A Framework for Managing Artificial Intelligence & Third-Party Risk Management: Medicare Advantage

April 28, 2026

Joshua Aubey

Chief Compliance & Privacy Officer

WellBe Senior Medical

16+ years compliance

10 years audit, SOX

Brandin Brooks

Senior Credentialing Specialist

WellBe Senior Medical

7+ years credentialing

7 years computer tech

Disclaimer: The views and opinions expressed here are **solely those of the presenters** and do not reflect the official policy or position of WellBe Senior Medical.

Important Notice: This information is provided for **general educational purposes** and does not constitute **legal advice**. No attorney-client relationship is formed by this content. Because laws vary by jurisdiction, you should consult a **qualified professional** regarding your specific situation.

Agenda

I. AI Risks in Healthcare (AIRM)

II. Healthcare Third-Party Risk (TPRM)

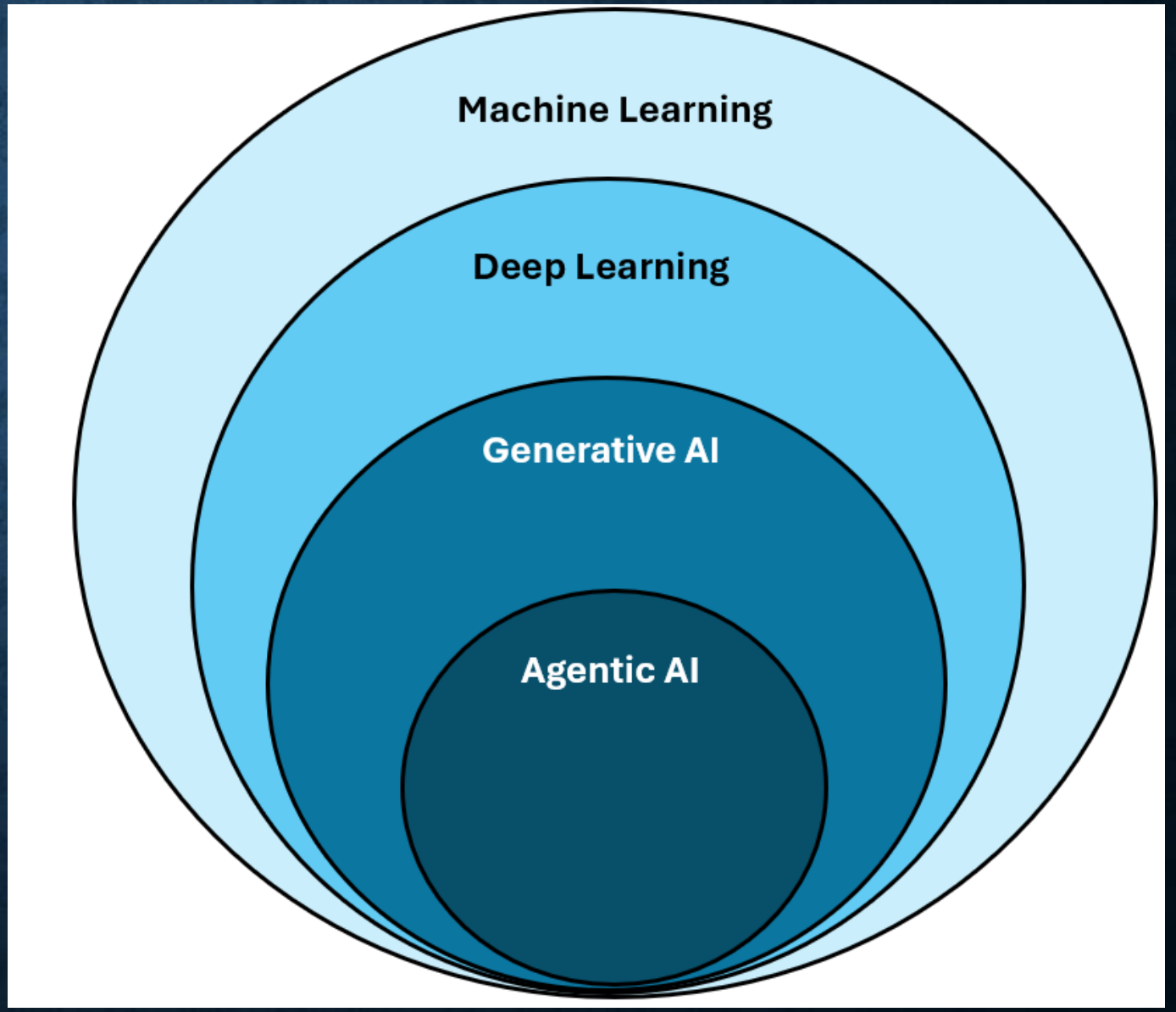
III. Risk Crossroads: AIRM + TPRM

IV. Key Contractual Safeguards

V. AIRM + TPRM Governance

Artificial Intelligence Types

- **Machine Learning**
  - Statistical models that improve a task
- **Deep Learning**
  - Algorithms learn more complex tasks like image recognition and text prediction
