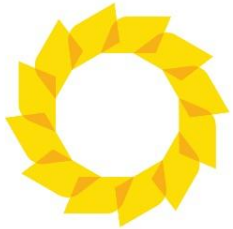


Enterprise Health

OCC HEALTH WEBINAR:
AI IN PRACTICE.
AI IN POLICY.

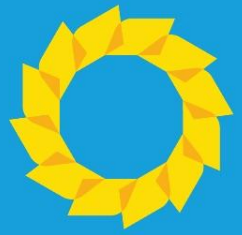
Speakers

Jeff Donnell
President, Enterprise Health

Stephanie Eckerle, JD
Healthcare Practice Chair
Krieg DeVault

Agenda

- Quick context
- Brief AI overview
- AI in action
- Governance
- Policy
- Q&A



Context

It’s here, it’s in healthcare

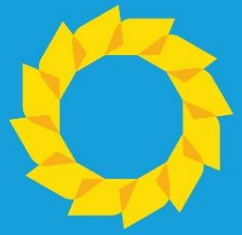
More than half of health system leaders and insurance executives are calling artificial intelligence an "immediate priority," and 73% of organizations said they were growing their financial commitments to the technology, according to a new survey, "Inside the C-Suite Payer & Provider Leaders Share Their Vision for AI."

Source: Healthcare Finance, Define Ventures Survey

Global AI in healthcare market valued at $14.92 billion in 2024, $21.66 billion in 2025, with projected CAGR of 38.6% through 20230

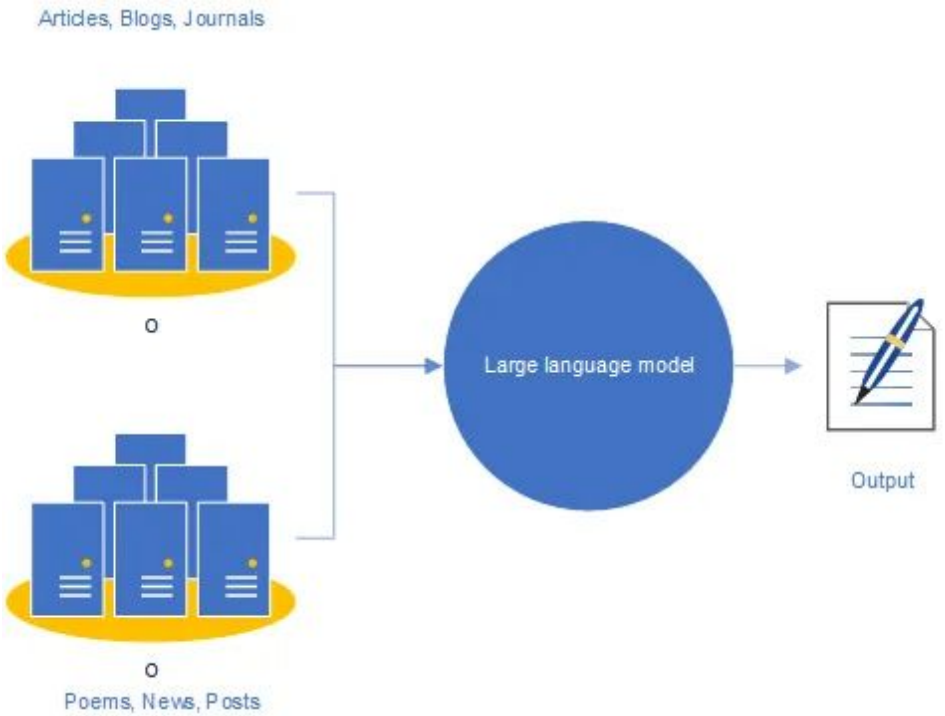
AI won’t take your job, but someone who embraces AI just might…

Enterprise Health



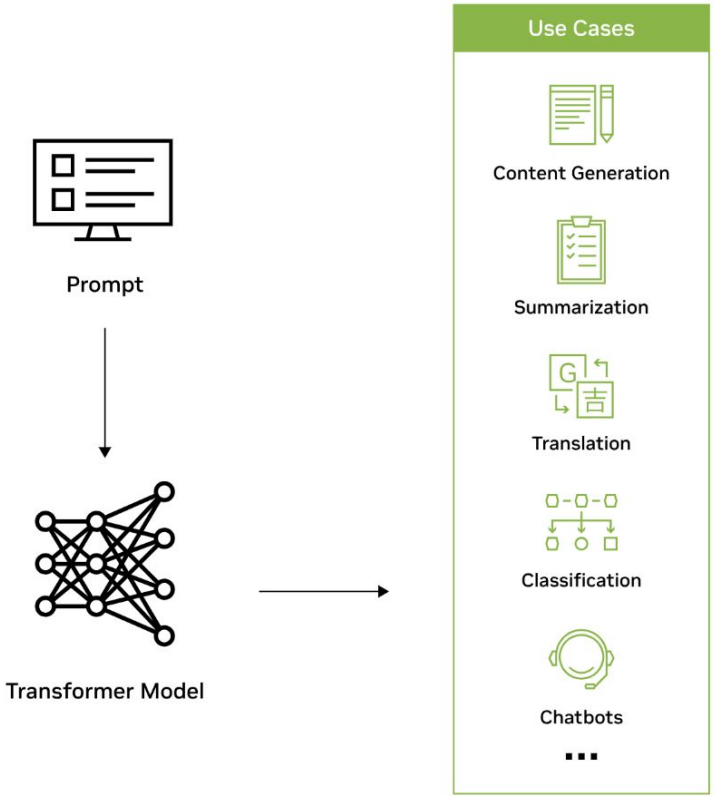
AI overview

Large Language Models (or LLMs)



