COMMUNITY HEALTH CARE ASSOCIATION of New York State

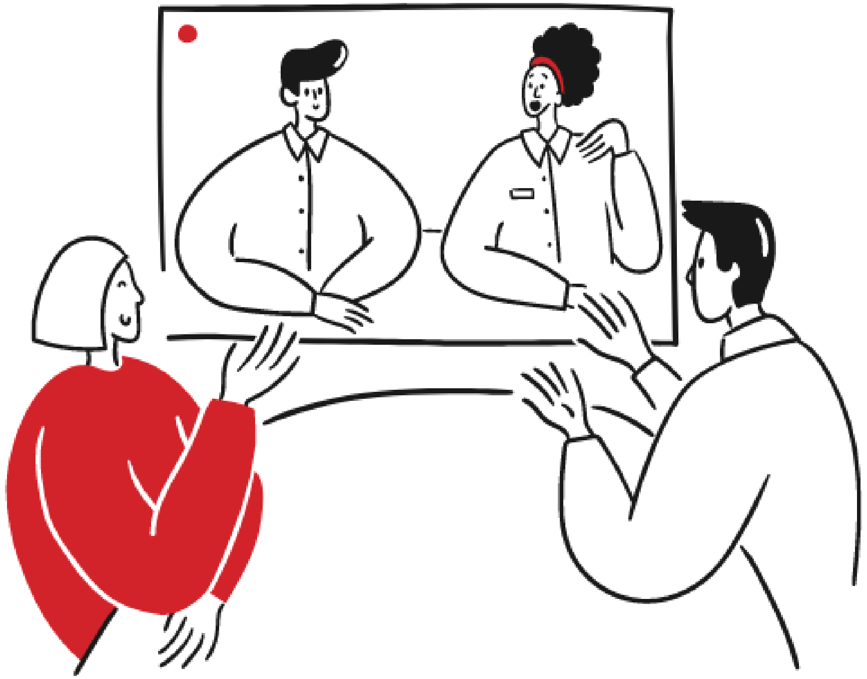
CHCANYS NYS-HCCN presents a three-part learning series with Online Business Systems

Privacy and Security Considerations for Artificial Intelligence

Session 3
March 19, 2024

Zoom Guidelines

- You have been muted upon entry. Please respect our presenters and stay on mute if you are not speaking.
- Please share your questions in the chat. CHCANYS staff will raise your questions to our speakers and follow up as needed if there are unanswered questions.
- The workshop is being recorded and slides will be shared after the session.



New York State HCCN Objectives

Project Period 2022-2025

1 **Clinical Quality**

2 **Patient-Centered Care**

3 **Provider and Staff Wellbeing**

2022-2025 Project Period

- ✓ Patient Engagement
- ✓ Patient Privacy & Cybersecurity
- ✓ Social Risk Factor Intervention
- ✓ Disaggregated Patient-level Data (UDS+)
- ✓ Interoperable Data Exchange & Integration
- ✓ Data Utilization
- ✓ Leveraging Digital Health Tools
- ✓ Health IT Usability & Adoption
- ✓ Health Equity and REaL Data Collection*
- ✓ Improving Digital Health Tools- Closed Loop Referrals*

** - Applicant Choice Objective*
Bold- Objective Carried over into 2022-2025

Privacy and Security Considerations for AI

COMMUNITY HEALTH CARE ASSOCIATION of New York State

Jordan Wiseman, MLS, CISSP, QSA

Fellow; Risk, Security & Privacy Team

Online Business Systems

COMMUNITY HEALTH CARE ASSOCIATION of New York State chcanys.org

online
HEALTH CYBERSECURITY

Community Health Care
Association of New York State

ARTIFICIAL INTELLIGENCE IN HEALTHCARE

On the potential impact of artificial intelligence in healthcare, health information security, HIPAA compliance, and other considerations.

JORDAN WISEMAN
FELLOW CONSULTANT

Results. Guaranteed.

01 INTRODUCTION

02 **PROMISES** AND PROBLEMS

03 PROMISES AND **PROBLEMS**

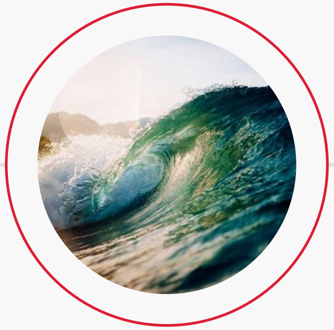
04 AI AND THE HIPAA RULES

05 PRACTICE MANAGEMENT

WHY WE’RE HERE TODAY

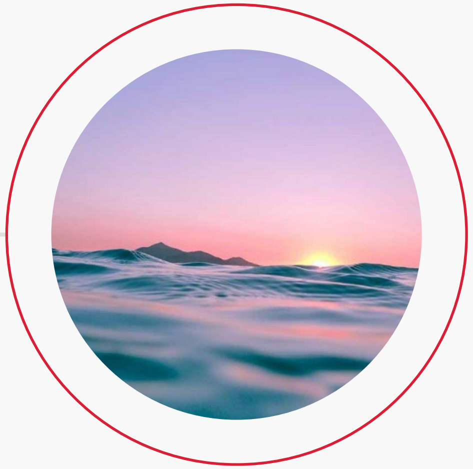
Large Language Models may be the new fad, but AI is not new, especially in healthcare settings where its use is increasing marginally…

IN THE BEGINNING, THERE WAS A DESIRE TO HELP US



AUTO CORRECT

"Fixing" typos in our text messages and making our lives interesting through misunderstandings

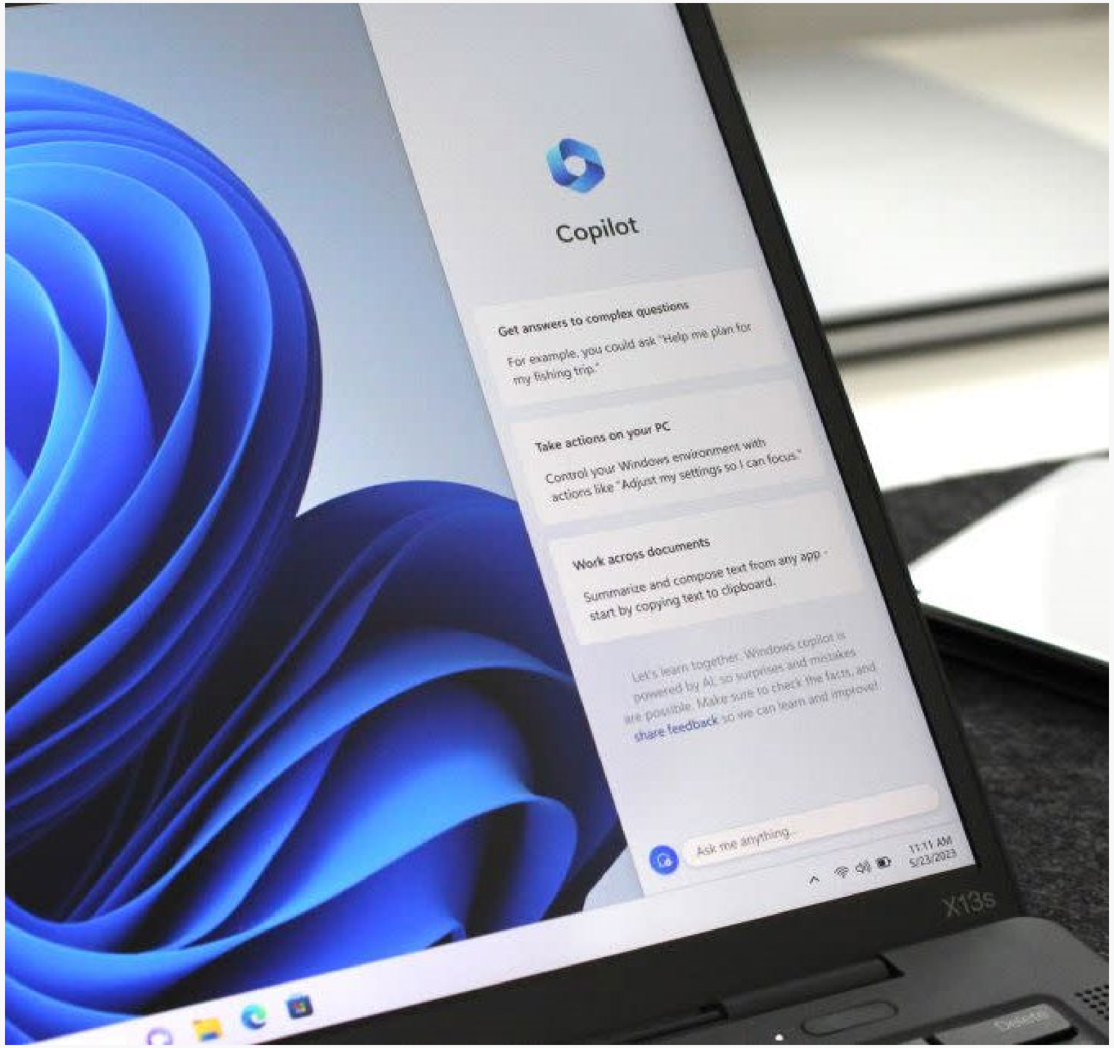


PREDICTIVE TEXT

Learning how we write and helping make us more efficient.

