AI in Healthcare: Emerging Uses and Security Risks in Hospitals

Chris Mouradian | Chris Ellingwood

BerryDunn

October 3, 2023

Presenters

Chris Mouradian, CPA

Senior Manager
Healthcare Practice Group

Chris Ellingwood, CISA

Principal
Technology Assurance Service

Agenda

1 Current State of AI

2 AI Trends in Healthcare

3 Security Risks

Learning objectives

By the end of this presentation, participants will learn about innovative applications of AI in healthcare and recognize the associated security risks for more secure and effective adoption.

Definitions

1. Artificial Intelligence (AI)
2. Generative AI
3. Large Language Model (LLM)
4. Chatbots

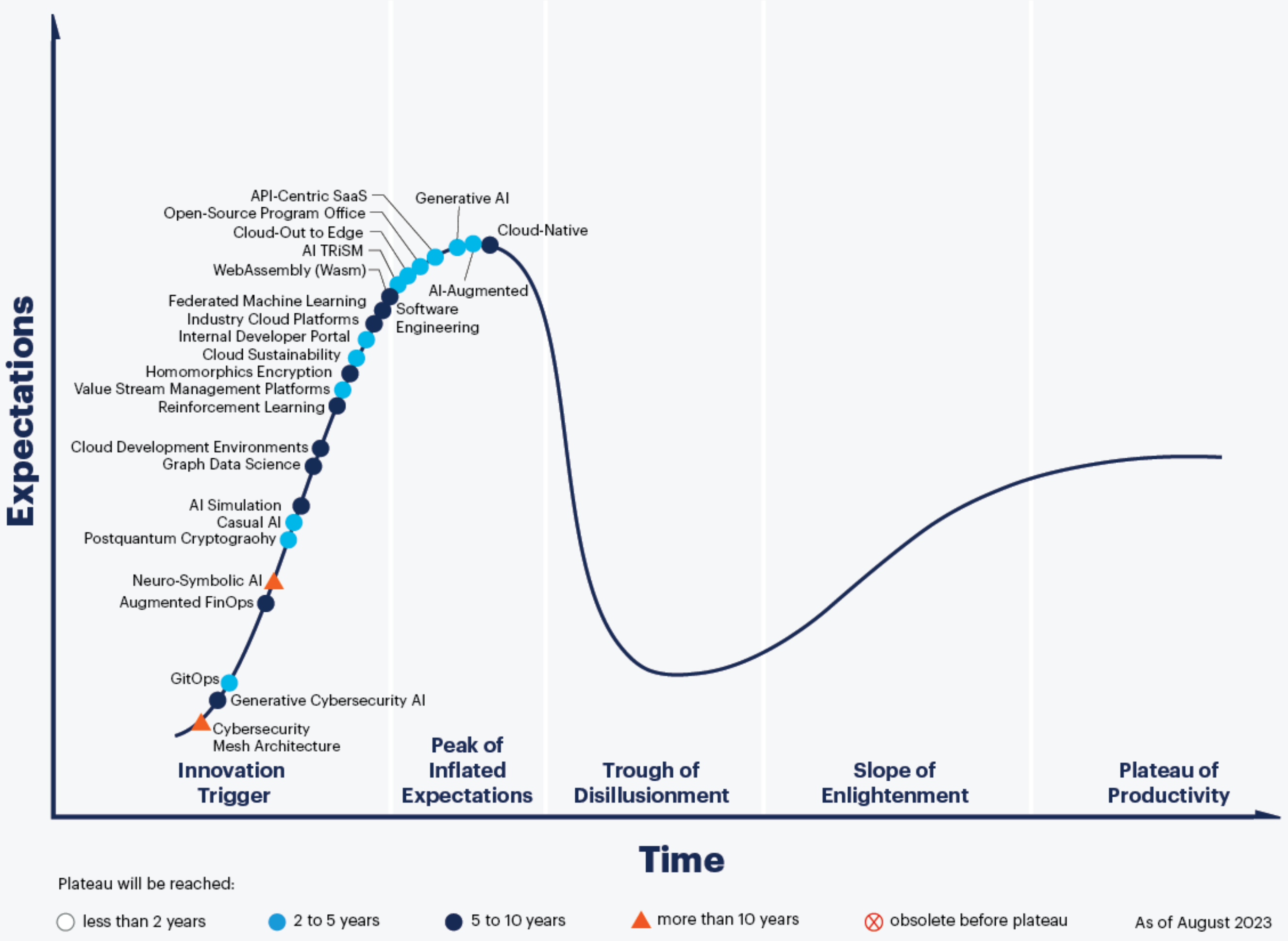
State of AI

- While AI is not new, the revolution is in the wide access to AI related tools and services
- Language models constantly evolve
- Rise of “AI” creates opportunities (and risks)

Hype

What’s real and what’s not

Hype Cycle for Emerging Technologies, 2023



gartner.com

Source: Gartner

Gartner.