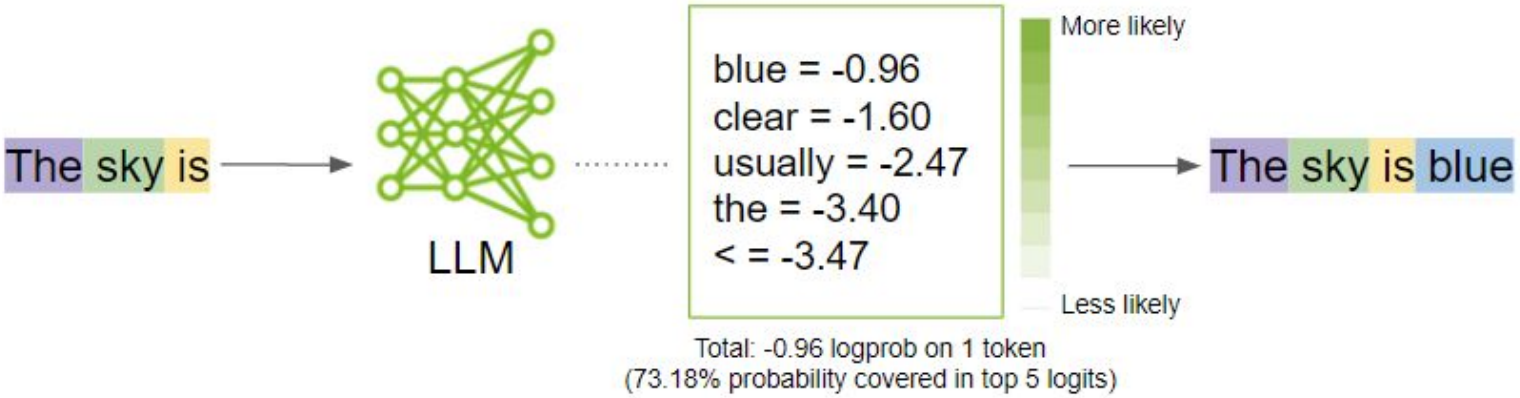
Training Data

Zooming in



Source: NVIDIA

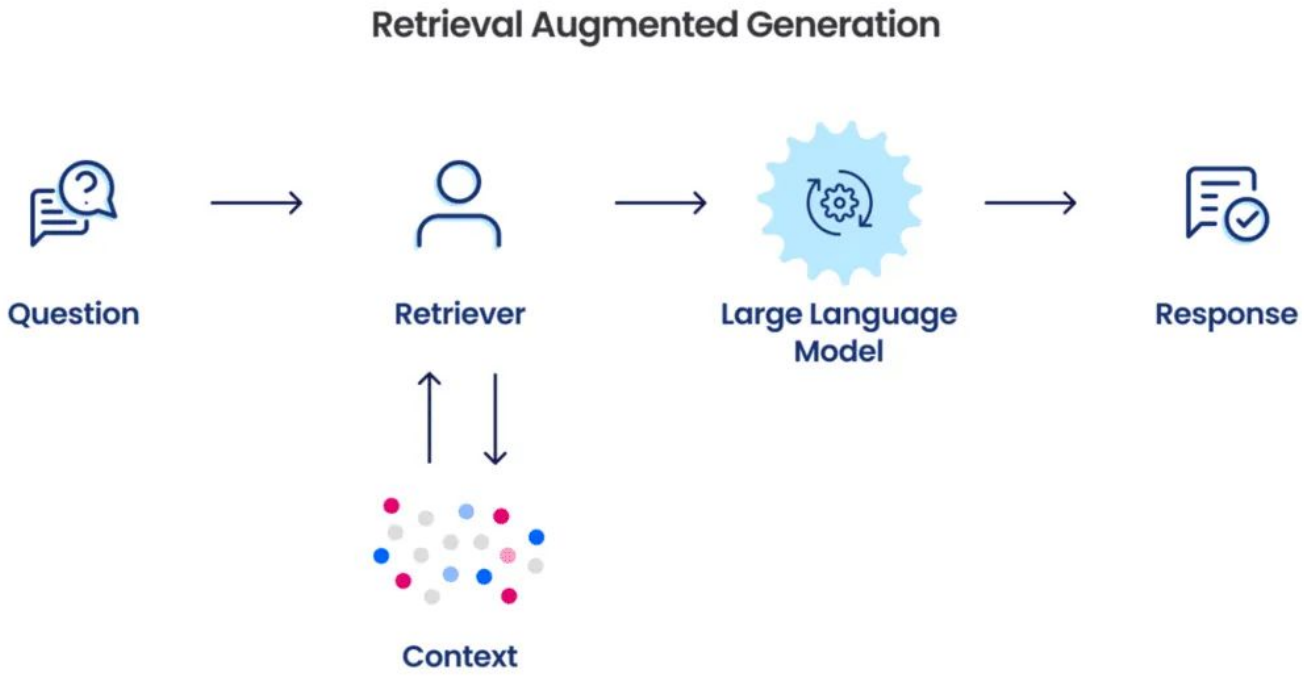