> These innovations are ubiquitous; they've been part of our digital lives for decades.

For most consumers, these features might have been the first exposure to and use of Artificial Intelligence. Rudimentary and requiring only local resources, they are like current models in that they start based on general training and learn or are tailored by usage.



For example, you could ask "Help me plan for my fishing trip."

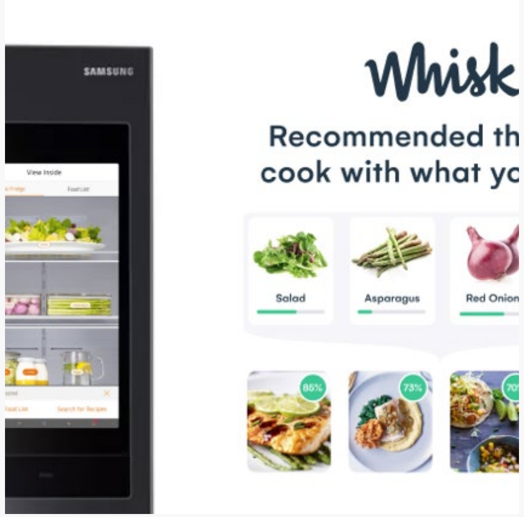
Control your Windows environment with actions like "Adjust my settings so I can focus."

Summarize and compose text from any app - start by copying text to clipboard.

Let's learn together. Windows copilot is powered by AI, so surprises and mistakes are possible. Make sure to check the facts, and share feedback so we can learn and improve!

AI IS COMING TO EVERYTHING

AI is being added to many tools we use everyday, from our laptops to our cars, and even our *refrigerators.* Essentially, it's trying to make our tech smarter and more useful.



Okay, but what does this mean for *us*?

INTO A NEW ERA

…through collaboration between providers, support staff, developers, and regulators, AI may…

- Improve patient outcomes
- Reduce costs
- Enhance data analysis
- Support telehealth
- Promote empowerment

CAUTIOUSLY THOUGH

…because without care by providers,
support staff, developers, and regulators,
AI may…

- Expose and disclose PHI
- Exhibit bias and unfairness
- Be uninterpretable and opaque
- Present compliance and regulatory challenges
- Harm data quality and integrity

PROMISES AND PROBLEMS

AI in healthcare: because who wouldn't want a brainy sidekick that can read a mountain of data faster than you can say “diagnosis”?

DICTATION+

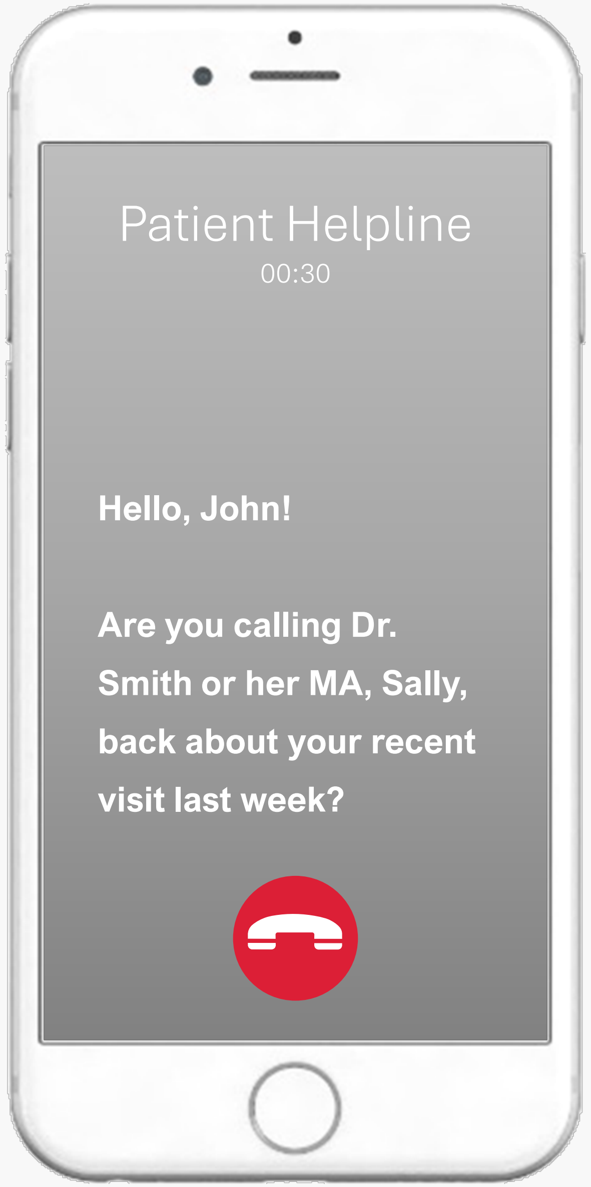
Artificial Intelligence (AI) can help streamline charting through accurate transcribe physicians' and patents' spoken words, reducing the time in populating relevant fields in patient charts, coding for diagnoses and procedures, leading to more efficient, accurate, and comprehensive medical documentation.

Using AI this way will allow providers to focus more on patient interactions and care rather than tedious administrative tasks.

An AI scribe may even identify inconsistencies, missing info, and possible chart corrections.

AI CALL LINE

This is not the classic “auto-attendant” approach. This is about a multi-layered approach where AI can help augment the capability and capacity of call centers and act as an engaging patient navigator.



Patient Helpline

00:30

Hello, John!

Are you calling Dr. Smith or her MA, Sally, back about your recent visit last week?

A FRIENDLY VOICE

LLM-based AI systems can answer calls and present a consistently personable, yet personalized, experience.

PREDICIVE ANALYTICS

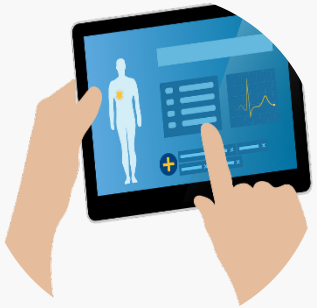
Analyze call-trend data and patient histories to find the reasons for expected or unusual calls help direct patients effectively.

INTELIGENT HANDLING

If your patients prefer “their” person, have specific questions, or call during peak times, AI can route their calls efficiently based on prior behavior or analyzed need.

AI IS A MAGICIAN’S ASSISTANT

AI is not magic, but like a good magician, it can help your providers and PSRs seem like they can do impossible, or at least impressive, things.



REFRESHER

AI, interfaced with an EHR or intake system, can whisper in your ear about who you’re interacting with, their history, and what their usual expectations or needs might be.

“

YOU FOLKS ALWAYS REMEMBER WHO I AM

”

COACH

AI, listening in during a conversation or exam can catch things you miss, guide the encounter workflow, and make recommendations in real time.

“

YOU FOLKS ALWAYS KNOW EXACTLY WHAT I NEED

”

ASSISTANT

AI, trained on your patient data, can draft notes, referrals, and patient messages to help save you time while ensuring alignment with patient care processes.

