Risk and Opportunities of AI Regarding Health Care & Managed Care Organizations

Hovannes Daniels, VP, Care Delivery Data & Analytics

Belinda Luu, Senior Counsel, Strategic Leader of AI & Data Governance

Kaiser Permanente

January 30, 2024

KAISER PERMANENTE®

Agenda

1.	AI bills, laws, regulations, and litigation that apply to health care and managed care organizations	Belinda Luu Senior Counsel, Strategic Leader of AI & Data Governance
2.	AI governance, frameworks, opportunities, and use cases	Hovannes Daniels VP, Care Delivery & Analytics
3.	AI employee guidelines and policies	Belinda Luu Senior Counsel, Strategic Leader of AI & Data Governance

AI Healthcare Bills, Laws, Regulations, and Litigation

Belinda Luu, Senior Counsel, Strategic Leader of AI & Data Governance

Risk and Opportunities of AI Regarding Health Care & Managed Care Organizations | January 30, 2024

KAISER PERMANENTE®

AI Uses By Manage Care and Healthcare Organizations

Managed Care & Healthcare

- Membership, billing, enrollment
- Claims payment, correspondence
- Clinical care delivery, telehealth
- Provider & network
- Sales & marketing
- Customer Service

Other Roles / Uses

- HR, employment
- Communications, marketing
- R&D, Clinical research
- Facility security
- Procurement
- Finance, accounting

Focus of AI Healthcare Bills, Laws, and Regulations

Automated decision-making

Privacy

PHI / PII

Mental health

Clinical decision support

Discrimination and bias

Medical devices

Federal Laws, Regulations, and Initiatives

BIDEN EXECUTIVE ORDER

HHS to establish (90 – 365 days):

- **HHS AI Task Force**
- **Strategy, policies, and possible regulatory action** to determine whether AI-enabled technologies in the health and human service sector (incl. R&D, drug/device safety, healthcare delivery and financing, and public health).
- **Understanding of, and compliance with, federal nondiscrimination laws** by HHS providers
- **Establish AI Safety program**
- **Strategy for regulating the use of AI or AI-enabled tools in drug-development processes**

Security and Data Management

- **Commerce Department** to establish guidelines and best practices to promote industry standards for developing safe, secure, and trustworthy AI (e.g., NIST RMF).
- **Red Teaming**: developers of foundation models that poses a serious risk to national public health and safety must **notify** the **federal government when model training**, and share results of all **safety tests**
- **DHS** shall develop a **training, analysis, and evaluation program** to mitigate AI-related IP risks.
- **Methods to detect AI generated content** – AI watermarking to detect AI content, authentication systems

HHS developed its **2021-2024 AI Strategic Plan** to oversee AI use in the health industry and leverage AI to reduce healthcare regulatory burdens

U.S. Laws, Regulations, and Initiatives

FDA's AI/ML-Based Software As Medical Device (SaMD) Action Plan

- Software as a Medical Device requirements and in addition:
  - April 2019: FDA released a discussion paper "Proposed Regulatory Framework for Modifications to AI/ML-Based Software as a Medical Device (SaMD) - Discussion Paper and Request for Feedback."
  - January 2021: FDA published an AI/ML-based SaMD "Action Plan" on FDA's development of a proposed regulatory framework for AI/ML-based medical devices.
- **Be aware of SaMD requirements if licensing or creating a SaMD**

ONC NPRM Regulations on HIT-1:

- Establishes a "**Decision Support Interventions**" (DSI) **certification criterion for EHR vendors to** create **new technical, transparency and risk-management requirements for certified Health IT Modules** that enable or interface with **certified EHR technology** intended to **support decision-making** based on predictive algorithms or models.

National Association of Insurance Commissioners (NAIC) Model Bulletin (in draft) - Use of Algorithms, Predictive Models & AI Systems By Insurers

- Use of AI systems is subject to the **Department's examination and investigation**, and **provide information and documentation,** including policies, procedures, data sources, algorithms, models, validation, testing, auditing, and contracts with third parties
- Insurers to **develop, implement, and maintain a written program for AI use** to assure their **decisions are accurate and fair,** and comply with **legal and regulatory standards**
- Insurer's Program should include **governance, risk management, internal controls, and third-party oversight**

State Law

Georgia Code 31-12-12 (HB 203): Practice of medicine

- **Prohibits** AI use as the **"sole basis"** for issuing a **eyeglasses prescriptio**n and requires **clinician to validate** specific data.

Colorado SB 21-169 (2021):

- Prohibits an insurer from **insurance practices that result in unfair discrimination** of a protected class.
- Insurers accountable for testing their **big data systems** to ensure they are not unfairly discriminating against consumers on the basis of a protected class
- Establish and maintain a **risk management framework** designed to determine if use of external data sources **unfairly discriminates** against individuals
- Provide **risk assessment results** and actions taken to minimize the risk of unfair discrimination

California AB 1502 (Law): Discrimination – Clinical algorithms

- Prohibits a **health care service plan** to **discriminate** on the basis of race, color, national origin, sex, age, or disability through the use of **clinical algorithms in its decision-making**
- Does not prohibit use of clinical algorithms that rely on variables to appropriately make decisions

Illinois SB. 2314: Safe Patients Limits Act (Pending): Nurse Professional Judgement

- **Provides for maximum number of patients** that may be assigned to nurses in specific situations, regardless of the use of remote monitoring systems
- **Software tools to set staffing levels** must be **"transparent in all respects"** including the methodology of determining staffing levels
- **Health facilities** cannot adopt a policy that **substitutes AI** or other technology output **for registered nurse professional judgment**