Polling Question #1

75% of healthcare leaders are considering AI strategy implementation.

Polling Question #2

Trend 1

AI in the Healthcare setting

- Interpreting and Diagnosing
- Automating Workflows and Reducing Administrative Burden

AI in Imaging

Natural language processing (NLP), is revolutionizing radiology, enabling faster, higher-quality analysis of X-rays and MRIs, leading to precise early diagnoses. GE Healthcare reports a **30% increase in speed and enhanced image quality.**

AI Virtual Nursing Assistants

One recent study reported **64% of patients trust AI for 24/7 support**. These AI systems answer queries, forward reports, and schedule visits, alleviating routine tasks for clinical staff and allowing more focus on personalized patient care.

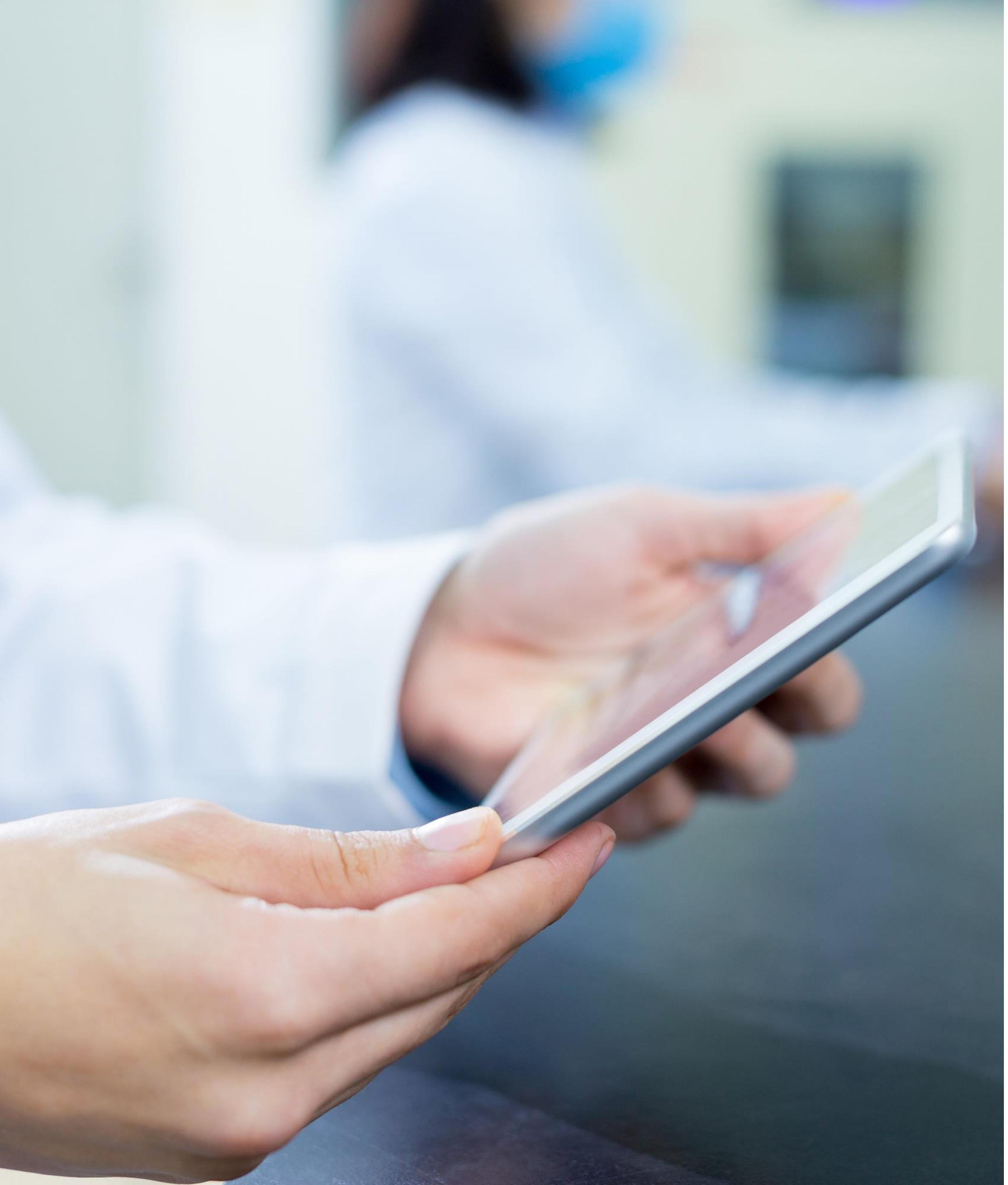
Trend 2

AI for the Patient Experience

- Improving Patient Communication and Engagement
- Improving Access to Care

28 million Americans didn’t have health insurance in 2020

83% of patients report poor communication as the worst part of their experience



Trend 3

Revenue Cycle

- **$9.8B** in potential savings by automating revenue cycle functions
- **9%** of all claims are denied
- **23.9%** of all denials are eligibility related