LLMs predict output



Source: NVIDIA

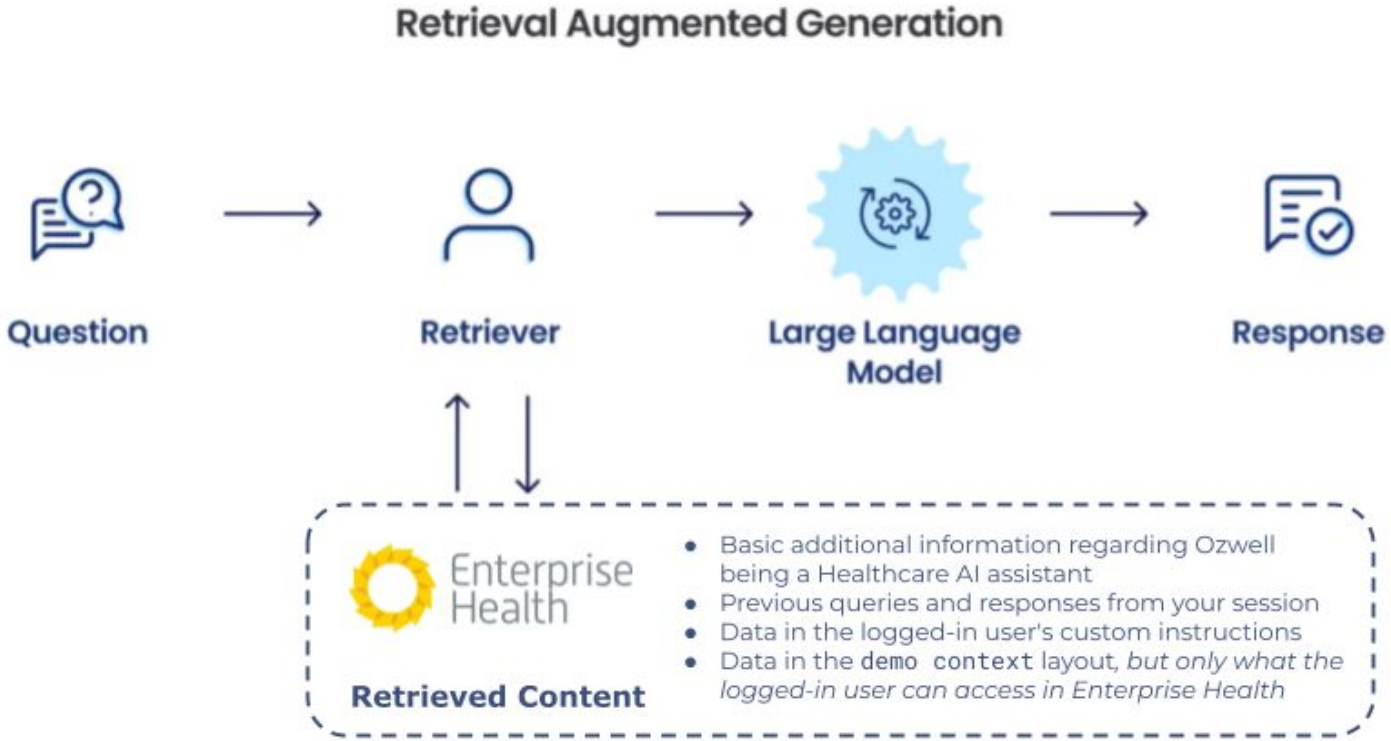
Meet Ozwell

Retrieval-Augmented Generation (RAG)