State Bills

California AB-331: Discrimination - Automated decision tools (ADTs)

- Requires AI developers and deployers (> 25 employees) to:
  - Conduct **annual impact assessments** and report on the algorithms to the California Civil Rights Department.
  - Maintain a **governance program**
  - Notify individuals **of automated processing for "consequential decisions"**
    - "**Consequential decision**" that has a significant effect on **individual's life** which includes **health care, health insurance, family planning, and employment.**
- Individual **opt-out rights** and request an alternate selection process / accommodation
- **Publicly disclose:** ADT types in use and how algorithmic discrimination risks are managed
- **Enforcement:** administrative fines (both developers & deployers)

GA legislation HB887:

- **AI Prohibition:** prohibits **sole use of AI** in making decisions regarding **insurance coverage, healthcare, and public assistance**.
  - Decision to deny, limit, or reduce **insurance coverage or a treatment** must be **reviewed by a human**
  - Prohibits AI use in patient **diagnosis, treatment, or prescription**, unless AI is supervised by a **licensed physician**

Massachusetts H.1974 (Pending): Mental Health AI

- Use of AI in the provision of **mental health services** by a mental health professional requires **approval of the state licensing board**
- AI systems must be "designed to prioritize **the safety and well-being of individuals** seeking treatment. . . **continuously monitored by a licensed mental health professional** to ensure its safety and effectiveness."
- Patients must be **notified and have an opt out right**

Applying Existing Healthcare Laws to AI

- **Privacy and Data**
  - **Regurgitation** and **Reidentification**
  - **Consumer grade tools are not HIPAA compliant**
  - **Rights and permissions to the data** training the AI tool, including check data agreements
  - **Privacy Policy and Terms of Use** – proper disclosures
  - **Vendors use of the data** – data brokers, data use restrictions
  - **Data hosting, location,** and **transfer** by the vendor/subcontractor, follow the sun 24/7 support - **CMS disclosures Medicare Advantage**
  - **Tracking technologies** – HHS OCR rules for Covered Entities regarding tracking technologies, cookies and pixels, on websites and mobile apps to comply with HIPAA

- **Telehealth/Video, and Listening Technologies**
  - **State and federal privacy regulations** - consents
  - **State wiretapping statutes require consents for recording**

- **Auto-generated or Auto-populated Documentation/Notes/Orders, and Transcriptions and Summaries**
  - **Hallucinations, accuracy and completeness**
  - **<u>Hospital and licensed facility requirements</u> to authenticate medical records and orders**
  - Requires **clinician validation and judgement, and approval for orders**
    - CMS guidance: “**Avoid generating a note that does not require some action on the part of the provider”**
  - **Government Program** require **coding and billing accuracy** e.g. Medicare program requirements
  - **Medicare Program Integrity Manual:**
    - Healthcare services **ordered** needs to be **authenticated by the person responsible for the care**
    - **If a scribe is used, the physician/NPP must sign to confirm information accuracy**
  - **False claims, upcoding, overdocumentation** e.g. CMS guidance, False Claims Act

Applying Existing Laws, Regulations to AI

- **Claims/Risk adjustment, ajudication, submissions**
  - **CMS** prohibits **automated decision making with no clinician review of the record**
  - Health Plan and clinicians **still responsible for decisions**
    - CMS guidance:
      - "**Avoid generating a note that does not require some action on the part of the provider**"
      - "**Set policy requiring the provider to review and edit all defaulted data to ensure recording only patient-specific data for that visit**."

- **Non-Discrimination, bias, health equity: E&O**
  - Has the **application or training data** and **AI generated output been vetted for a biased or discriminatory impact**
    - Denial of care or claims, care coverage, claims adjustment, coding suggestions, risk adjustment, benefits decisions;
    - Ask for vendor's bias assessment report;
  - **California Department of Insurance Bulletin 2022-5: Insurers using of AI tools need to vet them to comply with existing insurance discrimination laws**
  - **Facial Recognition Cameras** – bias and accuracy; space (privacy concerns)

- **Content generation – copyrights and right of publicity e.g. marketing and communications teams**
  - **Chatbot and virtual assistants on customer care and marketing websites** – identifying its AI not a human/clinician
  - Marketing and member/patient communications and emails
    - **Identifying GenAI generated content, watermarking**
  - **Deep fakes, image generation**
  - **Right of publicity** – tone and style
  - FTC – **false and misleading business practices and advertising**

Litigation Claims

- **Coverage Decisions:** *Joanne Barrows v Humana (D. Kentucky 2023); Estate of Gene B. Lokken v UnitedHealth Group (D. Minn 2023)*
  - Allegedly making **coverage decisions in place of medical professionals' judgment**
  - Allegedly **restrict medically necessary care** for Medicare Advantage patients

- **Claims Rejection:** *Kisting-Leung v Cigna (E.D. Cal. 2023)*
  - Used its own AI algorithm to **reject claims -** 300,000 rejected over 2 months
  - Alleged violation of **CA Standards for Prompt, Fair and Equitable Settlement law** (10 CCR §2695.7(d)):
    - **"thorough, fair and objective" investigation** into each patient claim

- **Claims Denial:** *Estate of Gene B. Lokken v United Healthcare* (D. Minn 2023)
  - Alleges that **UHC improperly used an AI Model to deny extended care claims** for elderly patients based on **erroneous health care determinations** generated by AI

- **Risk adjustment and auto-note population:** *Ormsby v Sutter* (Cal 2020)
  - Alleges that **EHR auto-pulled diagnoses codes from a problem list into the provider's assessment notes** and **physicians did not review them**.