Trend 3 (continued)

AI in Revenue Cycle

- Increase cash collections / reduce AR days
- Reduce dependency on recruiting and training staff
- Greater employee satisfaction

Trend 4

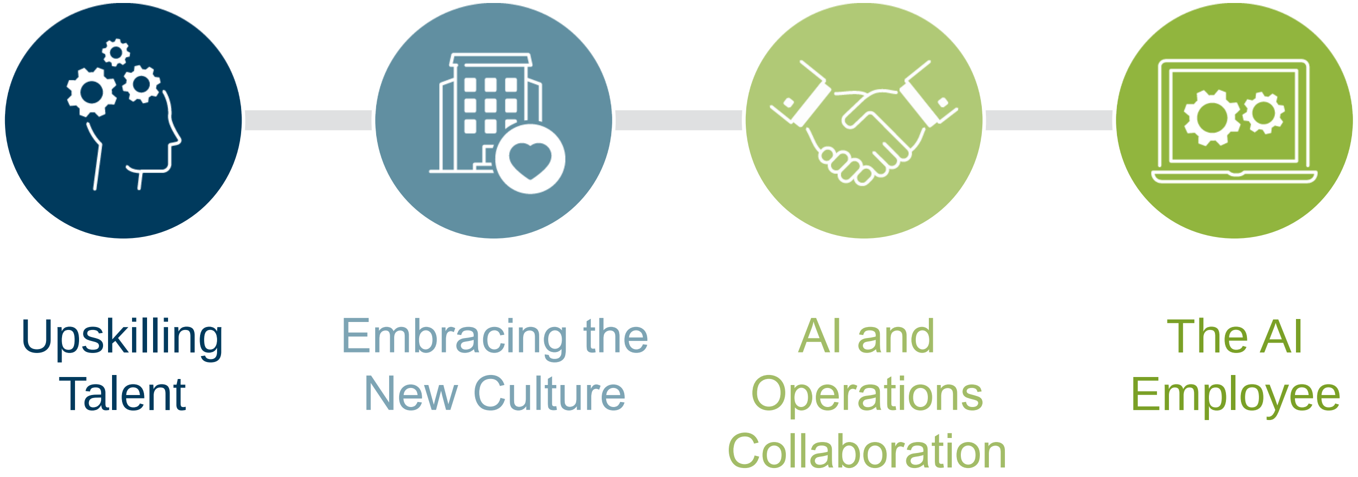
AI in Finance and Accounting

- Automating repetitive tasks
- AI-driven workflows

A recent IBM® study found that executives expect **48% of the staff** across their organizations (including 34% of finance staff) will use generative AI to augment their daily tasks in the next year.

Trend 5

AI Culture in the Workplace



Upskilling Talent

Embracing the New Culture

AI and Operations Collaboration

The AI Employee

Actions to Take

1 Change the enterprise mindset from “adding AI” to “starting with AI,” reinventing processes, tasks, workflows, and jobs to deliver productivity improvements.

2 Reevaluate prior automation scope based on the new generative AI capabilities.

3 Redefine jobs and skills based on the higher-value-added tasks where AI is less useful.

4 Re-skill the employee base to understand AI and the proper and improper use of it. Build AI ethics and bias identification training programs for employees and partners to comply with AI ethics regulations.