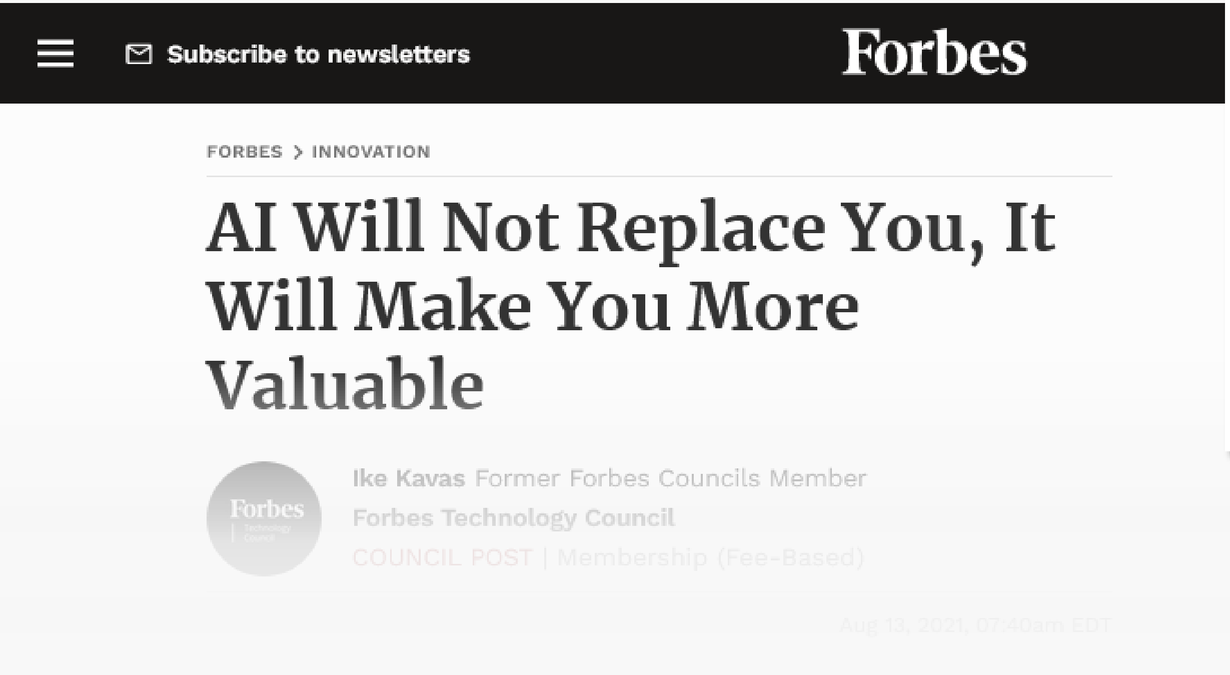
“

YOU FOLKS ALWAYS COMMUNICATE WELL

”

AI SWEATS THE SMALL STUFF

We have always looked to machines to more quickly and consistently perform tasks on our behalf. With modern AI, we've approaching a place where that includes tasks without a static or known procedure to follow.



Subscribe to newsletters

Forbes

FORBES > INNOVATION

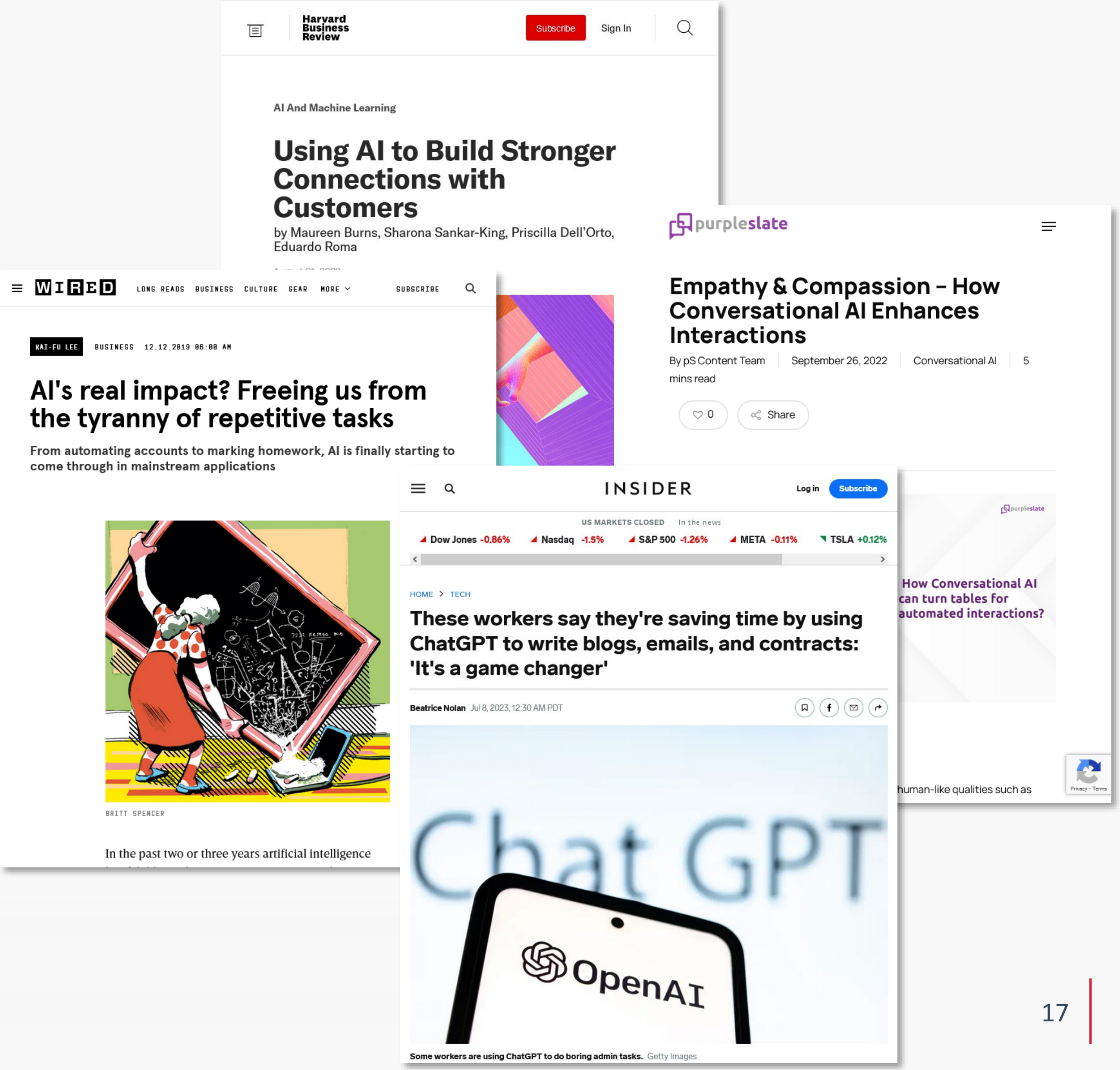
AI Will Not Replace You, It Will Make You More Valuable

Ike Kavas Former Forbes Councils Member

Forbes Technology Council

COUNCIL POST | Membership (Fee-Based)

Aug 13, 2021, 07:40am EDT



Harvard Business Review

Subscribe Sign In

AI And Machine Learning

Using AI to Build Stronger Connections with Customers

by Maureen Burns, Sharona Sankar-King, Priscilla Dell'Orto, Eduardo Roma

August 01, 2022

WIRED

LONG READS BUSINESS CULTURE GEAR MORE SUBSCRIBE

KAI-FU LEE BUSINESS 12.12.2019 06:00 AM

AI's real impact? Freeing us from the tyranny of repetitive tasks

From automating accounts to marking homework, AI is finally starting to come through in mainstream applications

BRITT SPENCER

In the past two or three years artificial intelligence

purpleslate

Empathy & Compassion – How Conversational AI Enhances Interactions

By pS Content Team | September 26, 2022 | Conversational AI | 5 mins read

0 Share

How Conversational AI can turn tables for automated interactions?

human-like qualities such as

Privacy - Terms

INSIDER

Log in Subscribe

US MARKETS CLOSED In the news

Dow Jones -0.86% Nasdaq -1.5% S&P 500 -1.26% META -0.11% TSLA +0.12%

HOME > TECH

These workers say they're saving time by using ChatGPT to write blogs, emails, and contracts: 'It's a game changer'