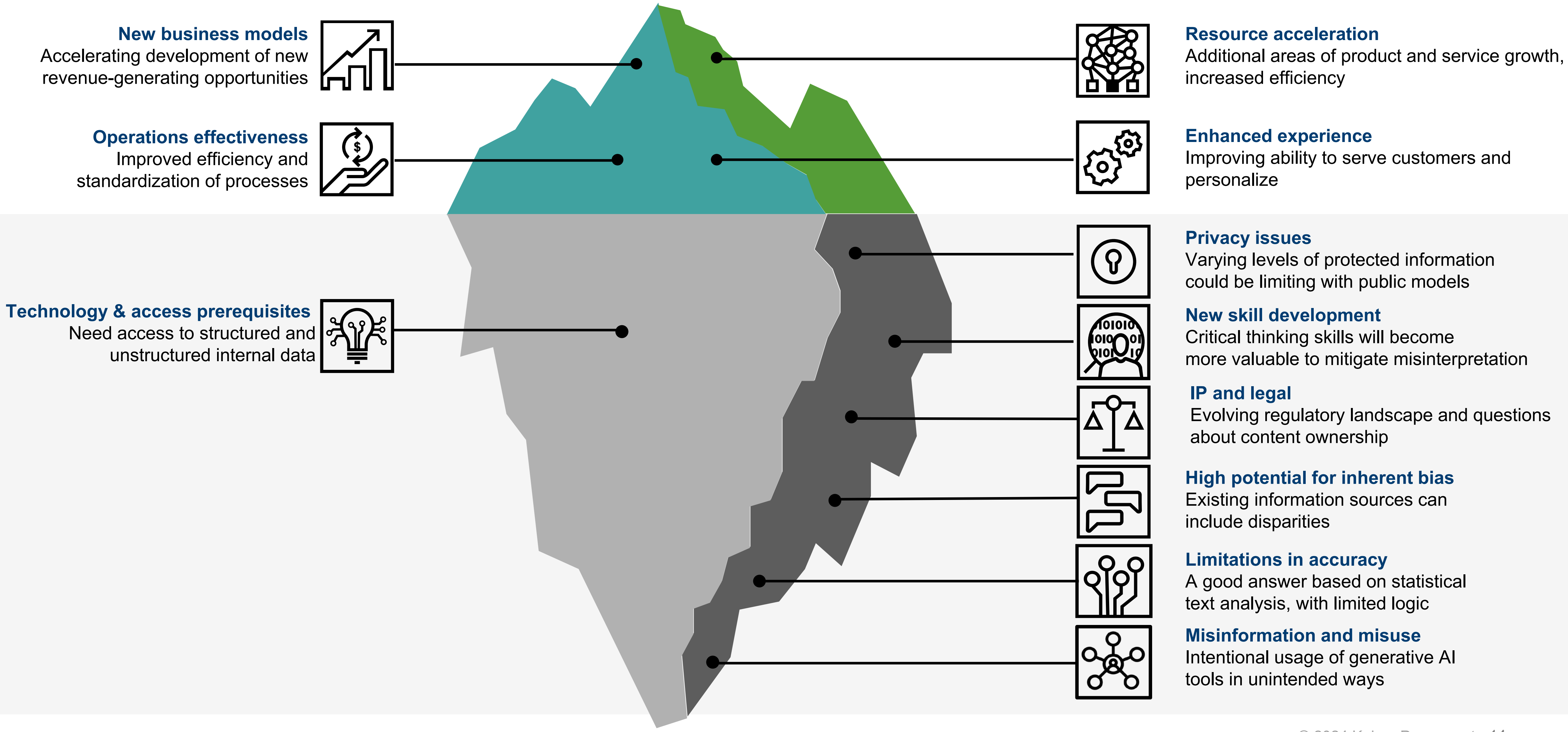
AI governance, frameworks, opportunities and use cases

Hovannes Daniels, VP, Care Delivery Data & Analytics

Risk and Opportunities of AI Regarding Health Care & Managed Care Organizations | January 30, 2024

KAISER PERMANENTE®

Adopting AI is not simple for an organization and has many obvious and not so obvious components; navigating the balance between risk and opportunity is key



New business models
Accelerating development of new revenue-generating opportunities

Operations effectiveness
Improved efficiency and standardization of processes

Technology & access prerequisites
Need access to structured and unstructured internal data

Resource acceleration
Additional areas of product and service growth, increased efficiency

Enhanced experience
Improving ability to serve customers and personalize

Privacy issues
Varying levels of protected information could be limiting with public models

New skill development
Critical thinking skills will become more valuable to mitigate misinterpretation