- **Generative AI**
  - Algorithms and training data have increased to enormous size, allowing near human level language generation
- **Agentic AI**
  - Autonomously solve multi-step problems



AI Risks in Healthcare: Instinct v. Intuition

- *Instinct*
  - Inborn, **unlearned**, and genetically hardwired behavior pattern allowing **organisms** to respond to environmental stimuli without conscious reasoning.
  - Often felt as an **emotion** (fear, urgency); Humans can be unpredictable
  - Deeply tied to social connection and moral judgment.
- AI's *"Synthetic Intuition"*
  - Ability to acquire knowledge or make decisions rapidly from pattern recognition, often experienced by humans as a "gut feeling".
  - While beneficial for fast decision-making, it can be flawed by biases.
- Take-Away – ***Illinois Public Act 104-0054 (Use in Behavioral Health)***
  - While AI will unlikely become indistinguishable from humans in its responses, it may never possess instinct in the biological sense. - ***Think about use case***
  - Rely on human instinct: ED, behavioral health, social workers, paramedics

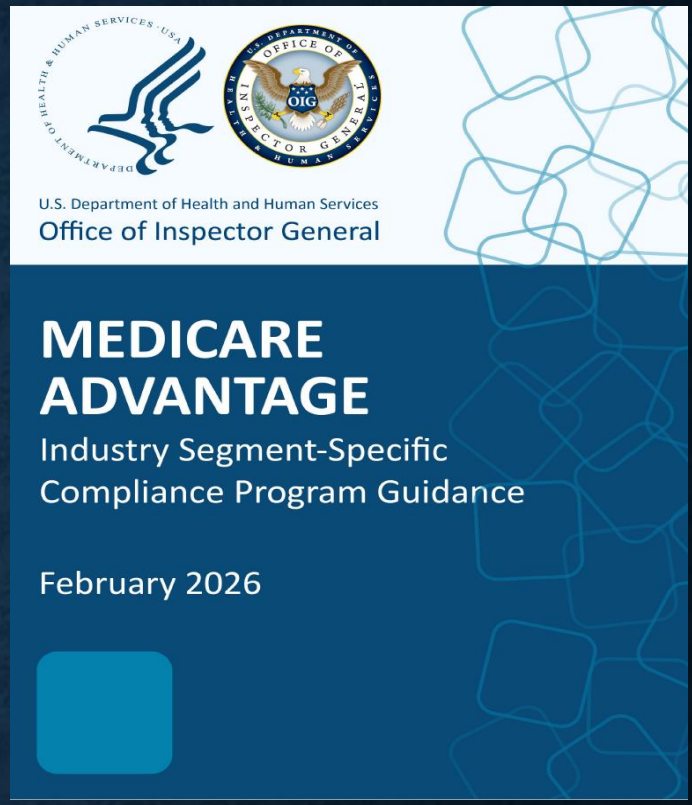
AI Risks in Healthcare: New Trust Boundaries