Beatrice Nolan Jul 8, 2023, 12:30 AM PDT

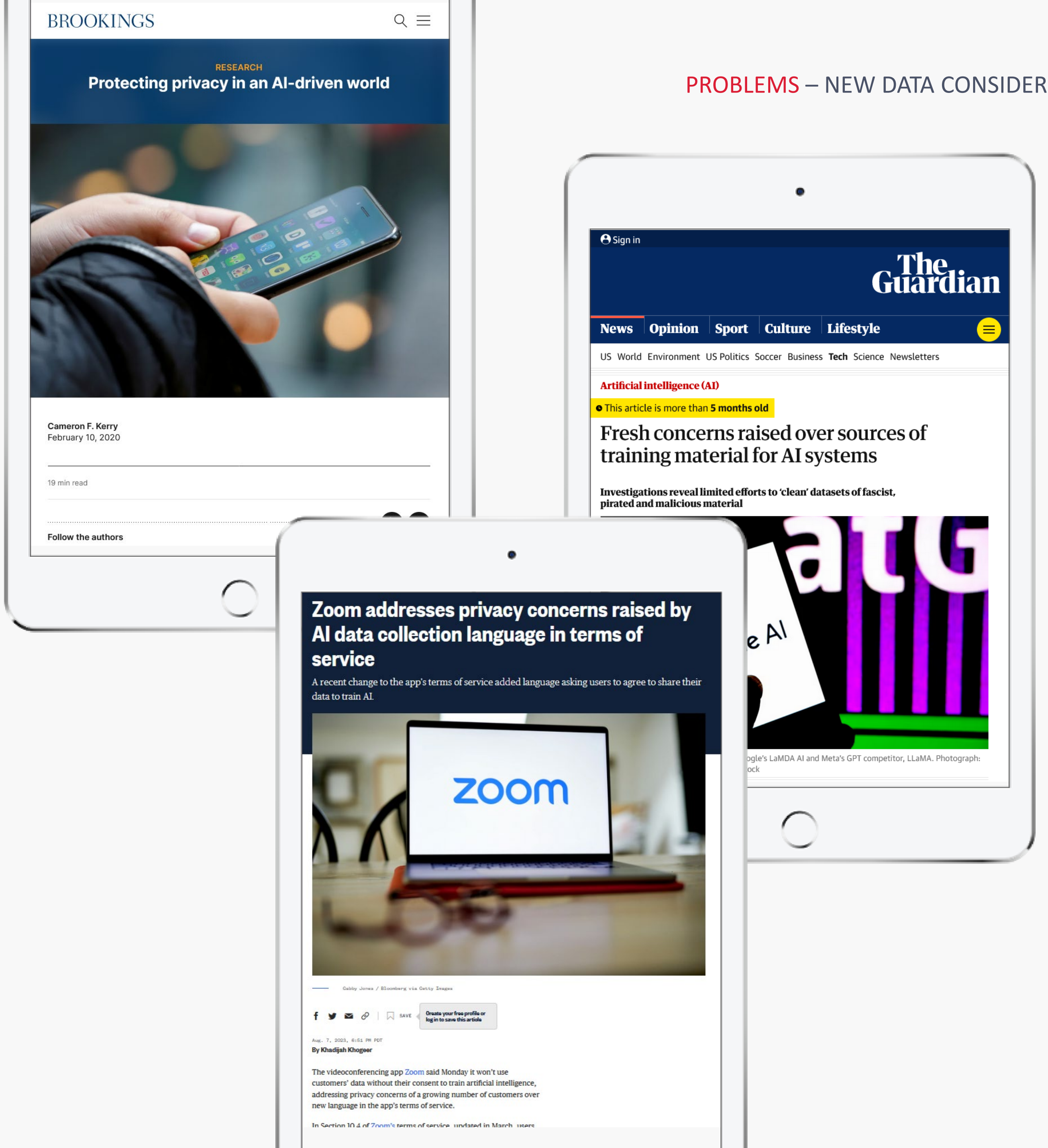
Some workers are using ChatGPT to do boring admin tasks. Getty Images

PROMISES AND PROBLEMS

AI in healthcare: like a promising intern with a PhD in data, yet still learning bedside manners, tact, and how to actually do the job.

AI systems are vulnerable, so are their platforms…

- They're trained on data collected from anywhere, even you
- Outdated data is in the model itself
- Data is in the prompts and output
- Most use a "trust us" privacy model



BROOKINGS

RESEARCH

Protecting privacy in an AI-driven world

Cameron F. Kerry
February 10, 2020

19 min read

Follow the authors

Sign in

The Guardian

News
Opinion
Sport
Culture
Lifestyle
US World Environment US Politics Soccer Business Tech Science Newsletters

Artificial intelligence (AI)

This article is more than **5 months old**

Fresh concerns raised over sources of training material for AI systems

Investigations reveal limited efforts to 'clean' datasets of fascist, pirated and malicious material

ogle's LaMDA AI and Meta's GPT competitor, LLaMA. Photograph:
ock

Zoom addresses privacy concerns raised by AI data collection language in terms of service

A recent change to the app's terms of service added language asking users to agree to share their data to train AI.

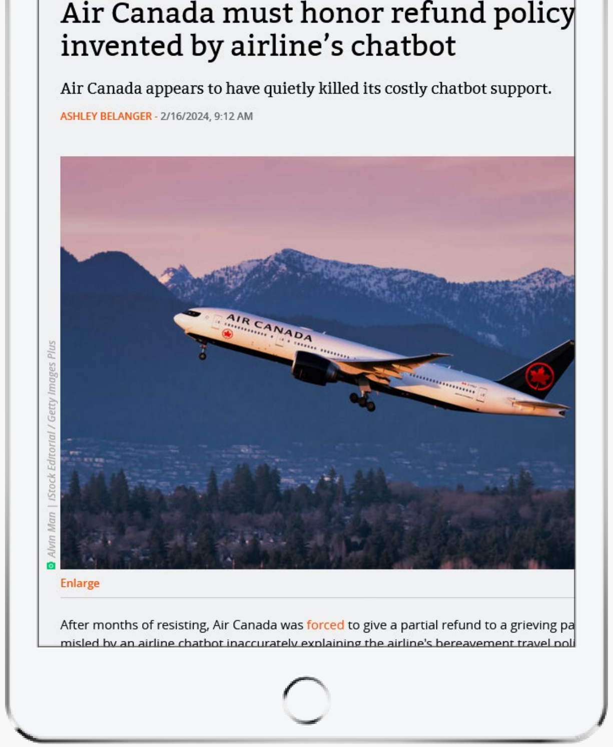
Gabby Jones / Bloomberg via Getty Images

Aug. 7, 2023, 6:51 PM PDT

By Khadijah Khogeer

The videoconferencing app Zoom said Monday it won't use customers' data without their consent to train artificial intelligence, addressing privacy concerns of a growing number of customers over new language in the app's terms of service.

In Section 10.4 of Zoom's terms of service, updated in March, users



Air Canada must honor refund policy
invented by airline's chatbot

Air Canada appears to have quietly killed its costly chatbot support.

ASHLEY BELANGER - 2/16/2024, 9:12 AM

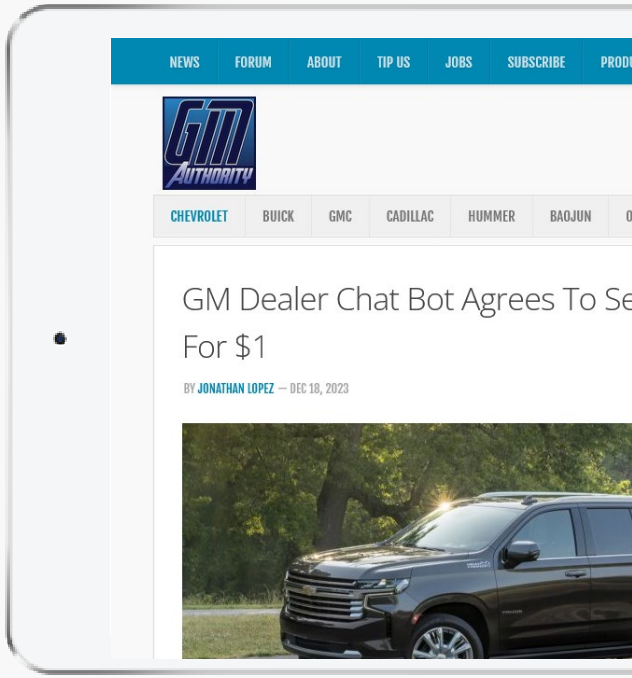
Alvin Man | iStock Editorial / Getty Images Plus

Enlarge

After months of resisting, Air Canada was forced to give a partial refund to a grieving pa
misled by an airline chatbot inaccurately explaining the airline's bereavement travel poli

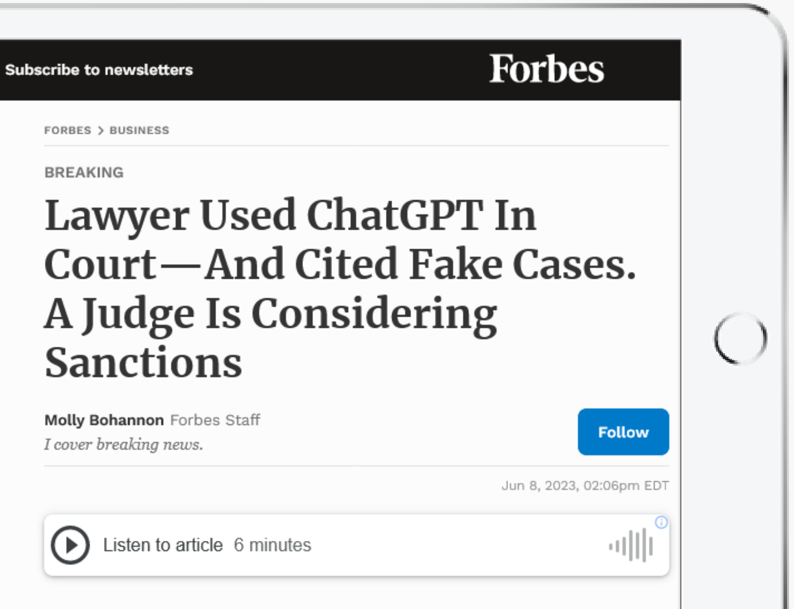
A growing list of unintended consequences…

- AI is built on knowledge, not experience.
- It cannot anticipate its own risks.
- It needs parenting, mentoring, and oversight.