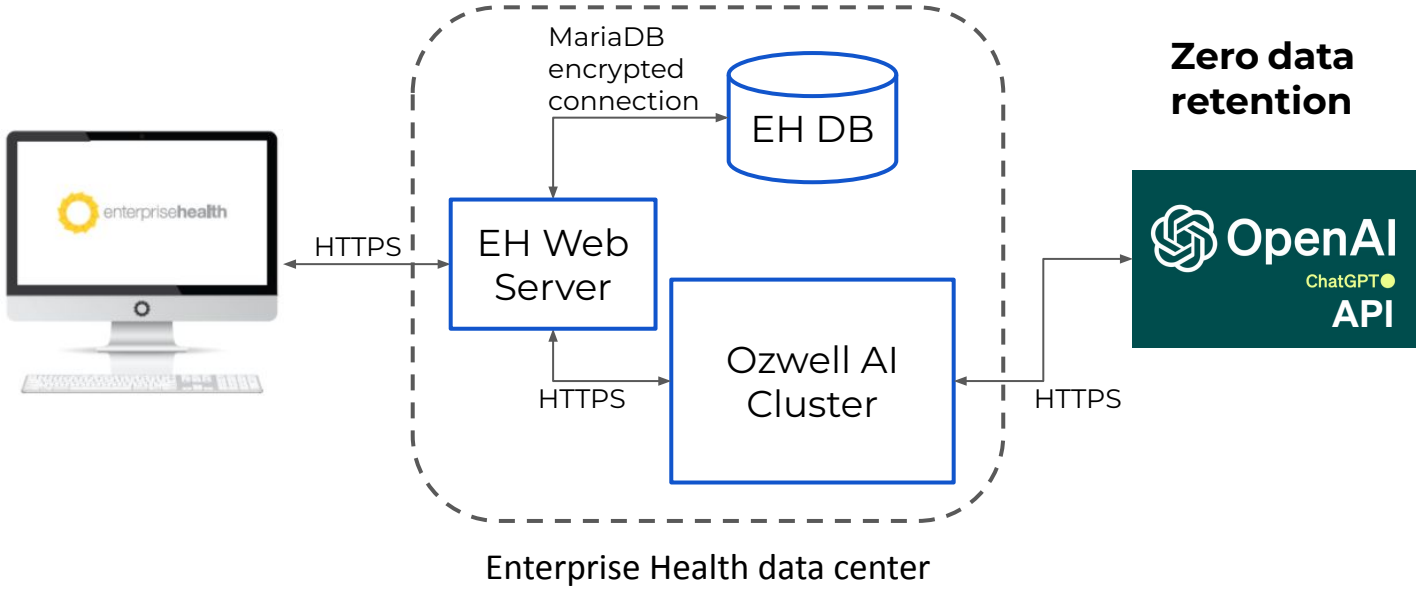


Source: TowardsAI.net

Ozwell's LLM / RAG architecture

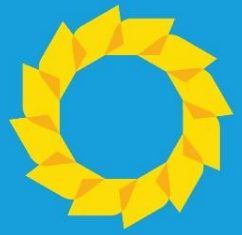


Everything encrypted, nothing retained (HIPAA compliant)



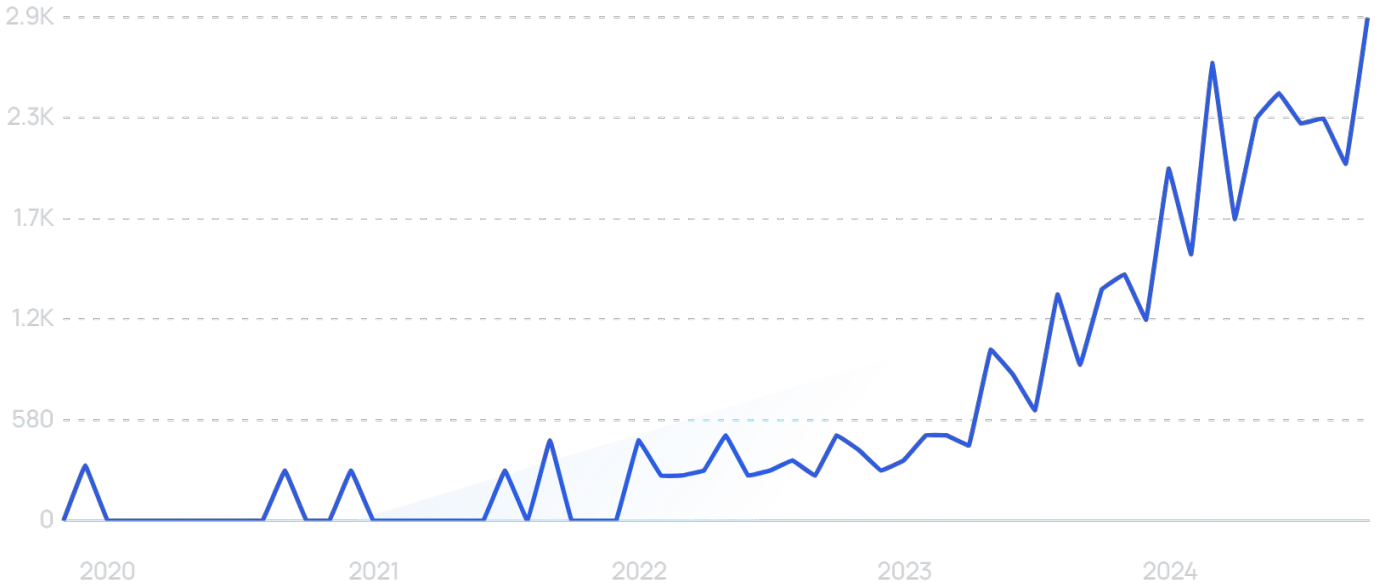
Ozwell in development

- AI driven, flex encounter with “smart actions”
- Ingestion, processing, data extraction from images, documents
- Data chaser capability - find people, interview them, collect data from them
- Reporting and analytics
- Medical surveillance setup/management
- Mental health counseling
- Immunization program management



Governance from my POV

You’re not alone



Searches for AI governance framework up 7000% over last 5 years

Source: Deloitte

AI in healthcare — risk framework

- **Fair** - Ensure outputs are unbiased and equitable, regardless of patient demographics or clinical context
- **Appropriate** - Ozwell is intended for use use as a supportive tool for healthcare professionals, not as a replacement for clinical judgment
- **Valid** - Outputs are accurate, relevant, and consistent with clinical guidelines and user prompts
- **Effective** - Results are actionable, useful and support efficient clinical documentation and workflow
- **Safe** - Ozwell is developed and maintained to minimize risks to patients, users, and organizations, with security, privacy, and risk management

More at DrummondGroup.com

Certification is serious business

ONC | Certified EHR

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations™

r2 HITRUST CERTIFIED

Regulatory Compliance

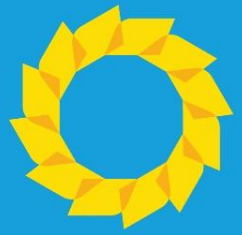
The HITRUST framework (HITRUST CSF) harmonizes over 60 regulations, standards, frameworks, and other authoritative sources and consolidates them into the most comprehensive, consistent, and clear set of controls available to achieve compliance.

