine in a separate environment from the data / data computing environment?

AI Risks - Compliance

- What kind of **audit trails** does the AI solution have?
- How do we get our data out of the AI platform if the **contractual** relationship **ends**?
- Can **data** be **deleted** from the system?
  - If so, how does that impact the training model?
- Do user log directly into the platform?
- Does the system have the means to **detect misuse**?
- Is data at rest encrypted?

Recommendations for AI Risk Management

- Establish AI governance
- Create an AI policy including acceptable use
- Educate the workforce on AI, AI policy requirements
- Identify changes in Supply Chain / Vendor Management contract language for purchases involving AI
- Ask questions of the vendor, get references
- Include AI risks as a dimension of HIPAA risk analysis
- Keep an eye on news, emerging laws (such as HR AI hiring biases)

Security
Healthcare Security & Privacy

BEST IN KLAS SECURITY & PRIVACY CONSULTING SERVICES 2025

BEST IN KLAS SECURITY & PRIVACY CONSULTING SERVICES 2024

Q&A
Closing Thought

Contact Information

Keith Fricke,
MBA, CISSP, PMP

tw-Security

www.tw-Security.com

keith.fricke@tw-Security.com

216-280-4430