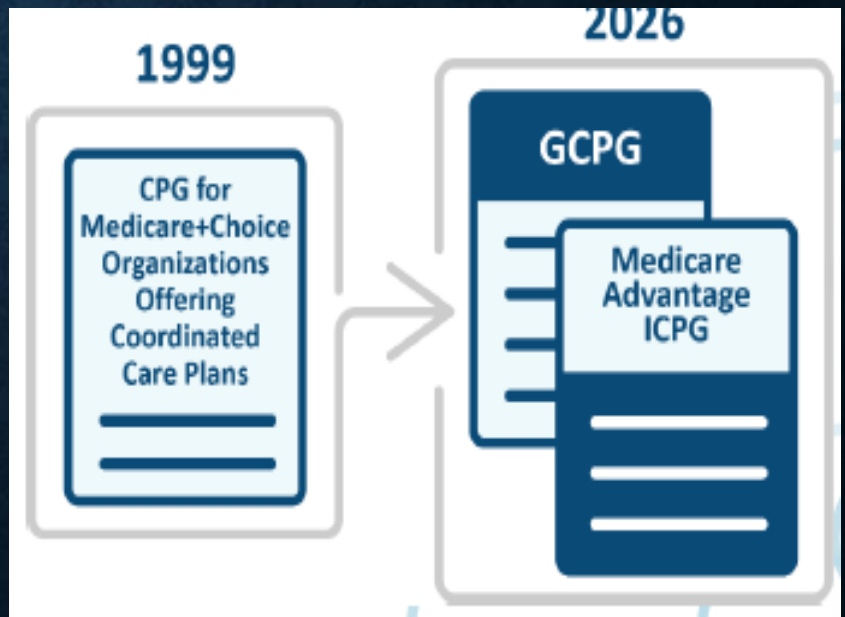
- Agents and Tools
  - When an AI system can call tools or take actions, the trust boundary shifts from "generate text" to "interact with business systems." The organization must ask what the model can access, what actions it can trigger, and under whose identity those actions run. This is a much bigger risk than a passive chatbot.
- RAG Connectors
  - Retrieval-augmented generation connects a model to enterprise content so responses are grounded in your own data. *Why this matters*: every connector is another data-access path and another governance point for permissions, retrieval quality, logging, and exposure.
- Pre-trained Models and Datasets
  - Many vendors rely on a base model and training corpus they did not build themselves. That creates a supply-chain boundary: your organization may be accountable for outputs and risks, but not fully control the upstream training data, safety tuning, or embedded limitations of the base system.

Healthcare Third-Party Risk: OIG - MA

- OIG recent guidance on effective MA compliance program – suggested elements and risk areas

- Key Risk Areas:
  - Access to Care
  - Marketing and Enrollment
  - Risk Adjustment
  - Quality of Care
  - **Oversight of Third Parties**
  - Compliance Programs Within Vertically Integrated Organizations and Other Ownership Structures
  - Submission of Accurate Claims





Third-Party Risk: OIG ICPG - MA

- First Tier, Downstream, Related Entity (FDR) "Critical Vendor"
  - CMS regulations require MAOs to conduct auditing and monitoring of FDRs
  - Medicare program requirements explicitly apply to FDRs to whom an MAO has delegated administrative or health care service functions
  - If an FDR fails to comply with program requirements, CMS can hold the MAO responsible
  - MAOs should adopt and consistently apply a clear policy that includes specific criteria for determining whether to categorize an entity as an FDR based on CMS's definition