HIPAA COMPLIANCE | NIST | ISO | GDPR | PCI DSS COMPLIANT

Completion of the Following pDSI Risk Management Certification:

DRUMMOND CERTIFIED™
pDSI-RISK 2025

Holds Certificate No: **pDSI-061325-01**
Date Certified: **6/18/25**



Governance from a legal POV

KRIEG DEVAULT

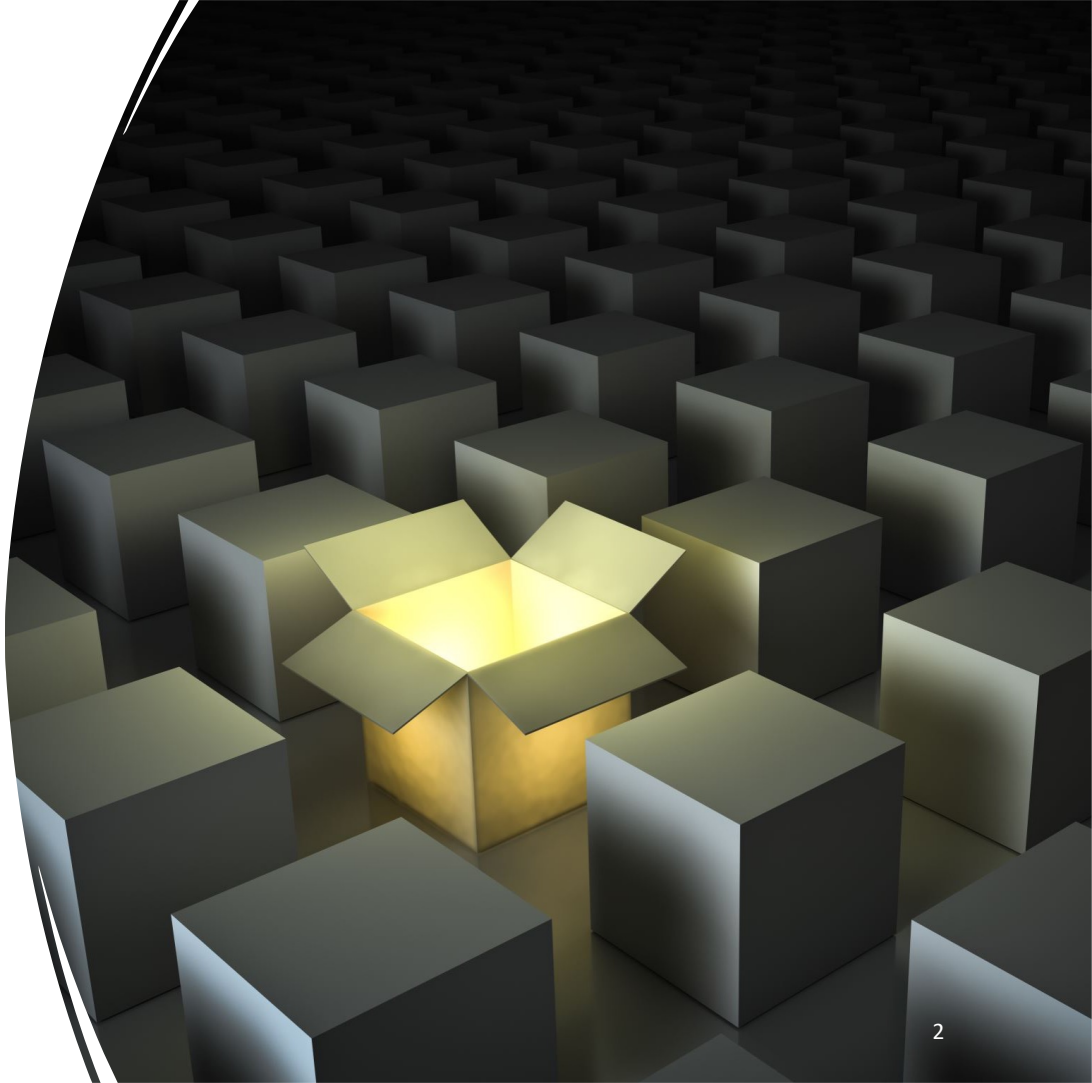
Occ Health Webinar:
AI in Practice
AI in Policy

Presented by:

Stephanie Eckerle, JD

The Artificial Intelligence Black Box

- No national framework
- Few state laws directly governing AI
- No standardized AI policies or guidelines
- Multiple AI platforms and integrations
- Ethical and discrimination concerns
- Privacy and security concerns