GM Dealer Chat Bot Agrees To Se
For $1

BY JONATHAN LOPEZ — DEC 18, 2023

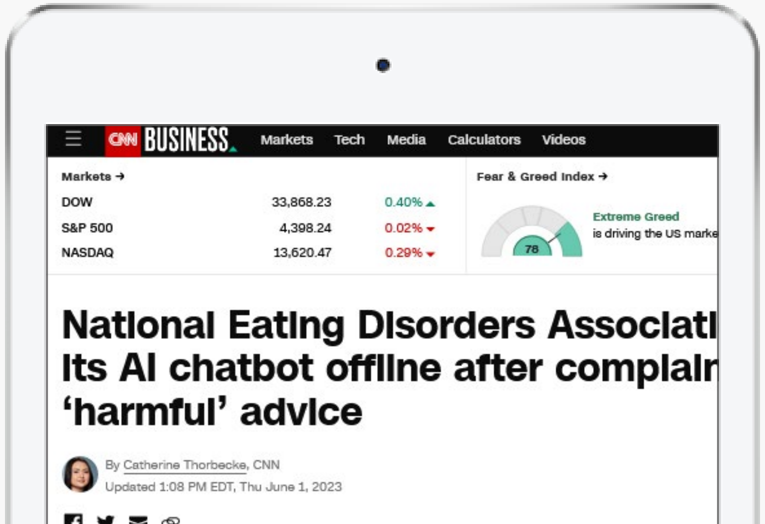


BREAKING

Lawyer Used ChatGPT In Court—And Cited Fake Cases. A Judge Is Considering Sanctions

Molly Bohannon Forbes Staff
I cover breaking news.

Jun 8, 2023, 02:06pm EDT



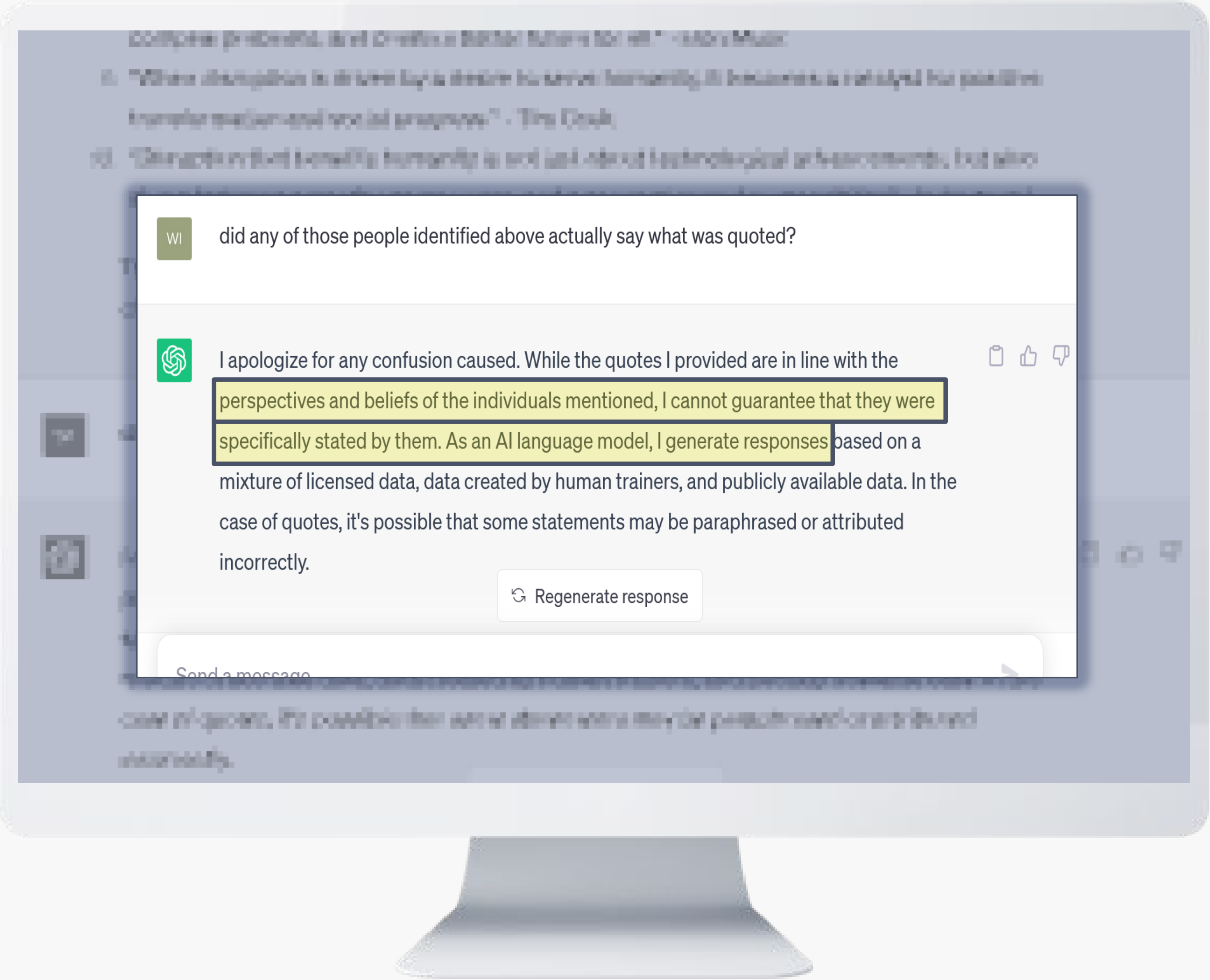
Markets →		
DOW	33,868.23	0.40% ▲
S&P 500	4,398.24	0.02% ▼
NASDAQ	13,620.47	0.29% ▼

Fear & Greed Index →

Extreme Greed
is driving the US marke

National Eating Disorders Associati
Its AI chatbot offline after complain
'harmful' advice

By Catherine Thorbecke, CNN
Updated 1:08 PM EDT, Thu June 1, 2023



did any of those people identified above actually say what was quoted?

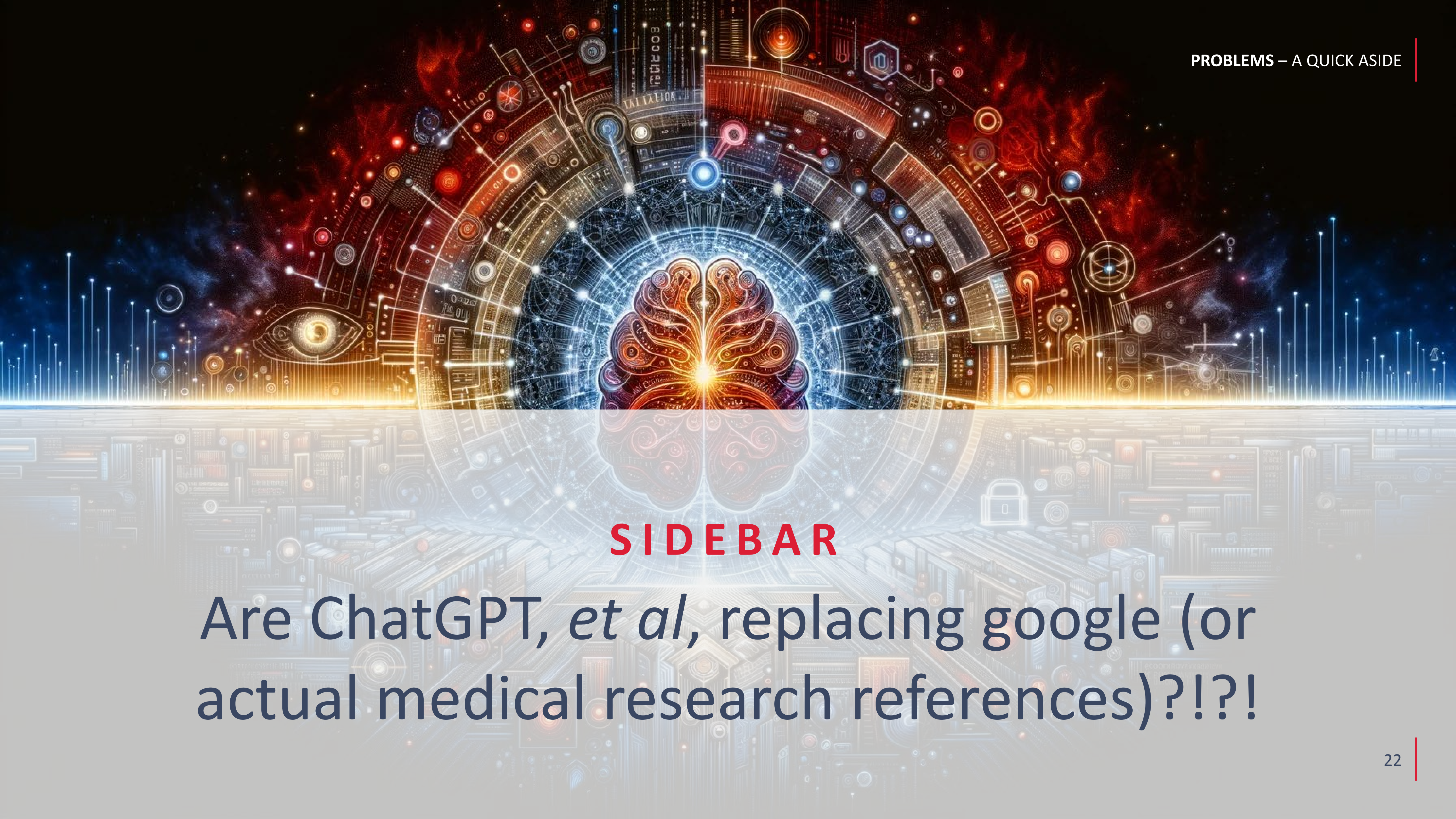
I apologize for any confusion caused. While the quotes I provided are in line with the perspectives and beliefs of the individuals mentioned, I cannot guarantee that they were specifically stated by them. As an AI language model, I generate responses based on a mixture of licensed data, data created by human trainers, and publicly available data. In the case of quotes, it's possible that some statements may be paraphrased or attributed incorrectly.