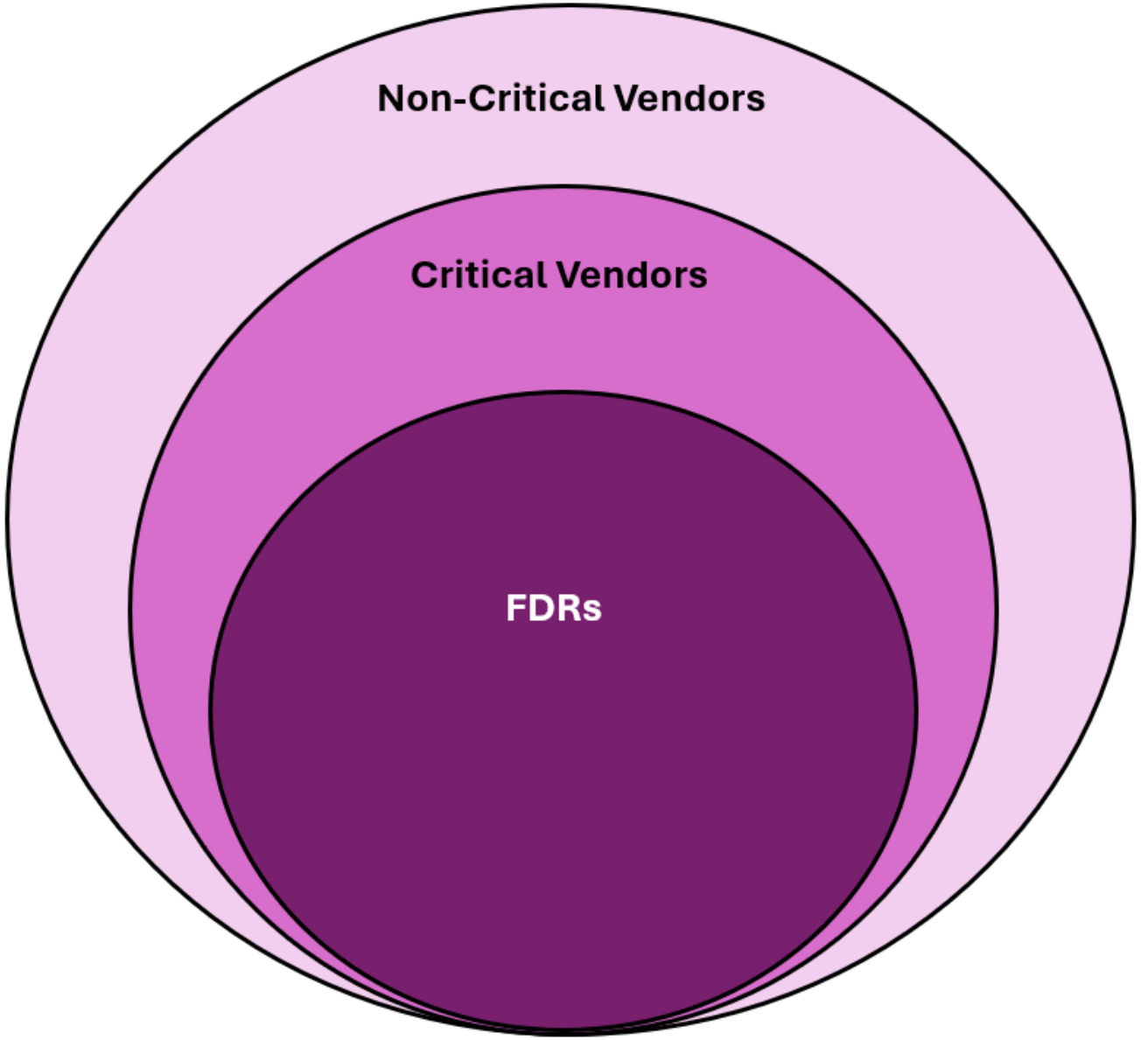
What is an FDR? An FDR is a First Tier, Downstream, or Related Entity. A first tier entity is any party that enters into a written arrangement, acceptable to CMS, with an MAO to provide administrative services or health care services to a Medicare-eligible individual under the MA program. A downstream entity is any party that enters into a written arrangement, acceptable to CMS, with persons or entities involved with the MA benefit, below the level of the arrangement between an MAO and a first tier entity. These written arrangements continue down to the level of the ultimate provider of both health and administrative services. A related entity means any entity that is related to an MAO by common ownership or control and that: (1) performs some of the MAO's management functions under contract or delegation, (2) furnishes services to Medicare enrollees under an oral or written agreement, or (3) leases real property or sells materials to the MAO at a cost of more than $2,500 during a contract period.