IP and legal
Evolving regulatory landscape and questions about content ownership

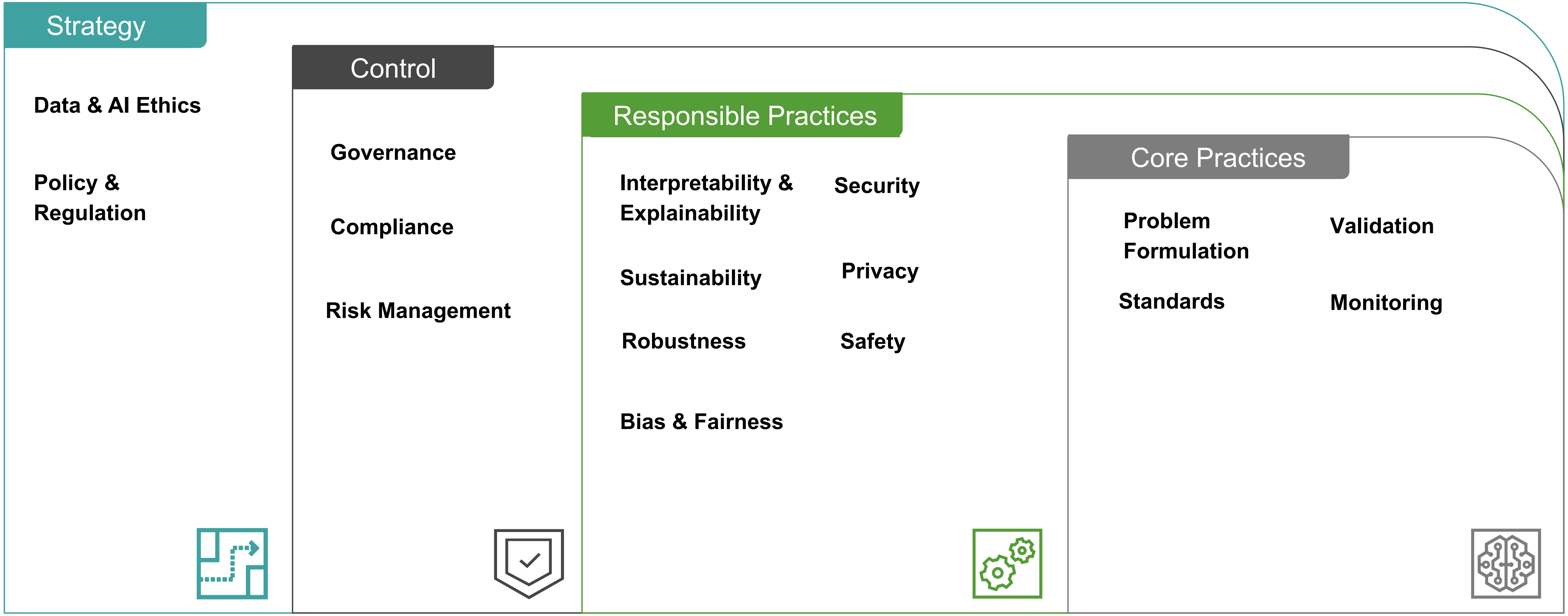
High potential for inherent bias
Existing information sources can include disparities

Limitations in accuracy
A good answer based on statistical text analysis, with limited logic

Misinformation and misuse
Intentional usage of generative AI tools in unintended ways

Becoming an AI-enabled organization requires developing a responsible AI strategy and framework with appropriate controls, policies and practices

Responsible AI at its core is simply good data science, governed by key guiding principles and made operational **from strategy to execution.**



Strategy

Data & AI Ethics

Policy & Regulation

Control

Governance

Compliance

Risk Management

Responsible Practices

Interpretability & Explainability

Security

Sustainability

Privacy

Robustness

Safety

Bias & Fairness

Core Practices

Problem Formulation

Validation

Standards

Monitoring

A responsible AI framework and governance structure will help achieve these minimally necessary operational objectives

- Consistency of risk management practices
- Transparency and compliance with regulation
- Enablement of innovation and adoption of AI
- Ability to cater to local market needs and objectives
- Consistency and coordination in use of AI tools and technologies

Achieving these goals requires a trade-off between governance requirements and flexibility in how teams develop and manage AI tools

Components of a comprehensive Responsible AI framework

Responsible AI Framework Components	
AI Principles and Risk Management	AI Principles and Policy
	AI Risk Taxonomy & Tiering
	Risk Management Guidelines & Best Practices
	Regulatory Scanning, Tracking, and Compliance
AI Risk Governance	Operating Model and Roles & Responsibilities
	Governance Committee and Escalations
	AI Use Case Inventory
	AI Use Case Intake Assessment
Culture & Awareness	Training and Communication
	Educational Resources
Application Lifecycle	AI Development and Deployment Standards and Requirements
	Testing
	Continuous Monitoring Standards and Requirements
	Risk Mitigation Tracking and Reporting

Implementation Considerations

- Determine which components to centralize, federate, or localize based on the organization's needs
- Decide what the organization is optimizing for flow vs control
- Establish foundational/design centrally while allowing teams to make more granular application-level execution decisions locally