AI Governance Must Start at the Top

AI is a powerful tool

Your employees are using it

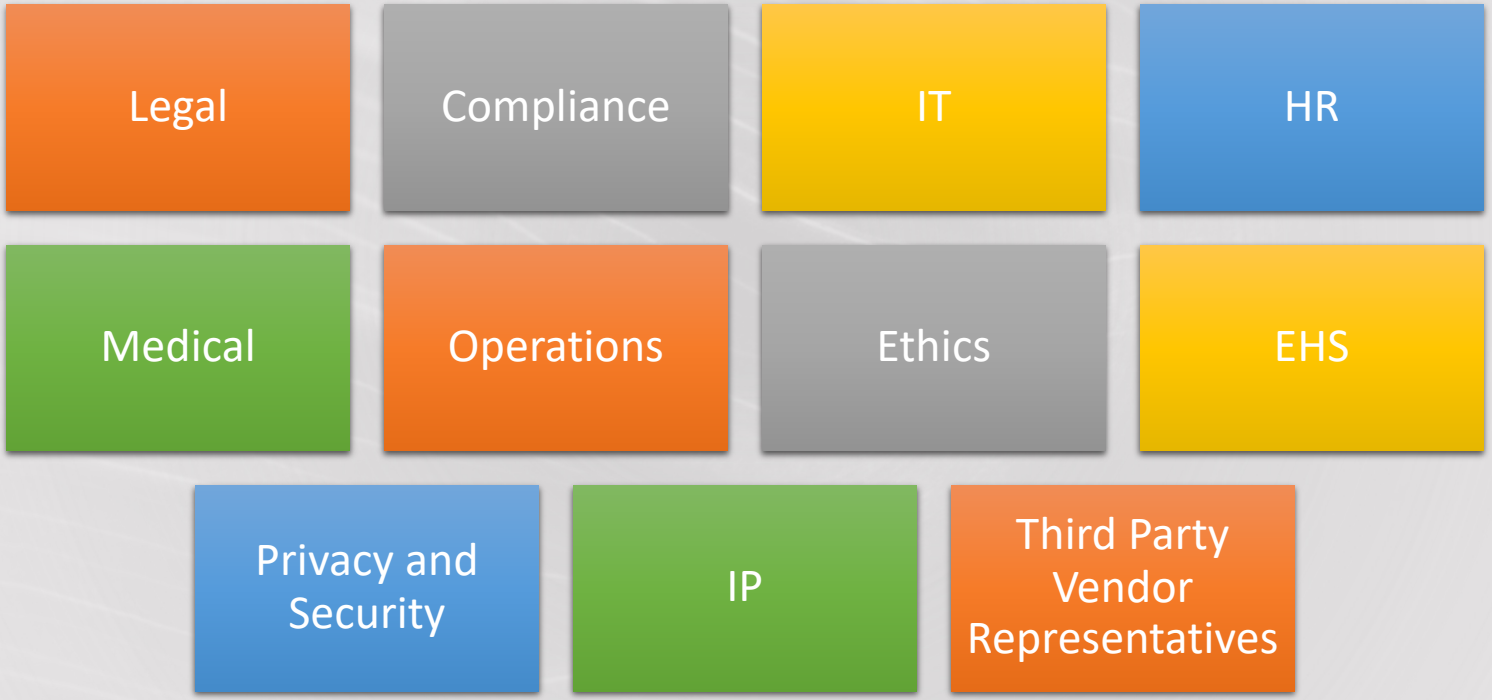
Your medical providers are using it

Your customers are using it

AI Governance Program

AI Governance Committee	General Governance Structure	Legal Framework	Rules and Ethics of Use
Privacy and Security	IP and Trade Secrets	Third Party Vendors	Occupational and Employee Health Issues

AI Governance Committee



General Governance Structure

- Statement on use, purpose, and intent
- Confidential reporting structure
- Communication of AI governance program
- Mandatory AI training
- Disciplinary process for violation of AI governance program
- Annual review and updates of AI governance program
- Review and approval (and buy-in) at the executive level

AI Legal Framework

STEP 1:

UNDERSTAND THE LAWS GOVERNING OCCUPATIONAL HEALTH SERVICES AND PROCESSING OF COMPANY DATA

Laws Governing Occupational Health and Processing of Employee Health Data

- State Privacy and Security Laws
  - Medical Records
  - Mental Health Records
  - Communicable Disease Records
  - EAP Records
  - Records of Minors
  - Provider-Patient Privilege
  - Security and Breach Reporting Laws
- State Record Retention and Access Laws
- Office of Civil Rights, US. Department of Health and Human Services
  - HIPAA for Professionals
  - HIPAA Disclosures for Workers' Compensation Purposes
  - HIPAA and Employment Records
- Substance Abuse and Mental Health Services Administration
  - Substance Use Confidentiality Regulation
- Occupational Health and Safety Administration
  - April 15, 1999 OSHA Letter, Maintenance and Transfer of Records
  - OSHA Access to Employee Exposure and Medical Records, 29 C.F.R. 1910
  - Clinician Website

Laws Governing Occupational Health and Processing of Employee Data

- Equal Employment Opportunity Commission/American with Disabilities Act
  - Employer Wellness Programs
  - Disability Related Inquiries and Medical Examinations EEOC Laws & Guidance
  - EEOC Law and Guidance

- Federal Communications Commission (FCC)
  - FCC Cyber Security and Network Reliability

- U.S. Securities and Exchange Commission (SEC)
  - SEC, Spotlight on Cybersecurity, the SEC and You
  - Commission Statement and Guidance on Public Company Cybersecurity Disclosures

- EU General Data Protection Regulation

- NIST Cybersecurity Framework (Voluntary Guidance)

- U.S. Department of Labor
  - Cybersecurity Guidance

- Office of National Coordinator (ONC)
  - Cures Act and Information Blocking

AI Legal Framework

Step 2:

Understand laws and agency guidance governing AI

Laws and Agency Statements* Governing Artificial Intelligence

- Emerging State Laws and Guidance
- Local City Ordinances
- Joint Agency Statements
  - Joint Statement on Enforcement of Civil Rights, Fair Competition, Consumer Protection, and Equal Opportunity Laws in Automated Systems
  - U.S. Cybersecurity and Infrastructure Agency (CISA) and UK National Cyber Security Centre (NCSC) Guidelines for Secure AI System Development
- U.S. Department of Justice
  - U.S. Department of Justice Criminal Division Evaluation of Corporate Compliance Programs
  - DOJ Civil Rights Division: Algorithms, Artificial Intelligence, and Disability Discrimination in Hiring.
- U.S. Health and Human Services
  - OCR: 42 C.F.R. 92.210, Nondiscrimination in the use of patient care decision support tools
  - ASTP: Clinical Decision Support

*Note that some agency statements have been retracted and by the agency and should not be relied upon but still provide helpful guidance.