Is it really

HALLUCINATION

when it's

FABRICATED!?



SIDEBAR

Are ChatGPT, *et al*, replacing google (or actual medical research references)?!?!

SIDEBAR

Are ChatGPT, et al, replacing google (or actual medical research references)?!

The short answer: NO

At least, I don't think so

For the most part:

- LLMs are trained and have only old data
- They don't index new data

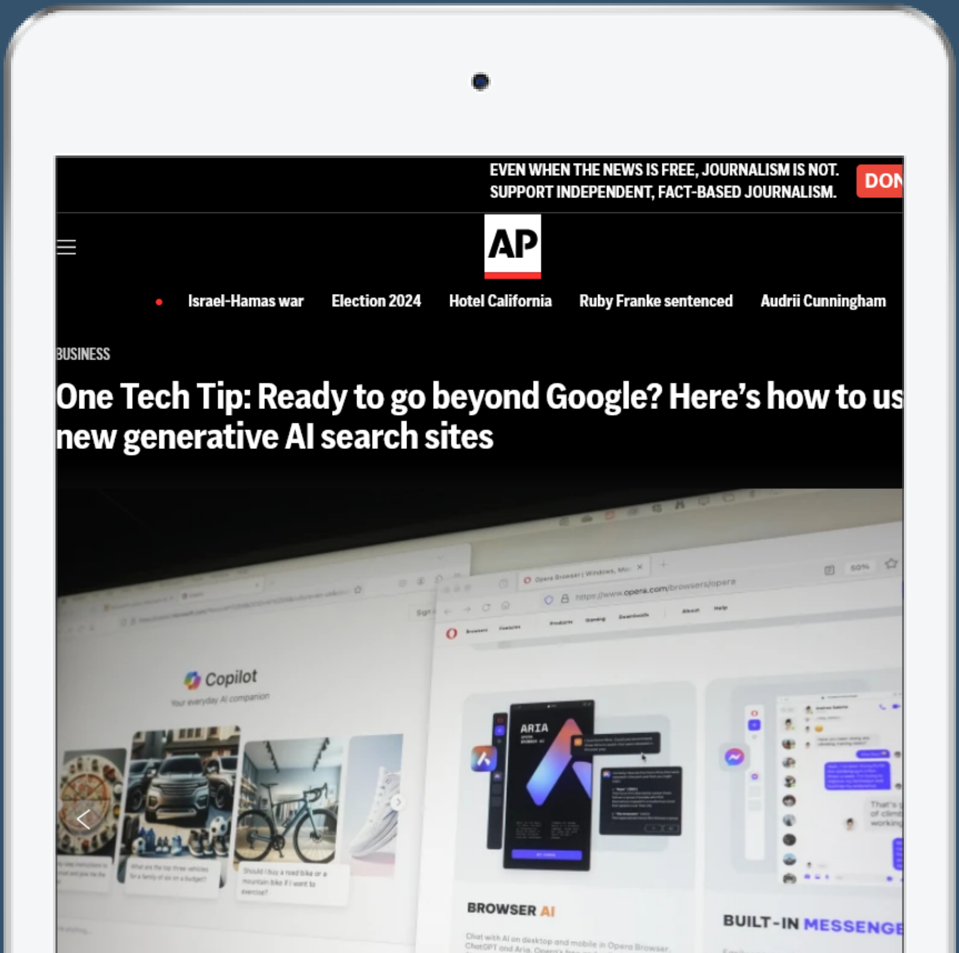
  AND

- *They serve different purposes*

SIDEBAR

Are ChatGPT, et al, replacing google (or actual medical research references)?!

WELL, MAYBE SO…



EVEN WHEN THE NEWS IS FREE, JOURNALISM IS NOT. SUPPORT INDEPENDENT, FACT-BASED JOURNALISM.

DON

AP

Israel-Hamas war Election 2024 Hotel California Ruby Franke sentenced Audrii Cunningham

BUSINESS

One Tech Tip: Ready to go beyond Google? Here's how to us new generative AI search sites

AI AND THE HIPAA RULES

Like a high-tech symphony, with HIPAA and regulations as the conductors ensuring every note of innovation harmonizes with patient privacy and safety.

THE SECURITY RULE

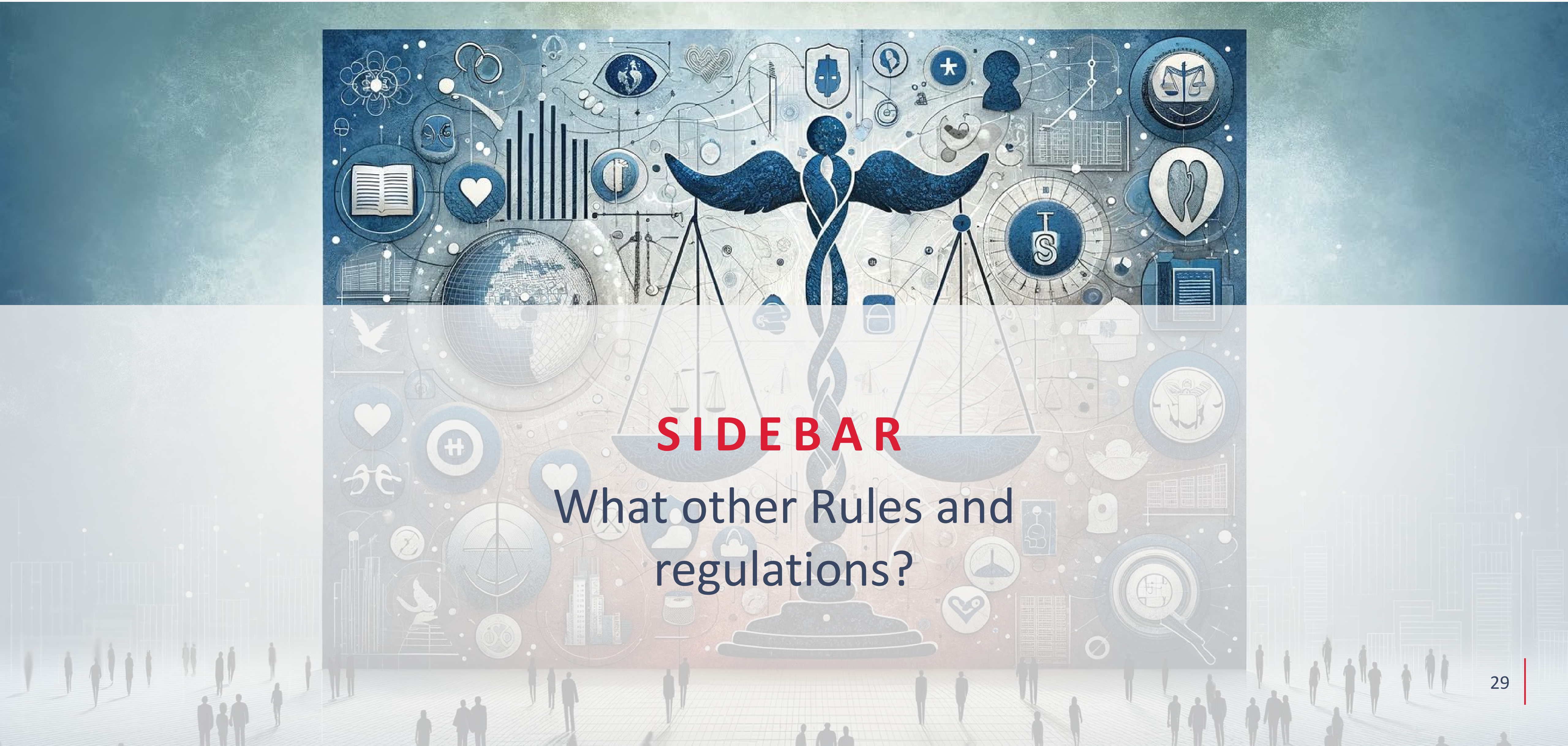
- Risk Analysis and Management
- Access Controls
- Audit Controls
- Data Integrity
- Transmission Security