A robust responsible AI approach is anchored in two foundational capabilities

Risk Tiering Framework

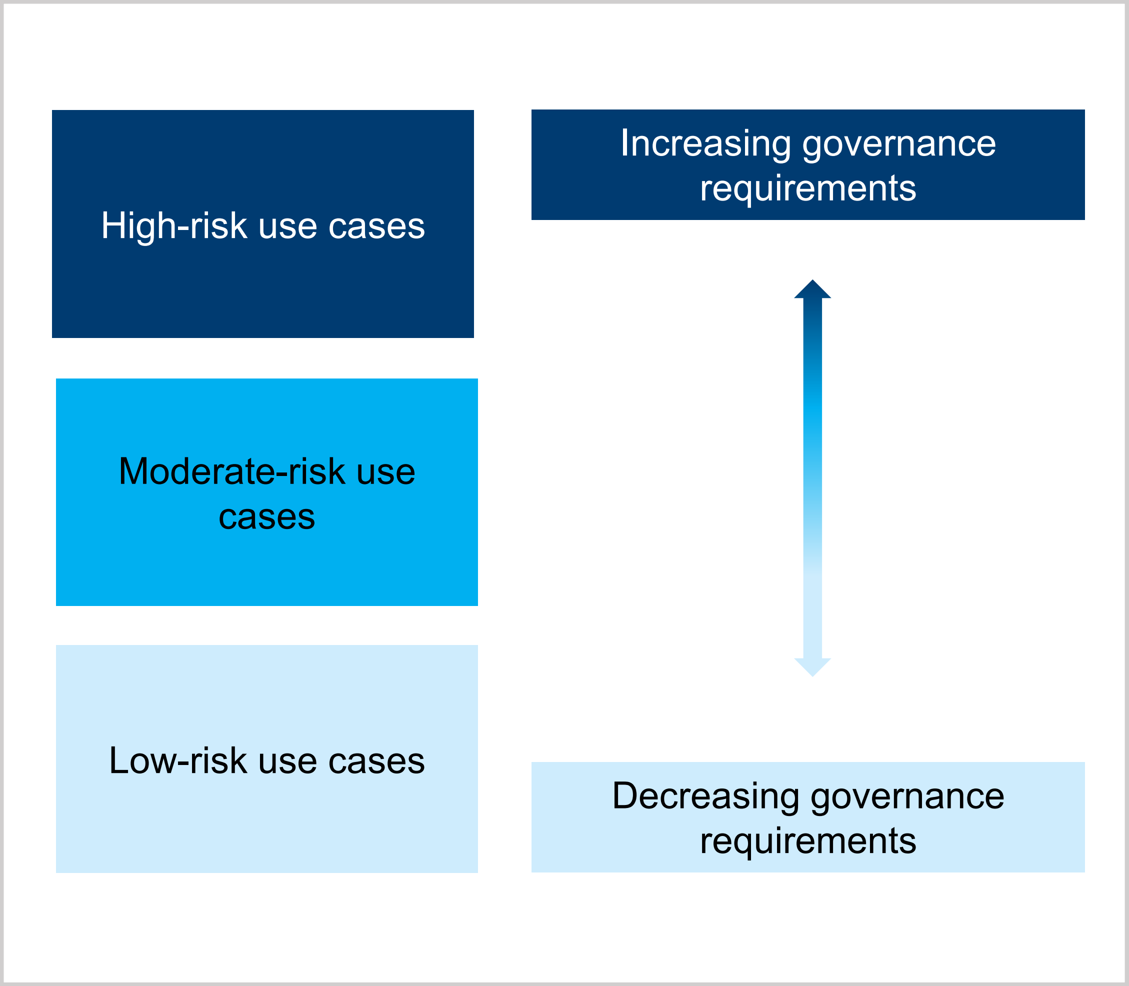
- Determine the inherent riskiness of an AI use case based on key characteristics such as the area of application and type of data uses
- Assign the level of governance and control required based on the inherent risk level

Risk Taxonomy

- Establish a taxonomy to enable the consistent definition and identification of risks created by AI use cases
- Enable a structured approach to risk management and mitigation throughout the AI lifecycle

A risk-based approach allows for organizations to balance speed and safety

- Not all use cases will pose the same level of risk; risk can be remediated for certain use cases.
- A key characteristic of an effective and efficient responsible AI framework is a risk-based approach that adjusts governance requirements based on inherent risk.
- For example, a high-inherent-risk use case might have more rigorous and frequent testing requirements compared to a lower-risk use case.
- Leading-practice risk tiering frameworks involve a small set of targeted questions to indicate the inherent riskiness of a use case.
- Through an efficient and scalable questionnaire, organizations can assign use cases a high, moderate, or low risk rating, which then determines the downstream governance requirements.


High-risk use cases
Moderate-risk use cases
Low-risk use cases
Increasing governance requirements
Decreasing governance requirements

The risk tier informs the level of governance needed

The ultimate objective of the risk tiering framework is to enable an effective and efficient governance process that focuses time and resources on higher-risk use cases while subjecting lower-risk tools to a baseline set of commensurate expectations

Illustration of how governance requirements might be adjusted

Example governance lever	Lower Risk	Higher Risk
Committee review	Approval can be obtained at the local committee level depending on the use case	In-depth review and challenge by designated committee centrally
Documentation	More basic documentation focusing on model purpose, data sources, etc.	Extensive documentation detailing the development process, data lineage, testing results, etc.
Testing frequency and depth	Periodic testing for key areas of concern	Rigorous and more frequent testing protocols covering the full range of areas in the risk taxonomy
On-going monitoring	Limited requirements beyond basic performance measurements	Continuous monitoring of performance, impact, and compliance metrics
Contingency planning	Simple contingency plan with fallback to manual process or simpler tool	Comprehensive contingency plan with detailed playbooks and protocols

Risk tiering framework can account for this committee review from a central governance perspective

Depending on the riskiness of the use cases, these are additional dimensions to consider to enable effective governance