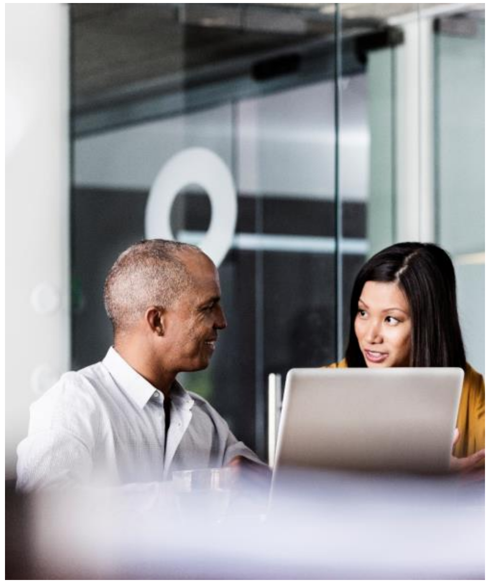
5 To manage risk, document—with fact sheets—every instance of AI use in the organization and the current governance around it.

Polling Question #3

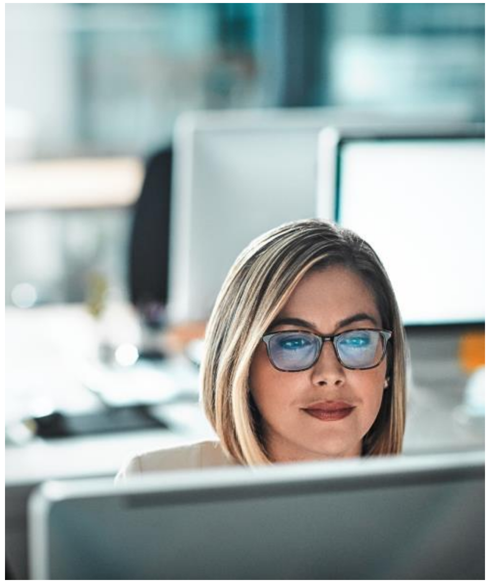
AI Risks Fall Into Four Categories

All apply to a healthcare setting

Data



Testing and trust



AI-driven attacks

Compliance

Data and Testing and Trust

Data is valuable – when it's good

AI tools may help with diagnoses…
and save time and tests – BUT…

- Data may be biased / stuck in the "box"
- Data may lead to poor outcomes or injury (think the stop sign photo used in driving cars)
- Data may be incomplete or junk; 1+1=3
- Data may contain ePHI (see compliance risk)
- Data may be toxic (see AI attack risks)
- Test, test, test!