Laws and Agency Statements* Governing Artificial Intelligence

- European Union
  - EU Artificial Intelligence Act
- U.S. National Labor Relations Board
  - Office of General Counsel: Memorandum on Electronic Monitoring and Algorithmic Management of Employees
- U.S. Equal Employment Opportunity Commission
  - Impact of AI On the Workplace: Latest Guidance from EEOC
- U.S. Food and Drug Administration
  - Software as a Medical Service (SaMD)
  - Artificial Intelligence and Machine Learning in Software as a Medical Device
  - Clinical Decision Support Software

*Note that some agency statements have been retracted and by the agency and should not be relied upon but still provide helpful guidance.

U.S. Department of Justice
Management of Emerging Risks

Does the company have a process for identifying and managing emerging internal and external risks that could impact the ability to comply with laws related to the use of new technologies?

How does the company assess impact of new technologies, such as AI?

Is management of risks related to use of AI and other new technologies integrated into broader enterprise risk management strategies?

What is the companies approach to governance regarding the use of new AI in its business and compliance program?

How is the company curbing the unintended consequences from use of AI?

How is the company mitigating potential for deliberate or reckless misuse of technologies by company insiders?

NLRB: Memorandum on Electronic Monitoring of Employees

In October 2022, NLRB General Counsel Jennifer A. Abruzzo published Memorandum GC 23-02 ("Memo") regarding electronic monitoring and algorithmic management of employees interfering with the exercise of rights under Section 7 of the National Labor Relations Act ("NLRA").

The Memo explores various types of technologies used to monitor employees, including recording conversations, tracking movements, monitoring employees through keyloggers and screenshotting programs, webcam photos, and audio recordings.

"An issue of particular concern to [Ms. Abruzzo] is the potential for **omnipresent** surveillance and other algorithmic-management tools to **interfere** with the exercise of Section 7 rights by significantly impairing or negating employees' ability to engage in protected activity and keep that activity confidential from their employer, if they so choose." (Emphasis added).

The Memo asserts that it is the NLRB's "responsibility 'to **adapt** the [NLRA] to changing patterns of industrial life.'" (Emphasis added). The Memo underscores the public policy consideration of safeguarding employee rights in the advent of rapid and sometimes intrusive advances in technology while also raising questions about NLRB's scope of authority under Section 7 of the NLRA.

EEOC Enforcement

EEOC v. iTutorGroup, Inc.

(Case No. 1:22-cv-2565--PKC-PK)

- August 2023: EEOC settles first lawsuit related to alleged AI discrimination in hiring
- Overview
  - EEOC settlement with a tutoring company that allegedly programmed the recruiting software to reject older applicants
  - Rejected applicants realized that they had been discriminated against after submitting a subsequent identical application with a more recent birth date
  - iTutorGroup, Inc. must pay **$365,000** to a group of rejected applicants, according to the consent decree filed August 9, 2023, in the US District Court for the Eastern District of New York

California: Artificial Intelligence in Health Care Services

Artificial Intelligence in Health Care Services

- Who: Health facilities, clinics, physician office's, group practice that utilize AI to generate written or verbal communications pertaining to ***clinical information (information relates to the health status of a patient)***
- Requirements:
  - Disclaimer stating the communication was generated by AI
  - Must be included on audio, video, and written communications
  - Instructions on how a patient can contact a human health care provider or employee of the facility
- Exemptions:
  - Does not apply to AI read and reviewed by a human licensed or certified health care provider
  - Does not apply to administrative matters, including appointment scheduling, billing or other clerical matters

California: Attorney General's Legal Advisory on the Application of Existing California Law to AI

- Comprehensive Statement from California AG on use of AI in healthcare
- Describes CA laws that may be implemented by use of AI:
  - Unfair Competition Law
  - Anti-Discrimination Laws
  - Patient Autonomy and Privacy Laws

Source: https://oag.ca.gov/system/files/attachments/press-docs/Final%20Legal%20Advisory%20-%20Application%20of%20Existing%20CA%20Laws%20to%20Artificial%20Intelligence%20in%20Healthcare.pdf

California: Attorney General's Legal Advisory on the Application of Existing California Law to AI

- Provides examples of what may be the unlawful use of AI in California:
  - Deny health insurance claims using AI or other automated decisionmaking systems in a manner that overrides doctors' views about necessary treatment.
  - Use generative AI or other automated decisionmaking tools to draft patient notes, communications,or medical orders that include erroneous or misleading information, including information based on stereotypes relating to protected classifications.
  - Determine patient access to healthcare using AI or other automated decisionmaking systems that make predictions based on patients' past healthcare claims data, resulting in disadvantaged patients or groups that have a history of lack of access to healthcare being denied services on that basis while patients/groups with robust past access being provided enhanced services.
  - Double-book a patient's appointment, or create other administrative barriers, because AI or other automated decisionmaking systems predict that patient is the "type of person" more likely to miss an appointment.
  - Conduct cost/benefit analysis of medical treatments for patients with disabilities using AI or other automated decisionmaking systems that are based on stereotypes that undervalue the lives of people with disabilities.