Healthcare Third-Party Risk: Oversight

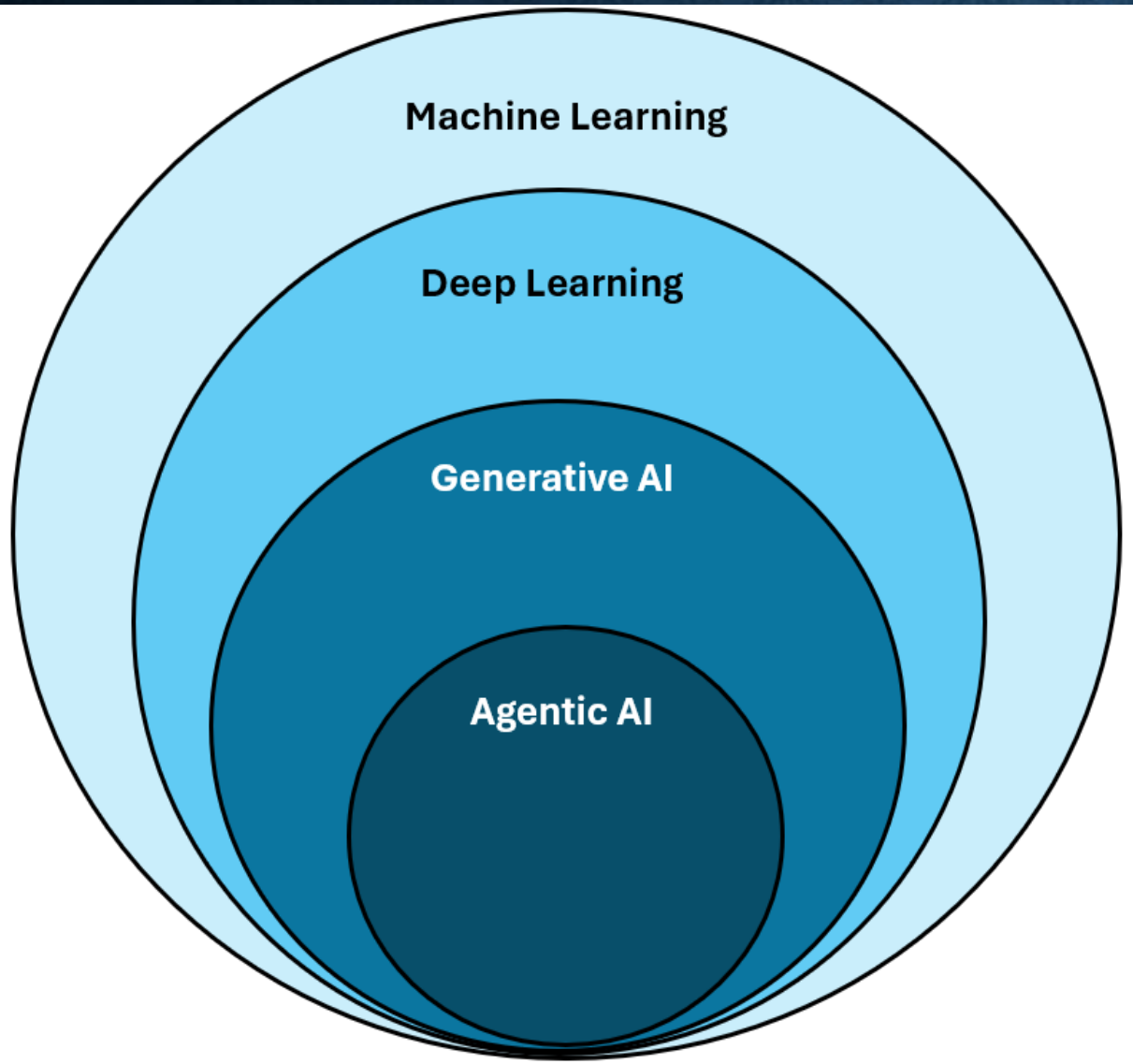
- **Selecting Third Parties (Business Owner)**
  - Ensure not excluded/preclusions
  - Offshoring/access to PHI (HIPAA) - Authorization from MAOs prior to contracting
- **Crafting Compliance-Focused Agreements (Contracting)**
  - Criteria for identifying whether a third party is a "**critical vendor**"
    - FDR is a subset of "critical vendor" (CMS delegated function)
    - Criteria for critical vendor = $, impact on patient care, impact on operations
  - Including appropriate language in contracts
    - Data backup/disaster recovery, audit rights (also a HITRUST tie-in)
    - Exclusions
    - Compliance training and monitoring
- **Ongoing Oversight of Third Parties and Corrective Action**
  - Audit rights / Attestations based on level and depth of risk
  - Centralized third party risk management, central inventory of all third parties – examples being vendors, distributors, consultants and agents