THE BREACH RULE

- Breach Discovery and Reporting
- Breach Risk Assessment

THE PRIVACY RULE

- Minimum Necessary Datasets
- Patient Rights
- De-identification of PHI
- Consent and Authorization
- Notice of Privacy Practices (NPP)



SIDEBAR

What other Rules and regulations?

HIPAA Related

- Enforcement Rule
- Transactions and Code Sets Rule
- Unique Identifiers Rule
- Omnibus Rule

Non-HIPAA

- Genetic Information Nondiscrimination Act (GINA)
- Patient Safety and Quality Improvement Act (PSQIA)

Other US Laws

- Privacy (e.g., CCPA, CPRA, MT CDPA– in Oct. 2024)
- Consumer Protection
- Wire Tapping?

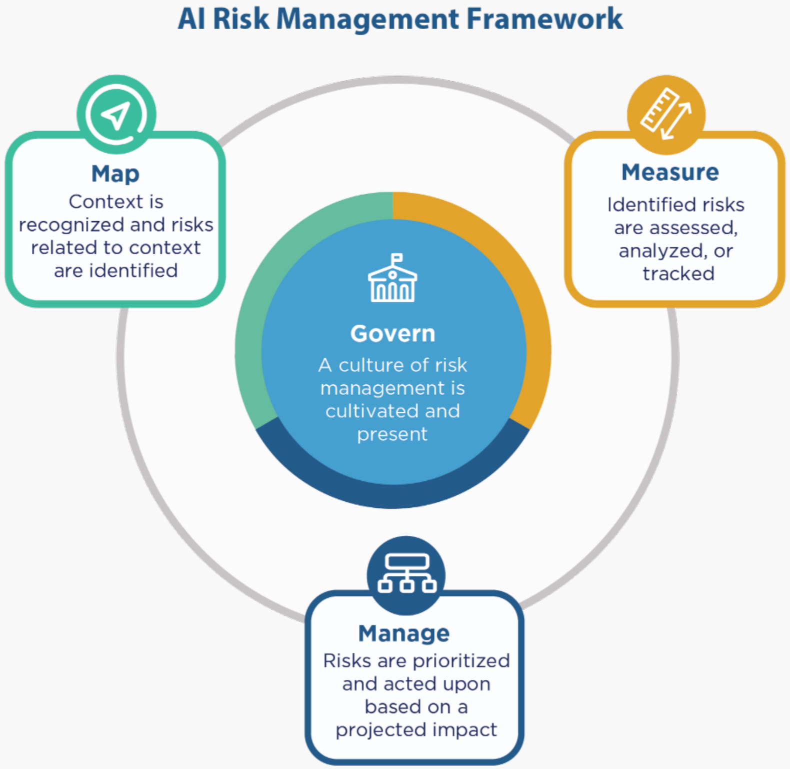
THERE ARE LOTS

The governments and industry groups of the world have not been sitting idly by,

- World Health Organization (WHO) Guidelines
- American Medical Association (AMA) Policy
- The Asilomar AI Principles
- The European Union’s Ethics Guidelines for Trustworthy AI
- The Montreal Declaration for a Responsible Development of Artificial Intelligence
- NIST AI Principles

ON SOLID GROUND

A useful, CSF-styled framework for managing risks associated with AI.



AI Risk Management Framework

Map
Context is recognized and risks related to context are identified

Measure
Identified risks are assessed, analyzed, or tracked

Govern
A culture of risk management is cultivated and present

Manage
Risks are prioritized and acted upon based on a projected impact

EXAMPLE KEY AI THREATS

- Model and Data Poisoning
- Backdoor Attacks
- Inference
- Memorization
- Training Data Reconstruction
- Confidentiality or Privacy Breach
- Bias and Discrimination
- Lack of Transparency
- Overreliance

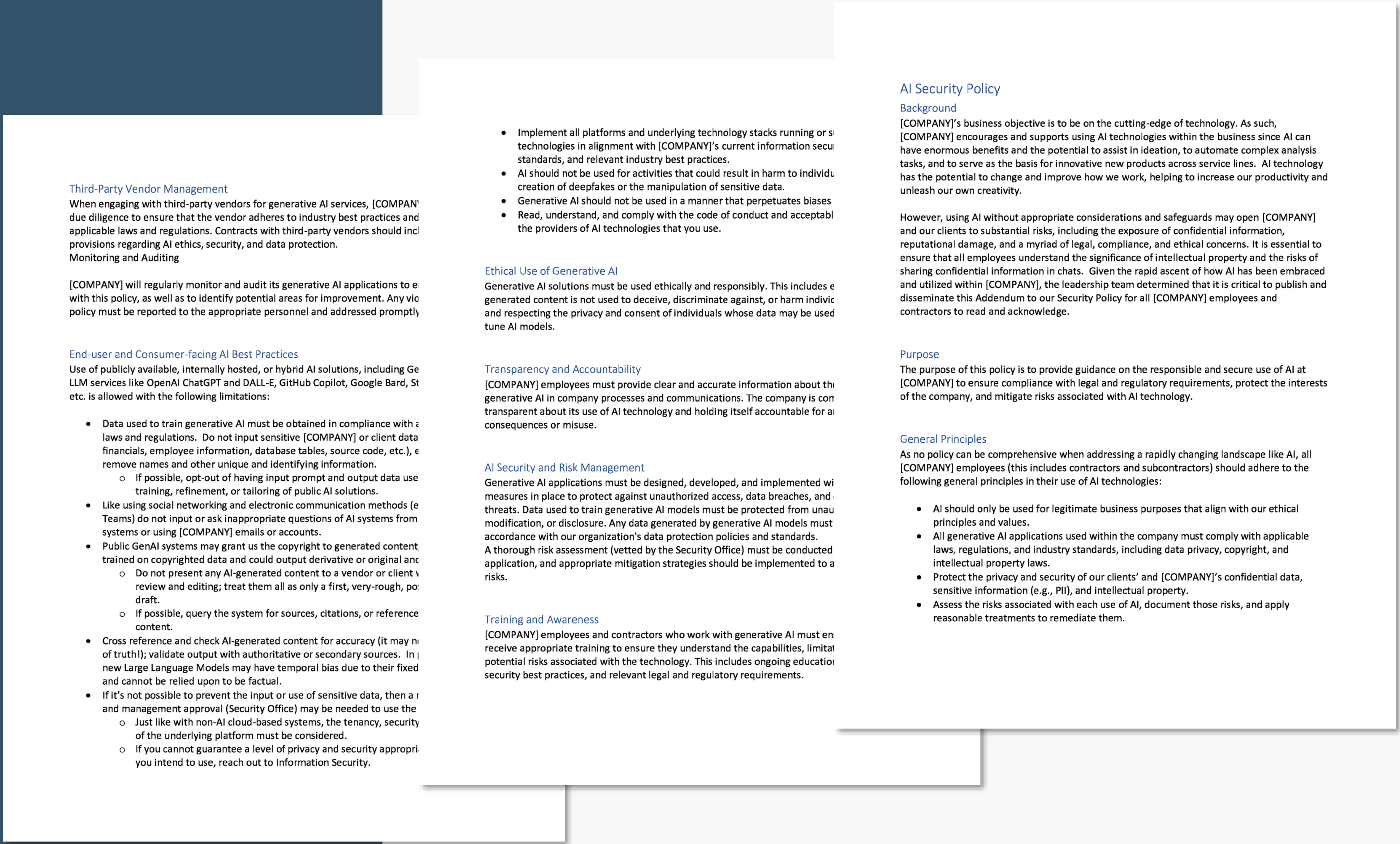
PRACTICE MANAGEMENT

Ensuring AI safety in healthcare is like being a digital lifeguard, constantly on the lookout to keep the AI swimming safely within the lanes of compliance and security protocols.