Typical areas of concern map to priority themes and responsible AI principles

Typical Areas of Concern	Risk Taxonomy	Mapping to Principles
Life, Health, Privacy, Safety	**A. Managing Adverse Outcomes** Harm, damage, or loss that can be experienced by individuals, organizations, or systems due to failures in the AI application	Privacy-protecting Reliable Customer-focused
Member Services		
Reputation and Brand		
Regulatory and Legal		
Financial		
Operational		
Protected Classes +	**B. Model Risks** Risk related to the training, development, and performance of the AI system, including conceptual soundness, performance, efficacy, fairness, and explainability	Equitable Trustworthy Transparent
Marginalized Groups		
Social Determinates of Health		
Mental Health		
Discrimination		
Employment Decision		
Medical Device		
Data Quality and Reliability	**C. Data Risks** Risk related to the collection, processing, storage, management, and usage of data during the training and operation of the AI system and issues that arise with inaccurate, biased, incomplete, manipulated, or unreliable data, impacting the overall integrity of the data used to train AI models	Outcome-driven
Security and Robustness	**D. System and Third-Party Risks** Risk related to the security and robustness, including cyber threats; AI system vulnerabilities; adversarial attacks	Privacy-protecting
Clinical Decision Support	**E. Use Risks** Risks related to the intentional or unintentional misuse, manipulation of, or attacks against an AI system	Trustworthy

Sample use cases to show potential risk tier outcomes

Low Risk

Policy Compliance

- Regulatory Change Identification: Generative AI summarizes key regulation updates and guidance for skilled worker review and evaluation.

Risk Factors (not exhaustive)

- Internal use only (employees)
- Internal business data (not necessarily proprietary)
- No legal/regulatory restrictions
- No concern for bias, fairness
- No patient/member safety risk, impact to access to care

Moderate Risk

ChatGPT

- Using ChatGPT that helps write code faster and with less work. It draws context from comments and code to suggest individual lines and whole functions instantly.

Risk Factors (not exhaustive)

- Internal use only (employees)
- Insights/Human involved in decision process
- **Internal, proprietary business data**
- No legal/regulatory restrictions
- No/limited concern for bias, fairness
- No patient/member safety risk, impact to access to care

High Risk

Virtual Assistant

- Patient Engagement: Engages with members/patients allowing review of health records, appointments, Rx, etc. to cultivate a personalized experience and supports language translation

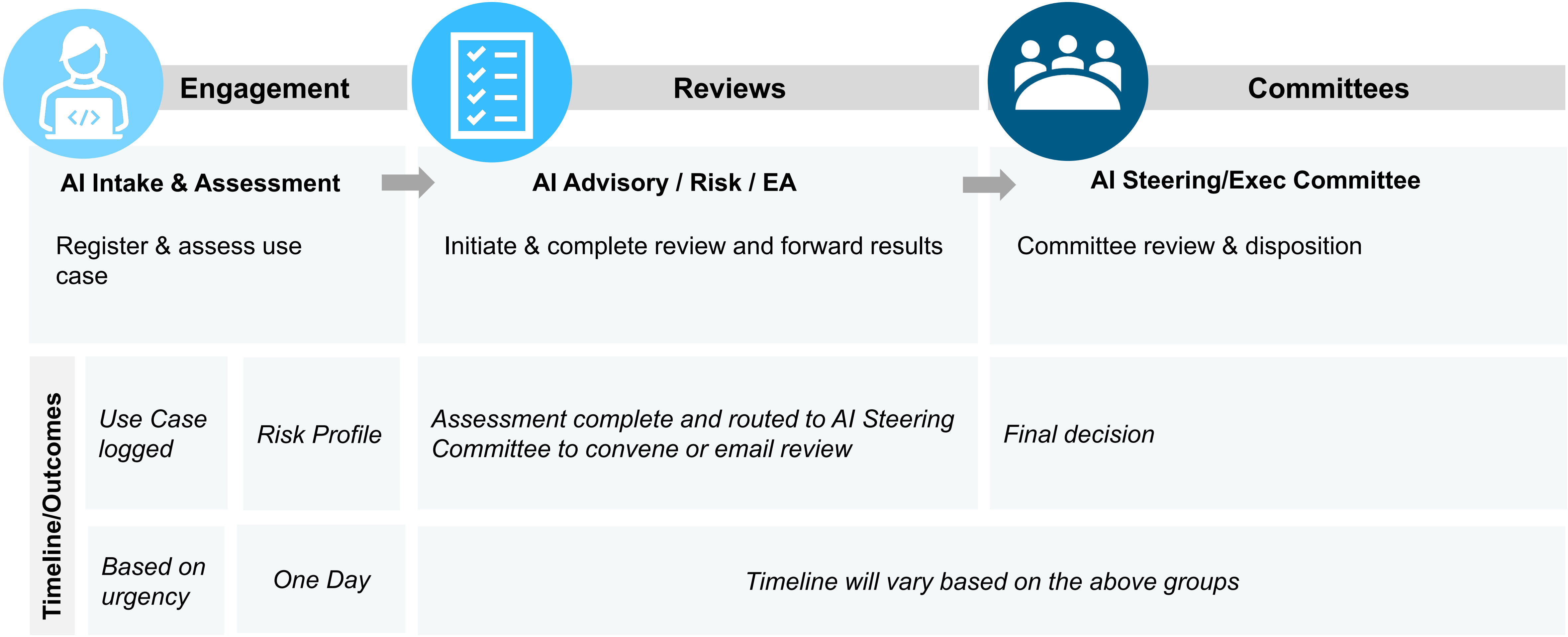
Risk Factors (not exhaustive)

- **Member use**
- **No Human involved, but needed**
- **PHI, PII data**
- **Known legal/regulatory restrictions**
- **Concern for bias, fairness**
- No patient/member safety risk, impact to access to care

RISK AND AI GOVERNANCE REQUIREMENTS INCREASING

Illustration only: Do not use for risk tiering. Actual use cases require assessment