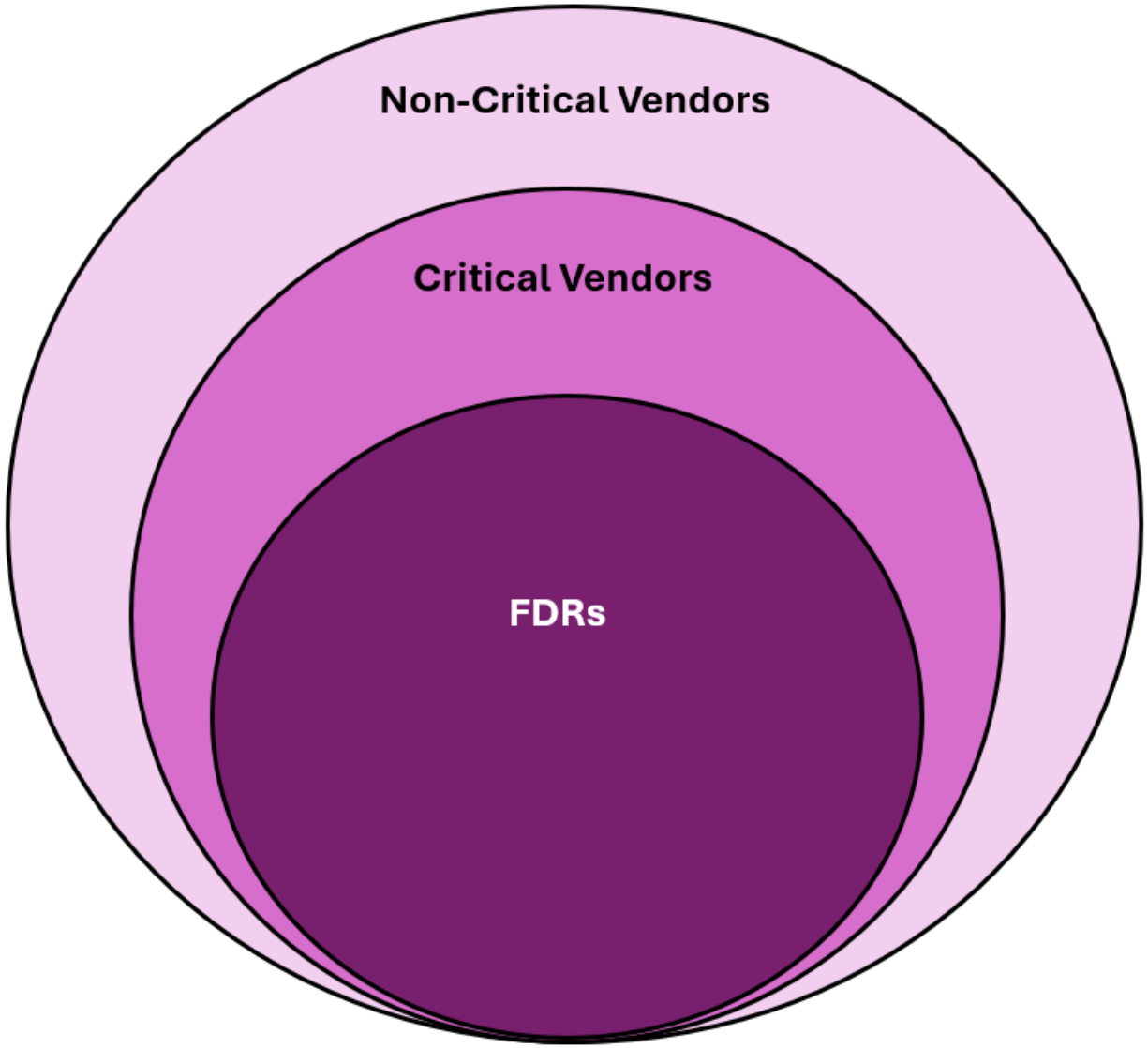
TPRM: Vendor Types

- **Non-Critical Vendors**
  - Require least effort during contract review/negotiation
    - No PHI involved
    - Exclusions check/Anti-kickback
    - No monitoring/infrequent monitoring
- **Critical Vendors** ("Keep the lights on")
  - Criteria:
    - Direct patient contact/interaction
    - Access to PHI/PII
    - Revenue impact
    - High $ cost (ex. $50,000/yr)
    - Operations impact (business continuity)
    - IT Security
- **FDRs**
  - More contracting provisions (offshore)
  - Frequent/mandatory monitoring