New York City Ordinance

- Automated Employment Decision Tools (Local Law No. 144)
- Effective January 1, 2023
- Overview (Conduct “Bias Audit,” Publish, Inform)
  - Employer may not use automated employment decision tools unless the tool has gone through a **bias audit** conducted no more than one year prior to its use
  - **Summary of results** of the most recent bias audit must be made publicly available on employer’s website or employment agency before the use of the tool
  - **Requires employer to notify** applicants who resides in NYC that an automated employment decision tool will be (1) used to assess or evaluate them; and (2) job qualifications / characteristics that the tool will use in the assessment

Illinois Laws

Biometric Information Privacy Act

"Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry

Requires private entities to obtain informed consent before collecting biometric data, include purpose and length of retention

Restricts sale and disclosure of biometric data unless statutory requirements are met

Requires detailed record retention and destruction policies

Numerous lawsuits have arisen including the AI context due to the use of biometric data in AI

Artificial Intelligence Video Interview Act (820 ILCS 42/1)

Applies to all employers that use AI technology to analyze applicant interview videos for Illinois-based positions

Employers must notify applicants prior to the interview that AI may be used in assessing the viability of the candidate for the position

Requires employers to provide information to applicants "before the interview explaining how the artificial intelligence works and what general types of characteristics it uses to evaluate applicants"

Requires employers to obtain consent from the applicant to be evaluated by the AI technology

Requires employers to annually report demographic data to the Department of Commerce and Economic Opportunity, if employer relies on AI in certain circumstances.

AI Governance:

Specific Considerations for Medical Services

- Practitioners must use independent medical judgment based on individual circumstances
- AI is not a replacement for prevention, diagnosis, or treatment of disease or condition
- Practitioners must verify all input and output of all data from AI
- Practitioners must verify all studies, research, or medical journals referred to by AI
- Risk mitigation plan for patient care decision support tools that utilize AI if factors of race, color, national origin, sex, age or disability are utilized

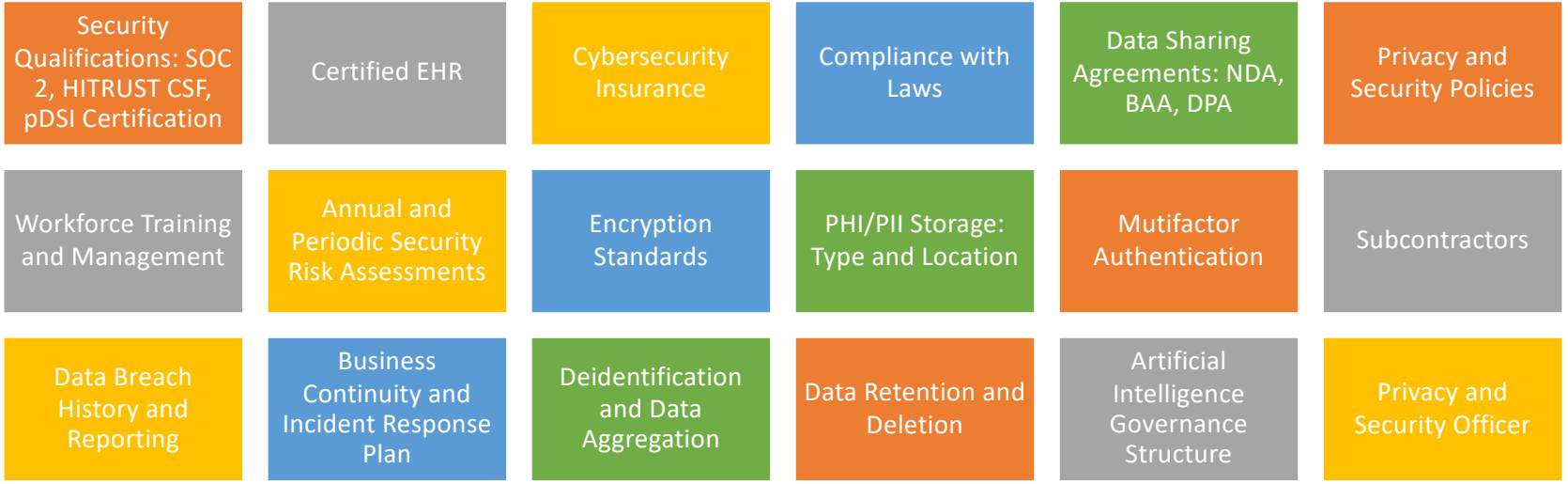
AI Governance:

Specific Considerations for Medical Services

- Determination of if patient notices or consents must be utilized when using AI
- AI is not to be used for clinical research unless approved by an institutional review board
- Third Party Payor requirements should be reviewed for compliance when utilizing AI
- Third party vendors should be vetted for AI considerations
- Review insurance coverage for use of AI

Vendor Vetting: Are you asking the right questions?

Vendor Vetting



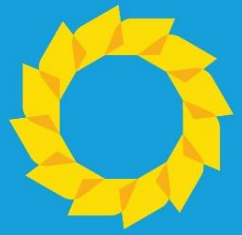
Questions?

Stephanie T. Eckerle
seckerle@kdlegal.com
317.238.6373

DISCLAIMER:

The contents of this presentation should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The contents are intended for general informational purposes only.

This presentation may constitute attorney advertising. Krieg DeVault LLP, Indianapolis, Indiana is responsible for this content unless otherwise noted. Certain images are royalty-free stock images.



Thank you!