Illustrative AI governance intake and review process



	Engagement		Reviews	Committees
	AI Intake & Assessment Register & assess use case		**AI Advisory / Risk / EA** Initiate & complete review and forward results	**AI Steering/Exec Committee** Committee review & disposition
Timeline/Outcomes	*Use Case logged*	*Risk Profile*	*Assessment complete and routed to AI Steering Committee to convene or email review*	*Final decision*
	Based on urgency	*One Day*	*Timeline will vary based on the above groups*	

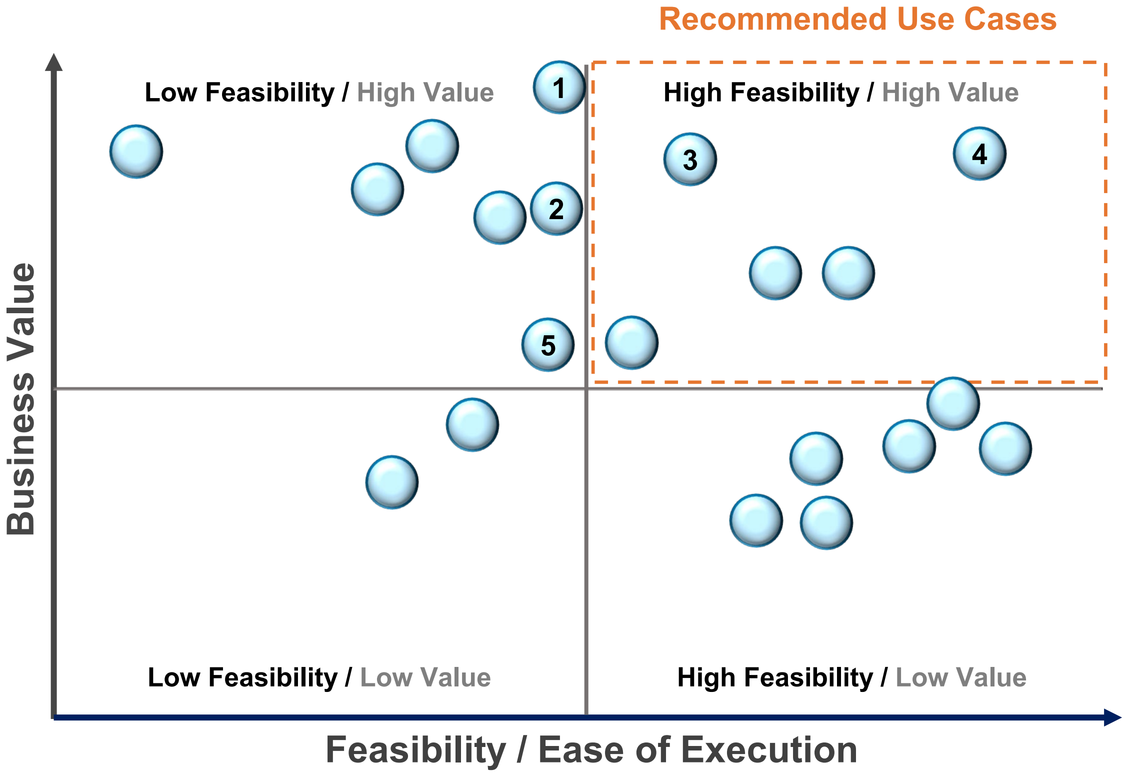
Key Points:

- Registry is hugely important; understand risk rating/tiering at intake and disposition accordingly
- Incorporate learnings to improve the process itself and above all:
- **Provide ongoing oversight and monitoring of AI use. Consider periodic review and report out on the state of the enterprise.**

Tailor the approach to your organization's objectives and capabilities to **prioritize** the most desirable, impactful, and feasible use cases

Illustrative Use Cases & Prioritization Matrix

#	Description
1	Contact Center Agent Assist
2	Member/ Provider Virtual Assistant
3	Mkt Research & Competitive Intel
4	Sales Content Generation
5	Appeals & Grievances
…	Etc.
…	Etc.
…	Etc,.



Evaluate use cases to re-validate value estimates, risk tiering, and data / architectural / talent readiness

To manage use case opportunities, develop a use case library, aligned with business units, featuring detailed descriptions, prioritization and risk ratings

Managed Care Specific Functions

Examples

- **Membership**, Billing, Enrollment, etc.
- **Claims** Payment, Correspondence, etc.
- **Sales & Marketing** Collateral, Campaigns, etc.
- Provider & **Network**… **Medical** Mgmt…, etc.

Business Functions / Corporate Services

Examples

- Corporate **Communications**
- **Finance** Budgeting, Forecasting, Close, etc.
- **Human Resources** Management
- Legal/**Regulatory** Compliance

Prioritize for value, risk, and execution

For feasibility, organizations should also ask themselves specific questions when deciding where and how to adopt and implement AI-powered processes

1 **Smart Infrastructures**: *Does my organization have the infrastructure capable of contemplating an AI roadmap? Are we sufficiently cloud-native, tech-savvy, and not addressing tech debt that limits our abilities?*

2 **Systems of Record:** *Does my organization have a digital system(s) of record? Are those systems integrated in a structured manner? Do I have pockets of digital blinders?*

3 **Decision Intelligence**: *Do I have the technical infrastructure and data to make intelligent decisions? Is the data timely and accurate? What opportunities could materialize through the application of intelligent decision support?*

4 **Intelligent Orchestration:** *Is my organization burdened by excessive and unnecessary human activity? What barriers make that human activity necessary? Are they intelligent barriers?*