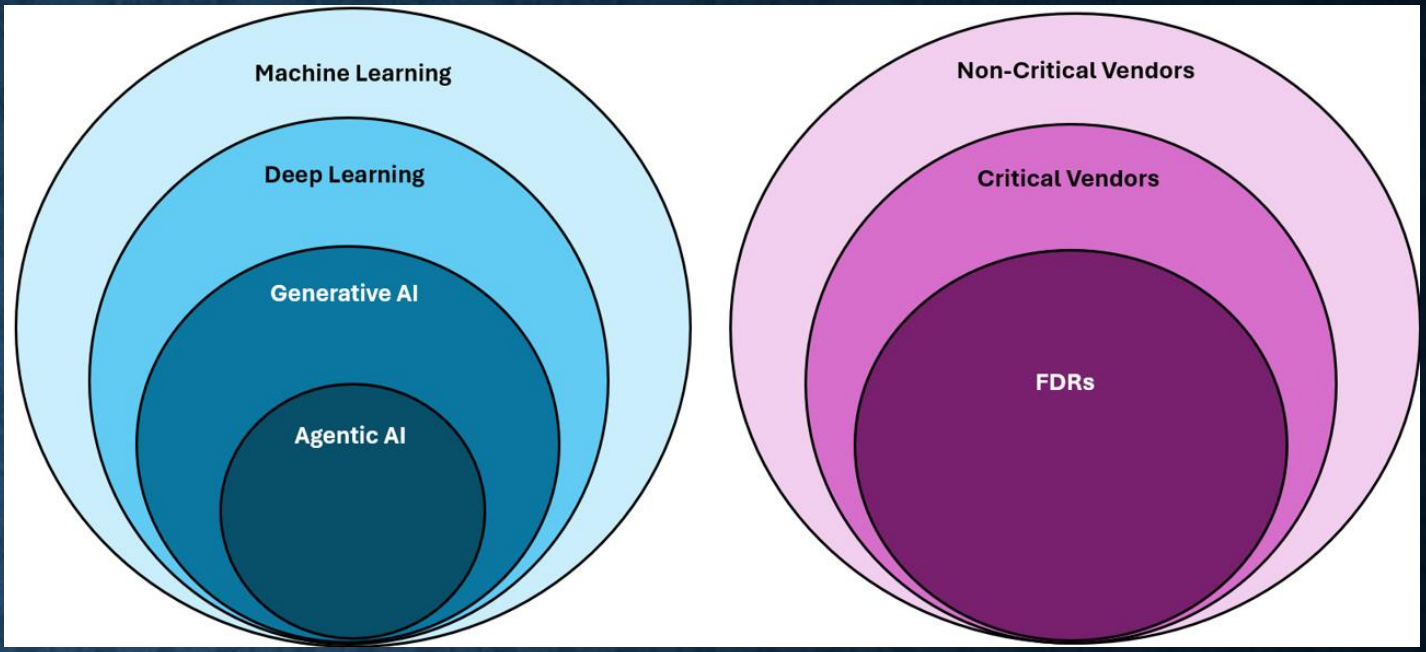
Risk Crossroads: AIRM + TPRM





Risk Crossroads

- **Category I (Least Risk)**
  - Non-critical vendors + Generic AI usage (automate a workflow)/Machine Learning/Deep Learning/Generative AI (**Use Case**: internal administrative support)
- **Category II (Medium Risk)**
  - Non-critical vendors + Machine Learning/Deep Learning/Generative AI (**Use Case**: external interaction or professional guidance)
  - Critical vendors + Machine Learning/Deep Learning
- **Category III (Highest Risk)**
  - Non-critical vendors + Agentic AI/Predictive
  - Critical vendors + Generative AI/Agentic
  - FDRs (downstream) + any form of AI



Consider Use Case for Non-Critical Vendors!

Two overarching caveats:

- State/Federal Laws
- Health Plan/Upstream Partner Contracts

Key Contractual Safeguards (One Framework)

- **Category I**
  - Exclusions (initial and ongoing monitoring)
  - Anti-kickback provision
  - Prohibited from using confidential information to train the model
  - Requirements for storage (encryption at rest/in transit) of client data
  - IT Security Risk Assessment/Questionnaire (mandatory for HITRUST)
  - Intellectual Property
  - Liability & Indemnification
  - If status of the AI system changes in a way that materially modifies scope & nature of AI, immediate notification and client prior approval required. In other words, vendor must stick to agreed-upon model characteristics
  - Business Associate Agreement (temporary access/storage of PHI)

Key Contractual Safeguards (One Framework)

- **Category II** (All Category I Safeguards +)
  - Patient Consent & Disclosure Requirements
  - Audit rights to review model drift & bias
  - Intellectual Property addresses third-party copyright risks