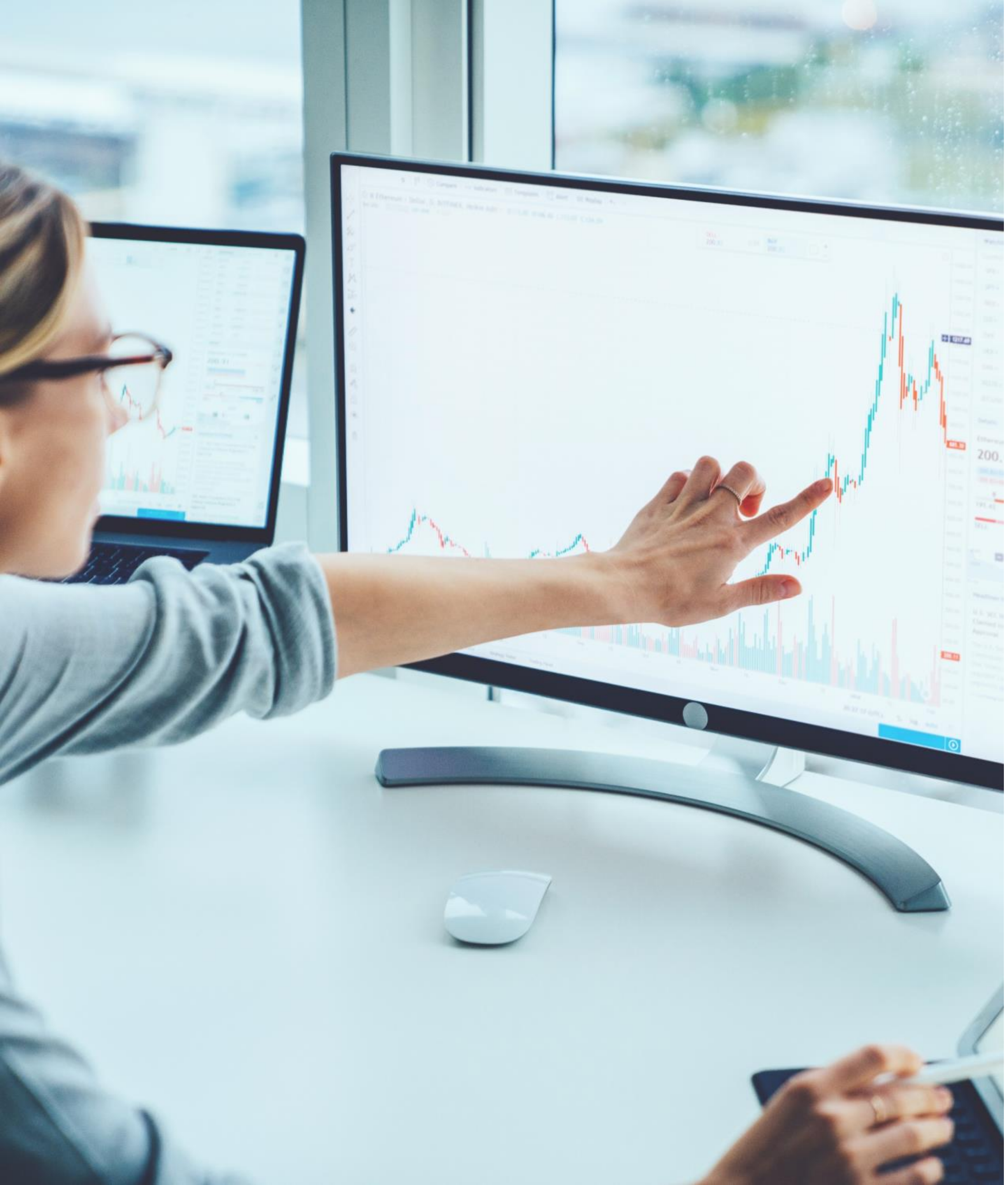
Mitigating Data and Trust Risks

- Understand what data is in the algorithm you use
- If you give patients the ability to interact with AI diagnosis tools, very carefully evaluate results
- Establish rules
- Monitor results for patterns and biased output
- Be prepared for false results or incorrect results
- Handle patient data with care
- ALWAYS have a human review before treating

AI-Driven Attacks

Now the robots are coming after us

- ChatGPT can be used to defraud, but not attack (and that's only by human design it won't attack)
- AI leads the way for effective "fakes" – think advanced ChatGPT
- Data poisoning – think of what the impacts in healthcare could be
- AI-driven attacks – DDoS, phishing, brute force, password guessing
- Able to learn systems and how to not be detected



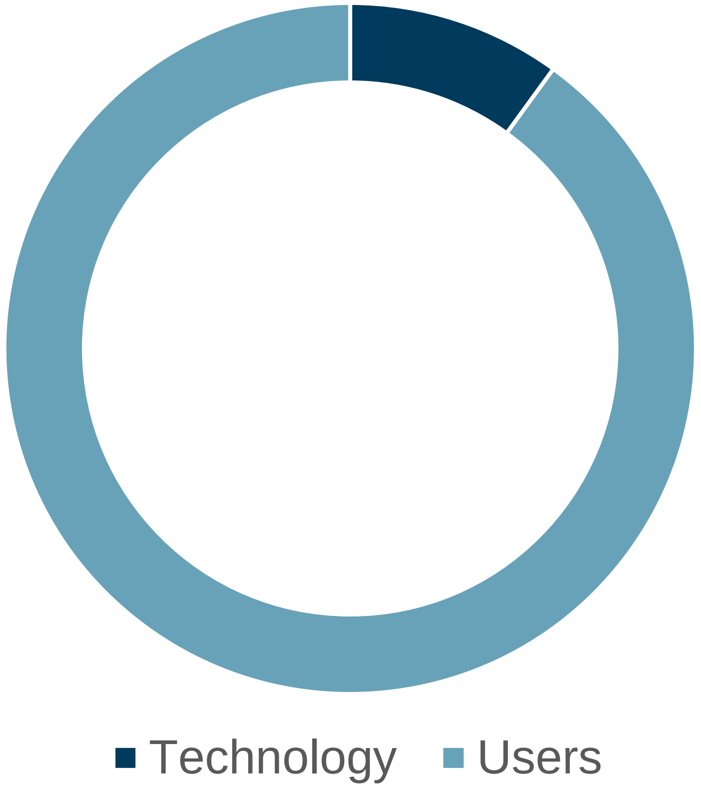
Mitigating AI Attacks

- Lock down the decision-making AI systems. Use a Checksum
- A need for very strong documented development standards and policies
- Critical need for rigorous auditing
- Ensure you have monitoring tools and alerting tools in place – fight AI with AI
- Train personnel on phishing!!!