5 **Amplified Experience:** *What would my organization look like with the amplification and digitization of the consumer/customer/patient experience? What opportunities are we missing because of limitations?*

6 **Competitive Landscape:** *What does the competitive landscape look like when assessed against the factors above? What threats do we face if we do not lean into this opportunity as aggressively as the competition?*

7 **Team/Talent/Timing:** *Do I have the right team, the right talent base, and the right timing around these opportunities? Where would this rank against other priorities? Can I balance this with my other priorities?*

List of key responsibilities and essential skill sets required for different compliance/ risk management roles during the AI governance lifecycle *(not exhaustive)*

Roles	Example Responsibilities	Skills Required
Legal/Privacy/ Compliance	• Monitor and interpret AI regulations, ensure compliance, offer guidance, assess risks, and prepare for audits with proper documentation	• Expert in AI regulations, translates technical standards, ensures ethical practices, compliance, assists audits, and develops governance frameworks
Enterprise Architecture	• Ensure cohesive enterprise architecture and review landscape to meet AI policy/needs	• Experience conducting AI assessments to provide recommendations based on the findings
Technology Risk / Vendor Management	• Facilitate AI procurement, review risks, and restrict data transfer in contracts	• Expert in third-party procurement, AI risk taxonomy and assessments
Cybersecurity & IT Operations	• Offer security and IT guidance, review AI projects, assess use cases, and maintain “golden” AI stack	• Skilled in AI/ML architecture, data management, infrastructure, and security assessments with actionable recommendations

AI Employee Guidelines, Policies, and Contracts

Belinda Luu, Senior Counsel, Strategic Leader of AI & Data Governance

Considerations for AI Policies and Procedures

Review existing policies to address new challenges of GenAI

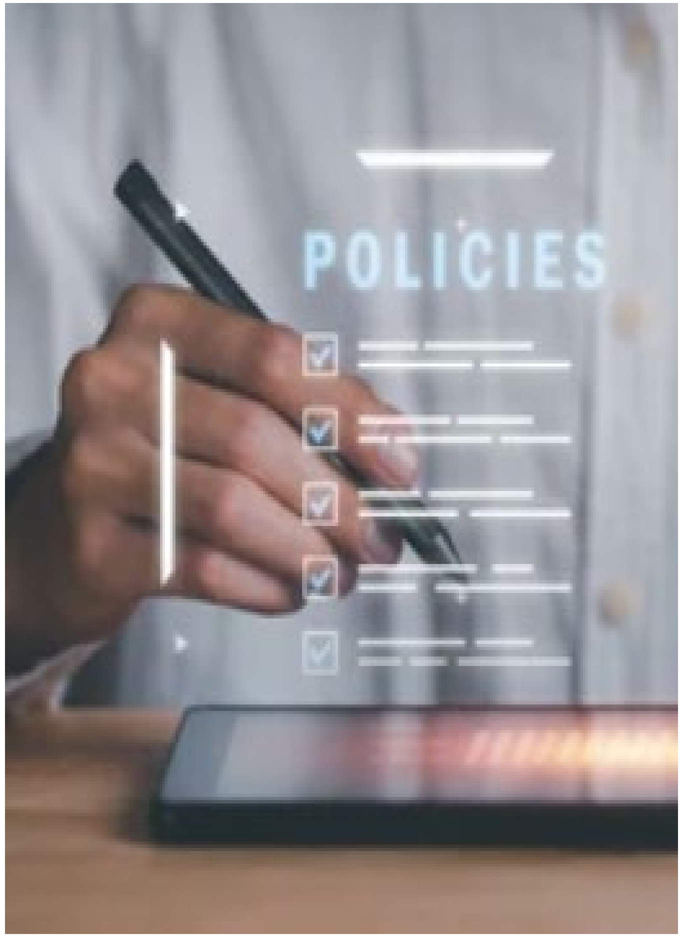
- Privacy, security, procurement, data and IT assets policies etc.
- Any **approved licensed GenAI** vs public tools
- **Additional security and privacy and data controls** e.g. NIST Risk Framework
- Categories of **permissible data** input into GenAI tools
- **Privacy Policy; consents** – data rights

Intake and approval process for AI use cases

- **AI use case intake and approval process**
- Include **risk taxonomy** and examples of **corresponding use cases**
- Describe **approved vs unapproved AI applications** and **use cases**

Make clear what employees are responsible for

- **Validate output** to be accurate and complete
- **Retain professional and clinical judgement** and decision-making
- **Don't violate third-party IP or privacy rights** – right of privacy or publicity
- **Check for bias** – training dataset and output impact



Considerations For Employee Guidelines and Training

Use guidelines for particular employee roles and use cases

- **End user and/or developer** of AI tool
- **Specific types of Gen AI** e.g. Chatbot/copilot, listening or transcription tool, image scanning, virtual assistant

Include flow down restrictions from Third Party Term of Use and AUPs

- **Identify when an AI tool is used** to generate AI outputs
- **Open-source terms restrictions** - identify acceptable open-source models

Development of AI inventory

- **Regulatory reporting** and disclosures
- **Patient and employee opt-outs**

Training

- ○ **Train on non-obvious GenAI uses** e.g. public ChatGPT or copilot embedded tools
  - ▪ Remind them of existing privacy, confidentiality, security, and procurement policies
- ○ **List of approved vs unapproved GenAI applications and use cases**

Thank You

Hovannes Daniels
VP, Care Delivery Data & Analytics

Belinda Luu
Senior Counsel, Strategic Leader of AI & Data Governance

KAISER PERMANENTE®