PRACTICAL AND HIPAA COMPLIANT AI USE

Establish an AI security policy

- Whatever your approach to AI is, define the expectations and rules of the road.
- Remember your people are already using, developing, or deploying AI.
- Don’t forget the AI you build.



AI Security Policy

Background

[COMPANY]'s business objective is to be on the cutting-edge of technology. As such, [COMPANY] encourages and supports using AI technologies within the business since AI can have enormous benefits and the potential to assist in ideation, to automate complex analysis tasks, and to serve as the basis for innovative new products across service lines. AI technology has the potential to change and improve how we work, helping to increase our productivity and unleash our own creativity.

However, using AI without appropriate considerations and safeguards may open [COMPANY] and our clients to substantial risks, including the exposure of confidential information, reputational damage, and a myriad of legal, compliance, and ethical concerns. It is essential to ensure that all employees understand the significance of intellectual property and the risks of sharing confidential information in chats. Given the rapid ascent of how AI has been embraced and utilized within [COMPANY], the leadership team determined that it is critical to publish and disseminate this Addendum to our Security Policy for all [COMPANY] employees and contractors to read and acknowledge.

Purpose

The purpose of this policy is to provide guidance on the responsible and secure use of AI at [COMPANY] to ensure compliance with legal and regulatory requirements, protect the interests of the company, and mitigate risks associated with AI technology.

General Principles

As no policy can be comprehensive when addressing a rapidly changing landscape like AI, all [COMPANY] employees (this includes contractors and subcontractors) should adhere to the following general principles in their use of AI technologies:

- AI should only be used for legitimate business purposes that align with our ethical principles and values.
- All generative AI applications used within the company must comply with applicable laws, regulations, and industry standards, including data privacy, copyright, and intellectual property laws.
- Protect the privacy and security of our clients' and [COMPANY]'s confidential data, sensitive information (e.g., PII), and intellectual property.
- Assess the risks associated with each use of AI, document those risks, and apply reasonable treatments to remediate them.

- Implement all platforms and underlying technology stacks running or s technologies in alignment with [COMPANY]'s current information secu standards, and relevant industry best practices.
- AI should not be used for activities that could result in harm to individu creation of deepfakes or the manipulation of sensitive data.
- Generative AI should not be used in a manner that perpetuates biases
- Read, understand, and comply with the code of conduct and acceptabl the providers of AI technologies that you use.

Ethical Use of Generative AI

Generative AI solutions must be used ethically and responsibly. This includes e generated content is not used to deceive, discriminate against, or harm indivic and respecting the privacy and consent of individuals whose data may be used tune AI models.

Transparency and Accountability

[COMPANY] employees must provide clear and accurate information about th generative AI in company processes and communications. The company is con transparent about its use of AI technology and holding itself accountable for a consequences or misuse.

AI Security and Risk Management

Generative AI applications must be designed, developed, and implemented wi measures in place to protect against unauthorized access, data breaches, and threats. Data used to train generative AI models must be protected from unau modification, or disclosure. Any data generated by generative AI models must accordance with our organization's data protection policies and standards.
A thorough risk assessment (vetted by the Security Office) must be conducted application, and appropriate mitigation strategies should be implemented to a risks.

Training and Awareness

[COMPANY] employees and contractors who work with generative AI must en receive appropriate training to ensure they understand the capabilities, limita potential risks associated with the technology. This includes ongoing educatio security best practices, and relevant legal and regulatory requirements.

Third-Party Vendor Management

When engaging with third-party vendors for generative AI services, [COMPAN due diligence to ensure that the vendor adheres to industry best practices and applicable laws and regulations. Contracts with third-party vendors should incl provisions regarding AI ethics, security, and data protection.
Monitoring and Auditing

[COMPANY] will regularly monitor and audit its generative AI applications to e with this policy, as well as to identify potential areas for improvement. Any vio policy must be reported to the appropriate personnel and addressed promptly

End-user and Consumer-facing AI Best Practices

Use of publicly available, internally hosted, or hybrid AI solutions, including Ge LLM services like OpenAI ChatGPT and DALL-E, GitHub Copilot, Google Bard, St etc. is allowed with the following limitations:

- Data used to train generative AI must be obtained in compliance with a laws and regulations. Do not input sensitive [COMPANY] or client data financials, employee information, database tables, source code, etc.), e remove names and other unique and identifying information.
  - If possible, opt-out of having input prompt and output data use training, refinement, or tailoring of public AI solutions.
- Like using social networking and electronic communication methods (e Teams) do not input or ask inappropriate questions of AI systems from systems or using [COMPANY] emails or accounts.
- Public GenAI systems may grant us the copyright to generated content trained on copyrighted data and could output derivative or original anc
  - Do not present any AI-generated content to a vendor or client v review and editing; treat them all as only a first, very-rough, po draft.
  - If possible, query the system for sources, citations, or reference content.
- Cross reference and check AI-generated content for accuracy (it may n of truth!); validate output with authoritative or secondary sources. In new Large Language Models may have temporal bias due to their fixed and cannot be relied upon to be factual.
- If it's not possible to prevent the input or use of sensitive data, then a r and management approval (Security Office) may be needed to use the
  - Just like with non-AI cloud-based systems, the tenancy, security of the underlying platform must be considered.
  - If you cannot guarantee a level of privacy and security appropri you intend to use, reach out to Information Security.

PRACTICAL AND HIPAA COMPLIANT AI USE

Regular Risk Assessments and Management

- Identify specific risks with AI handling PHI, e.g., breaches and unauthorized access.
- Implement strategies to reduce identified risks.
- Keep detailed records of risk assessments and mitigation efforts.
- Update risk assessments to accommodate new threats and changes in AI applications.

PRACTICAL AND HIPAA COMPLIANT AI USE

Robust Data Encryption and Security

- Use strong encryption for data at rest and in transit within AI systems.
- Conduct frequent audits to ensure encryption and other security measures are effective.
- Implement the latest security technologies and best practices.
- Educate staff about the importance of security measures and proper handling of encrypted data.

PRACTICAL AND HIPAA COMPLIANT AI USE

Strict Access Controls

- Ensure only authorized personnel can access PHI within AI systems.
- Implement strong user authentication protocols like MFA.
- Monitor and review access logs to detect and respond to unauthorized access attempts.
- Assign access based on the minimum necessary standard for each role.

PRACTICAL AND HIPAA COMPLIANT AI USE

De-identification of Data

- Use de-identification techniques to strip ID data before AI processing.
- Follow HIPAA guidelines for de-identifying PHI.
- Regularly test de-identified data to ensure it cannot be re-identified.
- Where possible, use aggregated data to further reduce re-identification risks.

PRACTICAL AND HIPAA COMPLIANT AI USE

Transparent and Informed Consent

- Inform patients about the use of AI with their data.
- Secure explicit consent for the use of PHI with AI.
- Reflect the use of AI in privacy notices and consent forms.
- Allow patients the option to revoke their consent and explain the implications of doing so.

PRACTICAL AND HIPAA COMPLIANT AI USE

Regular Compliance Training

- Conduct regular HIPAA training for all staff involved with AI systems.
- Keep staff informed about changes in regulations and their implications for AI.
- Use real-world scenarios to enhance understanding of compliance.
- Implement certification processes to ensure understanding and compliance.

PRACTICAL AND HIPAA COMPLIANT AI USE

Incident Response Planning

- Have a detailed plan for responding to breaches and incidents involving AI.
- Conduct drills to test the effectiveness of the response plan.
- Establish clear procedures for reporting and managing incidents.
- Analyze incidents to improve future responses and prevent recurrence.

Are there any questions?

WE APPRECIATE YOUR TIME

THANK YOU

Enjoy the rest of your day.

www.obsglobal.com

QUESTIONS?

www.obsglobal.com

Incident Response Tabletop Workshop

New York, NY In-Person Event

Tuesday, April 16, 10:30AM-3:30PM

[Register Here]

Waitlist Spots Available

Coming Soon: AI Primer and Policy & Procedures Documents developed in partnership with Manatt Health

Workshop Evaluation Survey

Please share your feedback on this session. This should take less than 3 minutes to complete.

Survey Link:
https://forms.office.com/Pages/ResponsePage.aspx?id=YSZl7iDhjEqs_lCzVbYzoqmlH89zfFNPhDWTC9uAhXZUQzMyRTlEMkJRME1FQjlINTNBUFczSUYyWC4u

CHCANYS - Online Business Systems Evaluation for Privacy and Security Considerations for AI