A quick sidenote….The 90/10 Rule

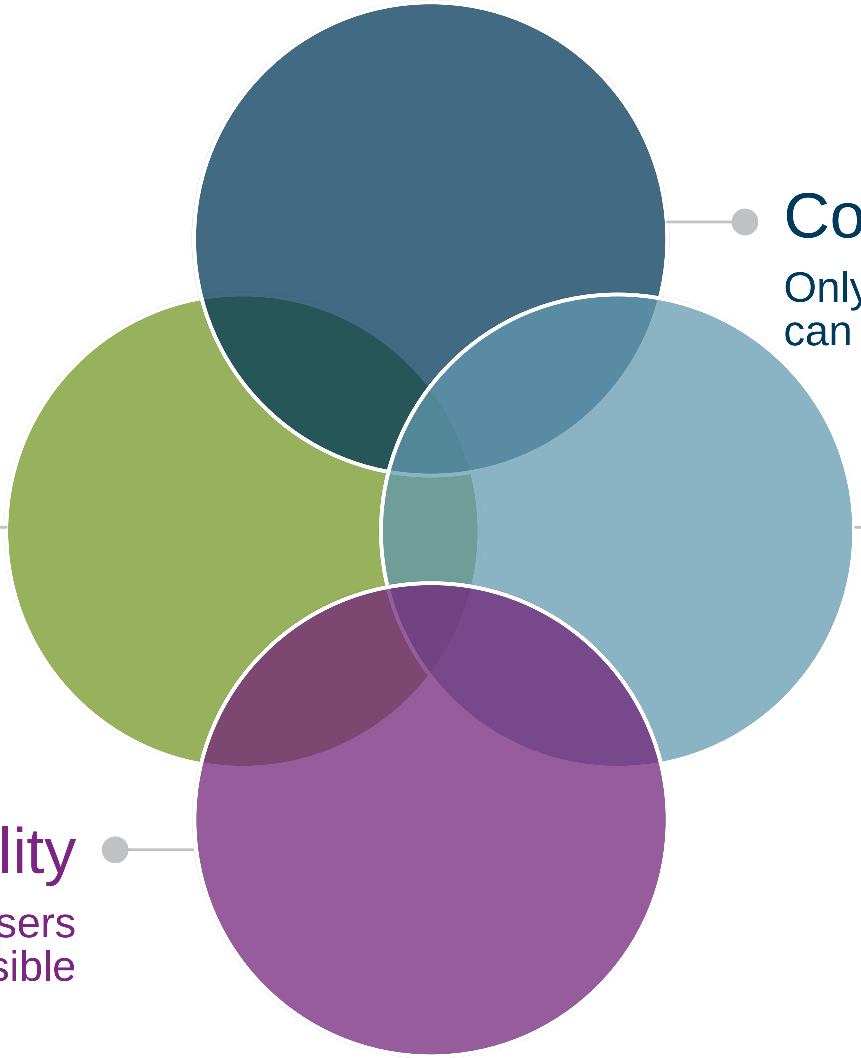
And what it means for your healthcare organization

- **10%** of security safeguards are technical
- **90%** of security safeguards rely on the user to adhere to best practices and follow policies and procedures



A quick side note…

Maybe it’s time for another “A” in the Security Matrix?



Confidentiality

Only authorized individuals can view the data

Integrity

Data is complete and reliable

Availability

Data and systems are accessible when needed

Accountability

Trace actions to users and hold responsible

AI Compliance Risks

Now the robots are coming after us

1. AI data in healthcare may contain ePHI/PII

2. Understand what is in the data – does it need to be there?

3. HIPAA Compliance!

4. State privacy laws

Mitigating AI Risks – Compliance

- Control access
- De-identify data if able
- Encrypt data at rest and in transit
- Re-visit HIPAA controls and processes

Questions?

Chris Mouradian, CPA
Sr. Manager
Healthcare Practice Group
cmouradian@berrydunn.com
207.541.2274

Chris Ellingwood, CISA
Principal
Technology Assurance Service
cellingwood@berrydunn.com
207.541.2290

BerryDunn

berrydunn.com