  - Liability & Indemnification – elevated risk
  - Insurance (cyber includes Errors & Omissions)
  - Immediate termination
  - Patient Safety Organization reporting (if advising on patient care)
  - Business Associate Agreement (if access to PHI) + cyber insurance covering breach

Key Contractual Safeguards (One Framework)

- **Category III** (All Category II Safeguards +)
  - Consider Pilot Program before full impl
  - Data Backup & Disaster Recovery requirements
  - General Audit Rights (includes DBDR Plan)
- **FDR** (All Category III Safeguards +)
  - Medicare Advantage Required Provisions
    - Code of Conduct
    - Compliance Policies
    - IT Security Policies (AUP)
    - Training within 90 days of hire and annually thereafter
      - FWA
      - HIPAA Privacy/Security
      - Code of Conduct
      - IT Security
      - HR (sexual harassment & bystander)
    - Access to Internal Records

AIRM+TPRM Governance

- Compliance/Legal: Evaluates regulatory fit, delegated-risk implications, consumer/member impacts, and whether the use case creates unacceptable legal or program risk. Redlines contracts to include Category I/II/III provisions.
- Privacy: Assesses data use, retention, training, consent, disclosures, and regulated-data implications.
- Information security: Evaluates architecture, access, logging, vendor dependencies, incident handling, and connector/tool risk.
- Clinical leadership: Needed when outputs can affect care decisions, utilization, member communications, or other clinical workflows.
- Enterprise AI Committee: Serves as the cross-functional approval body for higher-risk uses, exceptions, pilots, and major changes. Oversight of Category II & III vendors, while ratifying Category I.